UKRAINE MINISTRY OF TRANSPORT AND COMMUNICATION

STATE ADMINISTRATION OF COMMUNICATION

POPOV A.S. ODESSA NATIONAL ACADEMY OF TELECOMMUNICATIONS

FOREIGN LANGUAGES DEPARTMENT

E.V. Zavalevskaya, N.Ph. Minich

INFORMATION TECHNOLOGY

Odessa 2009

Zavalevskaya E.V., Minich N.Ph. Information Technology: Textbook, Odessa, Popov A.S. ONAT, 2009. – 144 p.

The present textbook on IT is intended for first and second year students of technical faculties. Assignments and exercises in the present book will aide in the development of technical terminology and related areas in order to work and dissmeninate their knowledge in a professional environment.

Ratified at
Foreign Languages Department of
Popov A.S. Odessa National Academy of Telecommunications
Protocol № 3 dated <u>31 November, 2008.</u>

Ratified at
the Academic Council meeting of
Popov A.S. Odessa National Academy of Telecommunications
Protocol № 6 dated <u>10 February, 2009.</u>

CONTENTS

MODULE I

UNIT I
COMPUTERS MAKE THE WORLD SMALLER AND SMARTER

The ability of tiny computing devices to control complex operations has transformed the way many tasks are performed, ranging from scientific research to producing consumer products. Tiny 'computers on a chip' are used in medical equipment, home appliances, cars and toys. Workers use handheld computing devices to collect data at a customer site, to generate forms, to control inventory, and to serve as desktop organisers.

Not only is computing equipment getting smaller, it is getting more sophisticated. Computers are part of many machines and devices that once required continual human supervision and control. Today, computers in security systems result in safer environments, computers in cars improve energy efficiency, and computers in phones provide features such as call forwarding, call monitoring, and call answering.

These smart machines are designed to take over some of the basic tasks previously performed by people; by so doing, they make life a little easier and a little more pleasant. Smart cards store vital information such as health records, drivers' licenses, bank balances, and so on. Smart phones, cars, and appliances with built in computers can be programmed to better meet individual needs. A smart house has a built-in monitoring system that can turn lights on and off, open and close windows, operate the oven, and more.

With small computing devices available for performing smart tasks like cooking dinner, programming the VCR, and controlling the flow of information in an organization, people are able to spend more time doing what they often do best – being creative. Computers can help people work more creatively.

Multimedia systems are known for their educational and entertainment value, which we call 'edutainment'. Multimedia combines text with sound, video, animation, and graphics, which greatly enhances the interaction between user and machine and can make information more interesting and appealing to people. Expert systems software enables computers to 'think' like experts. Medical diagnosis expert systems, for example, can help doctors pinpoint a patient's illness, suggest further tests, and prescribe appropriate drugs.

Connectivity enables computers and software that might otherwise be incompatible to communicate and to share resources. Now that computers are proliferating in many areas and networks are available for people to access data and communicate with others, personal computers are becoming interpersonal PCs. They have the potential to significantly improve the way we relate to each other. Many people today telecommute – that is, use their computers to stay in touch with the office while they are working at home. With the proper tools, hospital staff can get a diagnosis from a medical expert hundreds or thousands of miles away. Similarly, the disabled can communicate more effectively with others using computers.

Distance learning and videoconferencing are concepts made possible with the use of an electronic classroom or boardroom accessible to people in remote locations.

Vast databases of information are currently available to users of the Internet, all of whom can send mail messages to each other. The information superhighway is designed to significantly expand this interactive connectivity so that people all over the world will have free access to all these resources.

People power is critical to ensuring that hardware, software, and connectivity are effectively integrated in a socially responsible way. People – computer users and computer professionals – are the ones who will decide which hardware, software, and networks endure and how great an impact they will nave on our lives. Ultimately people power must be exercised to ensure that computers are used not only efficiently but in a socially responsible way.

A: *Answer the questions:*
1. Name some types of devices that use 'computers on a chip'.
2. What uses of handheld computers are mentioned in the text?
3. What are the benefits of using computers with the following items?
    a) Security systems
    b) Cars
    c) Phones
4. What smart devices are mentioned in the text?
5. What are smart cards used for?
6. What are the advantages of multimedia?
7. What can medical expert systems do?
8. How can computers help the disabled?
9. What types of computing systems are made available to people in remote locations using electronic classrooms or boardrooms?
10. What aspects of computing can people power determine?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Edutainment	**1)** Software that enables computers to 'think' like experts.
b) Multimedia	**2)** Use computers to stay in touch with the office while working at home.
c) Expert system	**3)** Internet system designed to provide free, interactive access to vast resources for people all over the world.
d) Telecommute	
e) Information superhighway	**4)** Multimedia materials with a combination of educational and entertainment content.
	5) A combination of text with sound, video, animation, and graphics.

C: *Mark the following statements as True or False:*
1) Desktop organisers are programs that require desktop computers.
2) Computers are sometimes used to monitor systems that previously needed human supervision.
3) Networking is a way of allowing otherwise incompatible systems to communicate and share resources.
4) The use of computers prevents people from being creative.
5) Computer users do not have much influence over the way that computing develops.

D: *What do these abbreviations mean? Use the Glossary if necessary.*
1) CD-ROM   **5)** AGP
2) RDRAM   **6)** SDRAM
3) MB   **7)** SVGA
4) GHz

UNIT II
CACHE MEMORY

Most PCs are held back not by the speed of their main processor, but by the time it takes to move data in and out of memory. One of the most important techniques for getting around this bottleneck is the memory cache

The idea is to use a small number of very fast memory chips as a buffer or cache between main memory and the processor. Whenever the processor needs to read data it looks in this cache area first. If it finds the data in the cache then this counts as a 'cache hit' and the processor need not go through the more laborious process of reading data from the main memory. Only if the data is not in the cache does it need to access main memory, but in the process it copies whatever it finds into the cache so that it is there ready for the next time it is needed. The whole process is controlled by a group of logic circuits called the cache controller.

One of the cache controller's main jobs is to look after „cache coherency" which means ensuring that any changes written to main memory are reflected within the cache and vice versa. There are several techniques for achieving this, the most obvious being for the processor to write directly to both the cache and main memory at the same time. This is known as a "write through" cache and is the safest solution but also the slowest.

The main alternative is the "write-back" cache which allows the processor to write changes only to the cache and not to main memory. Cache entries that have changed are flagged as 'dirty', telling the cache controller to write their contents back to main memory before using the space to cache new data. A write-back cache speeds up the write process, but does requite a more intelligent cache controller.

Most cache controllers move a "line" of data rather than just a single item each time they need to transfer data between main memory and the cache. This tends to improve the chance of a cache hit as most programs spend their time stepping through instructions stored sequentially in memory rather than jumping about from one area to another. The amount of data transferred each time is known as the "line size".

How a Disk Cache Works

Disk caching works in essentially the same way whether you have a cache on your disk controller or you are using a software-based solution. Tire CPU requests specific data from the cache. In some cases, the information will already be there and the request can be met without accessing the hard disk.

It the requested information isn't in the cache, the data is read from the disk along with a large chunk of adjacent information. The cache then makes room for the

new data by replacing old. Depending on the algorithm that is being applied, this may be the information that has been in the cache the longest or the information that is the least recently used. The CPU's request can then be met, and the cache already has the adjacent data loaded in anticipation of that information being requested next.

A: *Answer the questions:*

1. What is one of the main causes of a PC not running at its highest potential speed?

2. What word in the text is used instead of "buffer"?

3. What device looks after cache coherency?

4. What is the main alternative to "write-through cache"?

5. When does a write-back cache write its contents back to main memory?

6. When is data marked as "dirty" in a write-back cache?

7. What determines what data is replaced in a disk cache?

B: *Match the terms in Table A with the statements in Table B.*

Table A	Table B
a) Cache hit **b)** Cache controller **c)** Cache coherency **d)** Write-through cache **e)** Write-back cache **f)** Line size	**1)** The process of writing changes only to the cache and not to main memory unless the space is used to cache new data. **2)** The amount of data transferred to the cache at any one time. **3)** The process of writing directly to both the cache and main memory at the same time. **4)** The processor is successful in finding the data in the cache. **5)** Ensuring that any changes written to main memory are reflected within the cache and vice versa. **6)** The logic circuits used to control the cache process.

C: *Mark the following statements as True or False:*

a) Cache memory is faster than RAM.

b) The processor looks for data in the main memory first.

c) Write-through cache is faster than write-back cache.

d) Write-back cache requires a more intelligent cache controller.

e) Most programs use instructions that are stored in sequence in memory.

f) Most cache controllers transfer one item of data at a time.

g) Hardware and software disk caches work in much the same way.

UNIT III
DATA MINING

Data mining is simply filtering through large amounts of raw data for useful information that gives businesses a competitive edge. This information is made up of meaningful patterns and trends that are already in the data but were previously unseen.

The most popular tool used when mining is artificial intelligence (AI). AI technologies try to work the way the human brain works, by making intelligent guesses, learning by example, and using deductive reasoning. Some of the more popular AI methods used in data mining include neural networks, clustering, and decision trees.

Neural networks look at the rules of using data, which are based on the connections found or on a sample set of data. As a result, the software continually analyses value and compares it to the other factors, and it compares these factors repeatedly until it finds patterns emerging. These patterns are known as rules. The software then looks for other patterns based on these rules or sends out an alarm when a trigger value is hit.

Clustering divides data into groups based on similar features or limited data ranges. Clusters are used when data isn't labelled in a way that is favourable to mining. For instance, an insurance company that wants to find instances of fraud wouldn't have its records labelled as fraudulent or not fraudulent. But after analysing patterns within clusters, the mining software can start to figure out the rules that point to which claims are likely to be false.

Decision trees, like clusters, separate the data into subsets and then analyse the subsets to divide them into further subsets, and so on (for a few more levels). The final subsets are then small enough that the mining process can find interesting patterns and relationships within the data.

Once the data to be mined is identified, it should be cleansed. Cleansing data frees it from duplicate information and erroneous data. Next, the data should be stored in a uniform format within relevant categories or fields. Mining tools can work with all types of data storage, from large data warehouses to smaller desktop databases to flat files. Data warehouses and data marts are storage methods that involve archiving large amounts of data in a way that makes it easy to access when necessary.

When the process is complete, the mining software generates a report. An analyst goes over the report to see if further work needs to be done, such as refining parameters, using other data analysis tools to examine the data, or even scrapping the data if it's unusable. If no further work is required, the report proceeds to the decision makers for appropriate action.

The power of data mining is being used for many purposes, such as analysing Supreme Court decisions, discovering patterns in health care, pulling stories about competitors from newswires, resolving bottlenecks in production processes, and analysing sequences in the human genetic makeup. There really is no limit to the type of business or area of study where data mining can be beneficial.

A: *Answer the questions:*
1. What tool is often used in data mining?
2. What AI method is used for the following processes?
   a) Separate data into subsets and then analyse the subsets to divide them into further subsets for a number of levels.
   b) Continually analyse and compare data until patterns emerge.
   c) Divide data into groups based on similar features or limited data ranges.
3. What term is used for the patterns found by neural networks?
4. When are clusters used in data mining?
5. What types of data storage can be used in data mining?
6. What can an analyst do to improve the data mining results?

7. Name some of the ways in which data mining is currently used.

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Data mining **b)** AI **c)** Cleansed data **d)** Data warehouse	**1)** Storage method of archiving large amounts of data to make it easy to access. **2)** Data free from duplicate and erroneous information. **3)** A process of filtering through large amounts of raw data for useful information. **4)** A computing tool that tries to operate in a way similar to the human brain.

C: *Mark the following statements as True or False:*
a) Data mining is a process of analysing known patterns in data.
b) Artificial intelligence is commonly used in data mining.
c) In data mining, patterns found while analyzing data are used for further analysing the data.
d) Data mining is used to detect false insurance claims.
e) Data mining is only useful for a limited range of problems.

D: *Complete the following description of the data mining process using words from the text:*
Large amounts of data stored in data _____ are often used for data _____. The data is first _____ to remove _____ information and errors. The _____ is then analysed using a tool such as _____ _____. An analysis report is then analysed by an _____ who decides if the _____ need to be refined, other data _____ tools need to be used, or if the results need to be discarded because they are _____. The analyst passes the final results to the _____ makers who decide on the _____ action.

UNIT IV
A: Study this data about storage devices. Then complete the blanks in the following sentences comparing and contrasting the different types.

Device	Read/Write	Speed	Media Capacity	Media Removable	Cost
Floppy disk	Read and write	Slow	Very low	Yes	Low
Fixed hard disk	Read and write	Fast	Very high	No	Medium
Removable hard disk	Read and write	Medium to fast	High	Yes	Medium
CD-ROM	Read only	Medium	High	Yes	Low
CD-R	Recordable	Slow	High	Yes	Medium
CD-RW	Read and write	Medium	High	Yes	Medium
CD-MO	Read and write	Medium	High	Yes	High
DVD-ROM	Read only	Medium	High	Yes	Medium *
DVD-RAM	Read and write	Medium	Very high	Yes	High
Magnetic Tape	Read and write	Very slow	High	Yes	Medium

1. You can write to hard disks _____ _____ optical disks.
2. Floppy disks have a   _____ capacity _____ other devices.
3. CD-ROMs and floppy disks are _____ low priced.
4. DVD-RAM has a _____ capacity _____ other optical disks.
5. CD-ROMs cannot be re-recorded _____ some other optical disks can be.
6. _____ hard disks, you can read from and write to CD-MO drives.
7. _____ CD-ROMs, CD-Rs are recordable.
8. Magnetic tape is much _____ _____ other devices.
9. _____ DVD-RAM and fixed hard disks have very high media capacity.
10. Floppy disks are cheap _____ DVD-RAM is expensive.

B: Study this list of needs. Which type of peripheral would you advise in each case?
1) Inputting printed graphics;
2) building cars;
3) controlling the screen cursor in a fast action game;
4) making choices on a screen in a public information terminal;
5) recording moving images;
6) recording a book loan in a library;
7) printing very high quality text and graphics;
8) creating drawings;
9) printing building plan drawings;
10) recording sound;
11) listening to music without disturbing others;
12) storing programs and data;
13) inputting a lot of text;
14) backing up large quantities of data.

READY FOR THE BAZILLION-BYTE DRIVE?

Thinking about writing your memoirs – putting your life story down on paper for all eternity? Why not skip the repetitive strain injury and just capture your whole life on full-motion video, putting it all in a device the size of a sugar cube? It might not be as far off as you think.

Currie Munce, director of IBM's Advanced HDD Technology Storage Systems Division, has one avowed goal: Build bigger storage. Recently Munce and his fellow Ph.Ds restored Big Blue's lead in the disk space race with a new world record for areal (bit) density: 35.3 gigabits per square inch – roughly three times as dense as any drive shipping at press time.

During the 1990s, areal density doubled every 18 months, keeping pace with the transistor density gains predicted by Moore's Law. But increasingly daunting technical challenges face those who would push the storage envelope further. 'I think magnetic recording technology has another good 5 to 10 years,' says Munce. 'After that, we'll see substantial difficulties with further advances at the pace people are accustomed to.

From here on, a phenomenon called superparamagnetism threatens to make densely-packed bits unstable. Provided that new developments continue to thwart superparamagnetic corruption, scientists speculate that the theoretical limit for discrete bit recording is 10 terabits per square inch (1 terabit = 1,000 gigabits).

Approaching this limit will require new technologies. Two possible contenders are atomic force microscopy (AFM) and holographic storage.

AFM would use a spinning plastic disk, perhaps inside a wristwatch, and a tiny, 10-micron cantilever with a 40-angstrom tip (an angstrom represents the approximate radius of an atom) to write data. In theory, AFM win allow densities of 300 to 400 gigabits per square inch.

While AFM is still in the lab, holographic storage is closer to reality. According to Rusty Rosenberger, optical program manager for Imation, 'We are targeting a5 1/4 -inch disk with 125GB of storage and a 40MB-per-second transfer rase. Future iterations of holographic systems should improve substantially.

The three-dimensional nature of holography makes it an appealing storage medium because 'pages' of data can be superimposed on a single volume – imagine transferring a whole page of text at once as opposed to reading each letter in sequence. Hans Coufal, manager of IBM's New Directions in Science and Technology Research division, predicts that the fast access rates and transfer times of holographic storage will lead to improved network searches, video on demand, high-end servers, enterprise computing, and supercomputing.

Meanwhile, also-ran technologies are thriving. Tape, first used for data storage in 1951 with the Univac I, has been revitalized by the corporate hunger for affordable archiving solutions. In the consumer arena, says Dataquest analyst Mary Craig, recordable CD-ROMs and DVDs will remain the dominant high-capacity removable storage media for the next decade. Despite their failure to match the areal density gains of hard disks, optical disks are cheap to produce, making them ideal for software distribution (until a mature digital rights management system facilitates online delivery). Finally, solid state options such as flash cards can't yet match the pricing of hard disks at high capacities.

Further out, scientists salivate over the prospect of data manipulation and storage on an atomic level. Because consumer demand for capacity is laggig behind what technology can deliver, bringing new storage options to the masses will depend on seeing the need for more space.

A: *Answer the questions:*
1. What is Currie Munce's main aim?
2. How quickly did the possible areal density of hard disks increase in the 1990s?
3. How long does Munce think magnetic recording technology will continue to make rapid advances in capacity?
4. What problem does he predict for magnetic storage?
5. What is the predicted limit for discrete bit magnetic storage capacity?
6. What storage technologies might replace current magnetic systems?
7. What is the advantage of holographic storage being three-dimensional?

8. What improvements are predicted due to the fast access rates and transfer times of holographic storage?

9. What is predicted to be the most important high capacity removable storage media in the next 10 years?

10. What method of software distribution is likely to replace optical disks?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Big Blue	**1**) Atomic force microscopy.
b) Areal density	**2**) The approximate radius of an atom.
c) Moore's Law	**3**) IBM
d) Superparamagnetism	**4**) The data capacity of a storage device measured in bits per square inch.
e) Terabit	**5**) Prediction that the number of transistors that can be incorporated into a processor chip will double every 18 months.
f) AFM	**6**) A phenomenon that threatens to make densely packed bits unstable in magnetic storage devices.
g) Angstrom	**7**) One thousand gigabits.

C: *Mark the following statements as True or False:*

a) The development of AFM is more advanced than holographic storage.

b) The predicted maximum storage density of AFM is 400 gigabits per square inch.

c) Holography works in 3D.

d) Univac I was the first computer to use tape storage devices.

e) Users want higher capacity storage devices than technology can provide.

MODULE II

UNIT V

Study this description of a computer course. Then write a description of your own computing course, or one of its components, in the same way.

COMPUTER USE AND APPLICATIONS

AIMS:

1. To introduce complete beginners to computer systems.

2. To give a basic foundation in computer technology and to introduce appropriate terminology.

3. To give a description of the major components (hardware and software) which make up a computer system.

4. To show how computer systems are used in commerce and industry.

5. To give practical experience in using various systems.

DESCRIPTION:

The course is in four parts.

Part 1. Introduction to college computer science facilities, including how to access the computers, the Unix filestore, using email, the editor and simple network commands.

Part 2. The basic structure of computer hardware and systems software. Topics include compilers interpreters and memory management.

Part 3. Introduces some more advanced software tools, documentation tools and language processors.

Part 4. Discusses various uses of computers including spreadsheets, databases, communications and impacts on society.

STAFF:
Dr Peter Jones

METHOD AND FREQUENCY OF CLASS:
Two lectures per week with practical exercises once every two weeks.

ASSESSMENT:
Three formal coursework assignments.

UNIT VI
OPERATING SYSTEMS: HIDDEN SOFTWAR

When a brand new computer comes off the factory assembly line, it can do nothing. The hardware needs software to make it work. Are we talking about applications software such as word processing or spreadsheet software? Partly. But an applications software package does not communicate directly with the hardware. Between the applications software and the hardware is a software interface – an operating system. An operating system is a set of programs that has between applications software and the computer hardware.

The most important program in the operating system, the program that manages the operating system, is the supervisor program, most of which remains in memory and is thus referred to as resident. The supervisor controls the entire operating system and loads into memory other operating system programs (called nonresident) from disk storage only as needed.

An operating system has three main functions: (1) manage the computer's resources, such as the central processing unit, memory, disk drives, and printers, (2) establish a user interface, and (3) execute and provide services for applications software. Keep in mind, however, that much of the work of an operating system is hidden from the user, In particular, the first listed function, managing the computer's resources, is taken care of without the user being aware of the details. Furthermore, all input and output operations, although invoked by an applications program, are actually carried out by the operating system.

A: *Find the answers to these questions:*
1. What difference is there between applications software and operating systems?

2. Why is the supervisor program the most important operating system program?

3. What is the difference between resident and non-resident programs?

4. What are the main functions of an operating system?

B: *Complete the gaps in this summary of the text on operating systems using these linking words and phrases:*

although / in addition / because / such as / but / therefore

The user is aware of the effects of different applications programs _____ operating systems are invisible to most users. They lie between applications programs, _____ wordprocessing, and the hardware. The supervisor program is the most important. It remains in memory, _____ it is referred to as resident. Others are called non-resident _____ they are loaded into memory only when needed. Operating systems manage the computer's resources, _____ the central processing unit. _____, they establish a user interface, and execute and provide services for applications software. _____ input and output operations are invoked by programs, they are carried out by the operating system.

UNIT VII
LINUX

Linux has its roots in a student project. In 1992, an undergraduate called Linux Torvalds was studying computer science courses, a big component of it was taught on (and about) Unix. Unix was the wonder operating system of the 1970s and 1980s: both a textbook example of the principles of operating system design, and sufficiently robust to be the standard OS in engineering and scientific computing. But Unix was a commercial product (licensed by ATELT to a number of resellers), and cost more than a student could pay.

Annoyed by the shortcomings of Minix (a compact Unix clone written as a teaching aid by Professor Andy Tannenbaum) Linux set out to write his own 'kernel' – the core of an operating system that handles memory allocation, talks to hardware devices, and makes sure everything keeps running. He used the GNU programming tools developed by Richard Stallman's Free Software Foundation, an organization of volunteers dedicated to fulfilling Stallman's ideal of making good software that anyone could use without paying. When he'd written a basic kernel, he released the source code to the Linux kernel on the Internet.

Source code is important. It's the original from which compiled programs are generated. If you don't have the source code to a program, you can't modify it to fix bugs or add new features. Most software companies won't sell you their source code, or will only do so for an eye-watering price, because they believe that if they make it available will destroy their revenue stream.

What happened next was astounding, from the conventional, commercial software industry point of view – and utterly predictable to anyone who knew about the Free Software Foundation. Programmers (mostly academics and students) began using Linux. They found that it didn't do things they wanted it to do – so they fixed it. And where they improved it, they sent the improvements to Linux, who rolled them into the kernel. And Linux began to grow.

There's a term for this model of software development; it's called Open Source (*see* www.opensource.org/). Anyone can have the source code – it's free (in the sense of free speech, not free beer). Anyone can contribute to it. If you use it heavily you may want to extend or develop or fix bugs in it – and it is so easy to give your fixes back to the community that most people do so.

An operating system kernel on its own isn't a lot of use; but Linux was purposefully designed as a near-clone of Unix, and there is a lot of software out there that is free and was designed to compile on Linux. By about 1992, the first 'distributions' appeared.

A distribution is the Linux-user term for a complete operating system kit, complete with the utilities and applications you need to make it do useful things – command interpreters programming tools, text editors, typesetting tools, and graphical user interfaces based on the X windowing system. X is a standard in academic and scientific computing, but not hitherto common on PCs; it's a complex distributed windowing system on which people implement graphical interfaces like KDE and Gnome.

As more and more people got to know about Linux, some of them began to port the Linux kernel to run on non-standard computers. Because it's free, Linux is now the most widely-ported operating system there is.

A: *Answer the questions:*
1. What did Linus Torvalds use to write the Linux kernel?
2. How was the Linux kernel first made available to the general public?
3. What is a programmer likely to do with source code?
4. Why will most software companies not sell you their source code?
5. What type of utilities and applications are provided in a Linux distribution?
6. What is X?
7. What graphical user interfaces are mentioned in the text?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Kernel **b)** Free Software Foundation **c)** Source code **d)** Open Source **e)** A distribution **f)** X	**1)** A type of software development where any programmer can develop or fix bugs in the software. **2)** The original systems program from which compiled programs are generated. **3)** A complete operating system kit with the utilities and applications you need to make it do useful things. **4)** A standard distributed windowing system on which people implement graphical interfaces. **5)** An organization of volunteers dedicated to making good software that anyone could use without paying. **6)** The core of an operating system that handles memory allocation, talks to hardware devices, and makes sure everything keeps running.

C: *Mark the following statements as True or False:*
a) Linux was created in the 1980s.
b) Minix was created by a university student.

c) Linux is based on Unix.

d) Minix is based on Unix.

e) Linux runs on more types of computer than any other operating system.

UNIT VIII
USER INTERFACES

Cheaper and more powerful personal computers are making it possible to perform processor-intensive tasks on the desktop. Break-throughs in technology, such as speech recognition, are enabling new ways of interacting with computers. And the convergence of personal computers and consumer electronics devices is broadening the base of computer users and placing a new emphasis on ease of use. Together, these developments will drive the industry in the next few years to build the first completely new interfaces since SRI International and Xerox's Palo Alto Research Center did their pioneering research into graphical user interfaces (GUIs) in the 1970s.

True, it's unlikely that you'll be ready to toss out the keyboard and mouse any time soon. Indeed, a whole cottage industry – inspired by the hyperlinked design of the World Wide Web – has sprung up to improve today's graphical user interface. Companies are developing products that organize information graphically in more intuitive ways. XML-based formats enable users to view content, including local and network files, within a single browser interface. But it is the more dramatic innovations such as speech recognition that are poised to shake up interface design.

Speech will become a major component of user interfaces, and applications will be completely redesigned to incorporate speech input. Palm-size and handheld PCs, with their cramped keyboards and basic handwriting recognition, will benefit from speech technology.

Though speech recognition may never be a complete replacement for other input devices, future interfaces will offer a combination of input types, a concept known as multimodal input. A mouse is a very efficient device for desktop navigation, for example, but not for changing the style of a paragraph. By using both a mouse and speech input, a user can first point to the appropriate paragraph and then say to the computer, 'Make that bold'. Of course, multimodal interfaces will involve more than just traditional input devices and speech recognition. Eventually, most PCs will also have handwriting recognition, text to speech (TTS), the ability to recognize faces or gestures, and even the ability to observe their surroundings.

At The Intelligent Room, a project of Massachusetts Institute of Technology's Artificial Intelligence Lab, researchers have given sight to PCs running Microsoft Windows through the use of video cameras, 'Up to now, the PC hasn't cared about the world around it,' said Rodney Av Brooks, the Director of MIT's Artificial Intelligence Lab. 'When you combine computer vision with speech understanding, it liberates the user from having to sit in front of a keyboard and screen.

It's no secret that the amount of information – both on the Internet and within intranets – at the fingertips of computer users has been expanding rapidly. This information onslaught has led to an interest in intelligent agents, software assistants

that perform tasks such as retrieving and delivering information and automating repetitive tasks. Agents will make computing significantly easier. They can be used as Web browsers, help-desks, and shopping assistants. Combined with the ability to look and listen, intelligent agents will bring personal computers one step closer to behaving more like humans. This is not an accident. Researchers have -long noted that users have a tendency to treat their personal computers as though they were human. By making computers more /social/ they hope to also make them easier to use.

As these technologies enter mainstream applications, they will have a marked impact on the way we work with personal computers. Soon, the question will be not 'what does software look like' but 'how does it behave?'

A: *Answer the questions:*

1. What developments are driving the development of completely new interfaces?

2. What has inspired a whole cottage industry to develop to improve today's graphical user interface?

3. In what way have XML-based formats changed the user interface?

4. What type of computers is certain to benefit from speech technology?

5. Name a process where a mouse is particularly useful and a process where it is not so useful.

6. What facilities are multimodal interfaces likely to offer in the future?

7. What type of input device will be used to give vision to the user interface?

8. What development has led to an interest in intelligent agents?

9. List ways in which intelligent agents can be used.

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) GUI **b)** Multimodal interface **c)** Intelligent agent **d)** TTS **e)** The Intelligent Room	**1)** Software assistant that performs tasks such as retrieving and delivering information and automating repetitive tasks. **2)** Text to speech. **3)** Graphical user interface. **4)** A project of the Massachusetts Institute of Technology's Artificial Intelligence Lab. **5)** A system that allows a user to interact with a computer using a combination of inputs such as speech recognition, handwriting recognition, text to speech, etc.

C: *Mark the following statements as True or False:*

a) Fewer people are using computers because computer functions are becoming integrated into other electronic devices.

b) Keyboards and mice will soon not be required for using personal computers.

c) There have been no improvements in interface design since the development of the GUI.

d) Speech recognition is likely to completely replace other input devices.

e) Computer speech and vision will free the user from having to sit in front of a keyboard and screen.

f) Intelligent agents will make computers seem more like humans.

MODULE III

UNIT IX
APPLICATION SERVICE PROVIDERS

If your hard disk is packed to bursting point, the IT department is far too busy to fix your email problems, and your business can't afford to buy the tools that you'd like to develop the company website, then it's time to think about using an application service provider (ASP). Rather than installing software on each machine or server within your organisation, you rent applications from the ASP, which provides remote access to the software and manages the hardware required to run the applications.

There are a lot of advantages to this approach. The havoc caused by viruses makes the idea of outsourcing your email and office suite services an attractive option. It also gives you more flexibility – you pay for applications as and when you need them, rather than investing in a lot of costly software which you're then tied to for years. Not having to worry about upgrading to the latest version of your office suite or about battling with the complexities of managing an email system, leaves businesses with more time. Time to focus on what they do best.

However, there are some potential pitfalls. To use applications remotely requires a lot of bandwidth, which is only really available from a broadband connection or a leased line to the ASP itself. It is also important to ensure that the ASP will be able to provide a secure, reliable service which will be available whenever you need it.

Providing applications and storage space for vast numbers of users requires some powerful technology on the part of the ASP. This includes security controls and data storage as well as providing the physical links to customers. For the most part, ASPs don't own the data centres that store the information. Instead, they lease space from data storage specialists. In this way, they can be confident of meeting customers' increasing storage requirements by buying more space as it's needed.

There's a wide variety of applications available for use via ASPs. Office suite applications and email services are two of the most generic applications available through ASPs. Large, complex business applications such as enterprise resource planning tools like SAP are another popular candidate for delivery through an ASP. Other business services, such as payroll and accounting systems are also available. This is particularly beneficial to small businesses which are likely to grow quickly and don't want to deal with the problems caused by outgrowing their existing system and having to move to a high-end package. ASPs also offer a means of using specialist tools that would otherwise prove prohibitively expensive. Small businesses have the opportunity to use such tools for short periods of time as and when they need them, rather than having to buy the software as a permanent investment.

One of the major barriers for small businesses which want to make a start in e-commerce is ensuring that they have sufficient resources to cope with sudden large

increases in customers. This means not only having adequate storage for all your customers' details, but ensuring that you have the technology in place to handle stock levels, efficient delivery and large volumes of traffic. It's very rare for an e-commerce business to handle all of these elements by itself, making this one of the best-established areas of ASP use. Being able to respond rapidly to changes in the size of your customer base and the type of product that they want to order from your business, demands more flexibility than traditional software can provide.

A: *Answer the questions:*
1. How do you pay for the applications provided by an ASP?
  a) no charge
  b) charged according to use
  c) single payment
2. What two main services does an ASP provide?
3. How does an ASP ensure that they have enough storage space for the changing needs of customers?
4. What types of applications are available from ASPs?
5. Why is it useful for a small business to be able to rent specialist tools from an ASP?
6. What is one of the best established areas of ASP use?

B: *Note the advantages and disadvantages of using an ASP.*
C: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Website	**1)** Set of standard programs used in an office.
b) ASP	**2)** Facility for storing large amounts of information.
c) Virus	**3)** Capacity of a network connection.
d) Office suite	**4)** High capacity Internet connection.
e) Bandwidth	**5)** Self-replicating program.
f) Broadband	**6)** Common enterprise resource planning tool.
g) Data centre	**7)** Application service provider.
h) SAP	**8)** Collection of related webpages.

D: *Mark the following statements as True or False:*
a) Software from an ASP must be installed locally on a user's computer.
b) You need a high bandwidth connection to use an ASP service.
c) ASPs usually use their own storage space for customers.
d) Using an ASP gives you more flexibility.
e) An e-commerce business usually provides all of the required technology itself.

UNIT X
THE TRICKS TO MPEG'S SUCCESS

The most common system for the compression of video is MPEG. It works like this. The single data stream off the CD-ROM is split into video and audio components, which are then decompressed using separate algorithms. The video is processed to produce individual frames as follows. Imagine a sequence of frames

depicting a bouncing ball on a plain background. The very first is called an Intra Frame (I-frame). I-frames are compressed using only information in the picture itself just like conventional bitmap compression techniques like JPEG.

Following I-frames will be one or more predicted frames (P-frames). The difference between the P-frame and the I-frame it is based on is the only data that is stored for this P-frame. For example, in the case of a bouncing ball, the P picture is stored simply as a description of how the position of the ball has changed from the previous I-frame.

This takes up a fraction of the space that would be used if you stored the P-frame as a picture in its own right. Shape or colour changes are also stored in the P-frame. The next P-frame may also be based on this P-frame and so on. Storing differences between the frames gives the massive reduction in the amount of information needed to reproduce the sequence. Only a few P-frames are allowed before a new I-frame is introduced into the sequence as a new reference point, since a small margin of error creeps in with each P-frame.

Between I and P-frames are bi-directional frames (B-frames), based on the nearest I or P-frames both before and after them. In our bouncing ball example, in a B-frame the picture is stored as the difference between the previous I or P-frame and the B-frame and as the difference between the B-frame and the following I or P-frame. To recreate the B-frame when playing back the sequence, the MPEG algorithm uses a combination of two references. There may be a number of B-frames between I or P-frames. No other frame is ever based on a B-frame so they don't propagate errors like P-frames.

Typically, you will have two or three Bs between Is or Ps, and perhaps three to five P-frames between Is.

A: *Answer the questions:*
1. Into what two components is the data stream split?
2. What information does an Intra frame contain?
3. What is stored in the P-frames following an I-frame?
4. What is stored in a P-frame in the case of a bouncing ball?
5. What gives the massive reduction in the amount of information needed to reproduce a video sequence?
6. Why is a new I-frame used after a few P-frames?
7. What is stored in a B-frame?
8. Why do B-frames not propagate errors?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Algorithm	**1)** A common type of compression used for video data.
b) I-frame	**2)** A compressed video frame known as a predicted frame.
c) JPEG	**3)** A compressed video frame that stores changes between the frame before
d) P-frame	it and the frame after it.
e) B-frame	**4)** A formula used for decompressing components of a data stream.
f) MPEG	**5)** A type of compression used for bitmap images.
	6) A compressed video frame that contains the complete image information.

C: *Mark the following statements as True or False:*
a) JPEG is the most common compression system used for video.
b) P-frames only store the changes in the image.
c) There is always at least one P-frame between two I-frames.
d) B-frames store the complete picture information.
e) There can only be one B-frame between each I and P-frame.
f) There are typically about four P-frames between each I-frame.

UNIT XI
NETWORK COMMUNICATIONS

1. The application layer is the only part of a communications process that a user sees, and even then, the user doesn't see most of the work that the application does to prepare a message for sending over a network. The layer converts a message's data from human-readable form into bits and attaches a header identifying the sending and receiving computers.

2. The presentation layer ensures that the message is transmitted in a language that the receiving computer can interpret (often ASCII). This layer translates the language, if necessary, and then compresses and perhaps encrypts the data. It adds another header specifying the language as well as the compression and encryption schemes.

3. The session layer opens communications and has the job of keeping straight the communications among all nodes on the network. It sets boundaries (called bracketing) for the beginning and end of the message, and establishes whether the messages will be sent half-duplex, with each computer taking turns sending and receiving, or full-duplex, with both computers sending and receiving at the same time. The details of these decisions are placed into a session header.

4. The transport layer protects the data being sent. It subdivides the data into segments, creates checksum tests – mathematical sums based on the contents of data –that can be used later to determine if the data was scrambled. It can also make backup copies of the data. The transport header identifies each segment's checksum and its position in the message.

5. The network layer selects a route for the message. It forms data into packets, counts them, and adds a header containing the sequence of packets and the address of the receiving computer.

6. The data-link layer supervises the transmission. It confirms the checksum, then addresses and duplicates the packets. This layer keeps a copy of each packet until it receives confirmation from the next point along the route that the packet has arrived undamaged.

7. The physical layer encodes the packets into the medium that will carry them – such as an analogue signal, if the message is going across a telephone line – and sends the packets along that medium.

8. An intermediate node calculates and verifies the checksum for each packet. It may also reroute the message to avoid congestion on the network.

9. At the receiving node, the layered process that sent the message on its way is reversed. The physical layer reconverts the message into bits. The data-link layer recalculates the checksum, confirms arrival, and logs in the packets. The network layer recounts incoming packets for security and billing purposes. The transport layer recalculates the checksum and reassembles the message segments. The session layer holds the parts of the message until the message is complete and sends it to the next layer. The presentation layer expands and decrypts the message. The application layer converts the bits into readable characters, and directs the data to the correct application.

A: *Answer the questions:*

1) Into what units is data subdivided by the following layers?

a) transport layer

b) network layer

2) What is the purpose of a transmission checksum test?

3) How long does the data-link layer keep a copy of each packet?

4) What processes can be carried out at intermediate nodes?

5) Which network communications layer is described by each of the following statements?

a) Makes sure that the message is transmitted in a language that the receiving computer can understand

b) Protects the data being sent

c) Encodes and sends the packets

d) Supervises the transmission

e) The part of a communications process that a user sees

f) Starts communications and looks after communications among network nodes

g) Chooses a route for the message

h) Makes backup copies of the data if required

i) Confirms the checksum, then addresses and duplicates the packets

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Bracketing	**1.** Transmission mode in which each computer takes turns sending and receiving.
b) Half-duplex	**2.** Mathematical calculations based on the contents of data.
c) Full-duplex	**3.** Set boundaries for the beginning and end of a message.
d) Checksum	**4.** Transmission mode in which both computers send and receive at the same time.

C: *Mark the following statements as True or False:*

a) Most of the work that an application does to prepare a message for sending over a network is not seen by the user.

b) ASCII is always used to transmit data.

c) The encryption layer compresses the message.

d) The network layer keeps track of how many packets are in each message.

e) The network layer keeps a copy of each packet until it arrives at the next node undamaged.

f) Analogue signals are used on ordinary telephone lines.

g) When a message arrives at its destination, it passes through the same seven network communications layers as when it was sent, but in reverse order.

UNIT XII
CHOOSING A FREE ISP

Read these hints on choosing a free ISP. Then decide which of the options available offer the best deal to these users. Be prepared to defend your choice:

1) a household with a young family;
2) a small home-based business;
3) someone who enjoys online gaming;
4) someone who doesn't want a lot of spam in their email.

Using a free ISP requires no new technology – all you need is a computer, a modem, a telephone line, and the appropriate software (which is available free of charge when you sign up with the service). Once installed on your PC you can access the Internet as normal, but your connection costs only the price of a local call, and you pay nothing else – not even for features such as an unlimited number of email addresses, unlimited Web space and original content.

Most of the services are very similar, but it is still worth looking around for a service that offers at least the following features:

CD-ROM or Online sign up

Many free ISPs require you to sign up for their service online (which obviously means you already need to have an Internet connection and some experience with setting up a dial-up networking connection). If you are a complete beginner, you'll need a free ISP which can provide its sign-up software on CD-ROM that will automatically configure your computer to access the Internet.

Local rate calls

Although using the ISP is free, you still have to pay for your online time. Nearly all ISPs however provide local call access numbers. Any free ISP that uses a national rate number or charges an initial setup or administration fee should be avoided.

Email

Having several email accounts is very useful – you can separate business and personal email for example, or provide an address for each member of your family. Many free ISPs also offer only Web-based mail which is great if you need to get into your computer on the move as you can access it from any computer with Internet access. POP3 email however is faster and more efficient and can be downloaded to your PC to read offline – a combination of the two is ideal.

Free Web space

A decent amount of free Web space would be around 25-50Mb. This would be sufficient for most of your own personal website developments. Also check to see if there are any restrictions on your use of Web space, since some free ISPs will not let you use the space for commercial purposes.

Newsgroups

Newsgroups are huge discussion forums on the Internet that are an amazingly rich resource of information and a brilliant way to communicate with other Internet users. Unfortunately they are also the home to some of the most unsavoury content on the Internet (they are largely unmoderated) and as a result many free ISPs restrict access to some or all newsgroups.

Customer Support

Check support line charges; many free ISPs use their support lines as a source of revenue relying on your ignorance to make money from the call.

The target audience is generally Net novices and, as a result, support lines are pretty much jammed all day with queries and connection problems.

Most use premium rate telephone line charges. However, there are a few free ISPs who only charge local or national rates for their telephone helplines.

Reliable Service

Of course all the features in the world won't make a scrap of difference if the ISP is unreliable and you find it impossible to log on. Look out for recommendations from friends and shop around. Interestingly many of the more popular services have become saturated and seem to be in a constant 'upgrading the network' phase.

There is nothing to stop you having more than one free ISP account. Windows will even enable you to run a number of different free ISP connection setups on the same PC so you can easily have multiple accounts and just use the best one on the day.

Option A	Option B	Option C
Bigwig ▪ 7 POP3 email accounts each with up to 1,000 aliases ▪ Scans all emails for viruses before they reach you ▪ 15Mb free Web space ▪ Access to 25,000 newsgroups ▪ Technical support at 50p/minute ▪ Comprehensive online information and easy-to-follow help available	**Arsenal** ▪ 5 POP3 email accounts ▪ Access to most newsgroups ▪ 5Mb free Web space ▪ Technical support at 50p/minute	**ConnectFree** ▪ 5 POP3 email addresses each password-protected ▪ Full access to newsgroup ▪ Unlimited Web space ▪ Free online webpage design service ▪ Free access to online multiplayer games

Option D	Option E
Bun ▪ Unlimited email addresses ▪ 25Mb Web space ▪ Online help section ▪ Free access to CyberPatrol for blocking or restricting access to inappropriate content on the Web	**Free4all** ▪ Unlimited POP3 email accounts ▪ Email virus protection and junk email filters ▪ 25Mb of free Web space with option to increase at £1 per Mb per month ▪ Powerful enough to create quite advanced, functional sites ▪ Technical support at local call rates

HOW TCP/IP LINKS DISSIMILAR MACHINES

At the heart of the Internet Protocol (IP) portion of TCP/IP is a concept called the Internet address. This 32-bit coding system assigns a number to every node on the network. There are various types of addresses designed for networks of different sizes, but you can write every address with a series of numbers that identify the major network and the sub-networks to which a node is attached. Besides identifying a node, the address provides a path that gateways can use to route information from one machine to another.

Although data-delivery systems like Ethernet or X.25 bring their packets to any machine electrically attached to the cable, the IP modules must know each other's Internet addresses if they are to communicate. A machine acting as a gateway connecting different TCP/IP networks will have a different Internet address on each network. Internal look-up tables and software based on another standard – called Resolution Protocol – are used to route the data through a gateway between networks.

Another piece of software works with the IP-layer programs to move information to the right application on the receiving system. This software follows a standard called the User Datagram Protocol (UDP). You can think of the UDP software as creating a data address in the TCP/IP message that states exactly what application the data block is supposed to contact at the address the IP software has described. The UDP software provides the final routing for the data within the receiving system.

The Transmission Control Protocol (TCP) part of TCP/IP comes into operation once the packet is delivered to the correct Internet address and application port. Software packages that follow the TCP standard run on each machine, establish a connection to each other, and manage the communication exchanges. A data-delivery system like Ethernet doesn't promise to deliver a packet successfully. Neither IP nor UDP knows anything about recovering packets that aren't successfully delivered, but TCP structures and buffers the data flow, looks for responses and takes action to replace missing data blocks. This concept of data management is called reliable stream service.

After TCP brings the data packet into a computer, other high-level programs handle it. Some are enshrined in official US government standards, like the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). If you use these standard protocols on different kinds of computers, you will at least have ways of easily transferring files and other kinds of data.

Conceptually, software that supports the TCP protocol stands alone. It can work with data received through a serial port, over a packet-switched network, or from a network system like Ethernet. TCP software doesn't need to use IP or UDP, it doesn't even have to know they exist. But in practice TCP is an integral part of the TCP/IP picture, and it is most frequently used with those two protocols.

A: *Answer the questions:*
1. What purpose does the Internet address have apart from identifying a node?
2. What data-delivery systems are mentioned in the text?

3. What do IP modules need to know about each other to communicate?

4. How many Internet addresses does a gateway have?

5. What does UDP software do?

6. When does the TCP part of TCP/IP come into operation?

7. What processes are performed by TCP software to provide reliable stream service?

8. What standard protocols are mentioned which are used to deal with the data after TCP brings it into the computer?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Internet address **b)** Resolution Protocol **c)** Look-up table **d)** Gateway **e)** User Datagram Protocol **f)** Transmission Control Protocol	**1.** Standard used for software that routes data through a gateway. **2.** Standard used by software that moves information to the correct application on the receiving system of a network. **3.** Standard used by software that manages communication exchanges between computers on the Internet. **4.** A 32-bit number identifying a node on an IP network. **5.** Stored information used to route data through a gateway. **6.** A device for connecting dissimilar networks.

C: *Mark the following statements as True or False:*

a) Internet addresses are an integral part of the IP protocol.

b) Internet addresses can be written as a series of numbers.

c) UDP software provides the final routing for data within the receiving system.

d) UDP recovers packets that aren't successfully delivered.

e) TCP only works with packet-switched networks.

f) TCP only works when it is combined with IP.

MODULE IV

UNIT XIII
SEARCH ENGINES

Study these tips for conducting searches using AltaVista. Then decide what you would type into the search box to find this data. Compare your answers with others in your group and together decide what would be the best search. Restrict sites to English language.

Tip 1.

Don't use simple keywords. Typing in the word football is unlikely to help you to find information on your favourite football team. Unless special operators are included, AltaVista assumes the default operator is OR. If, for example, the search query is *American football*, AltaVista will look for documents containing either *American* or *football* although it will list higher those documents which contain both.

Tip 2.

AltaVista is specifically case sensitive. If you specify apple as your search term, AltaVista will return matches for apple, Apple and APPLE. However, if you use Apple or apPle, AltaVista will only match Apple and apPle respectively.

Tip 3.

AltaVista supports natural language queries. If you really aren't sure where to start looking, try typing a natural language query in the search box. The question Where can I find pages about digital cameras? will find a number of answers but at least it will give you some idea of where to start.

Tip 4.

Try using phrase searching. This is where you place quotation marks around your search term, e.g. *'alternative medicine'*. This will search for all documents where these two words appear as a phrase.

Tip 5.

Attaching a + to a word is a way of narrowing your search. It means that word must be included in your search. For example, if you were looking for information on cancer research, use +cancer+research instead of just cancer.

Tip 6.

Attaching a – to a word or using NOT is another way of narrowing your search. This excludes the search item following the word NOT or the – sign. For example, science NOT fiction or science – fiction will exclude sites in which these two words occur together.

Tip 7.

Use brackets to group complex searches, for example: (cakes AND recipes) AND (chocolate OR ginger) will find pages including cakes and recipes and either chocolate or ginger or both.

Tip 8.

You can refine your search by doing a field search. Put the field, then a colon and then what you are looking for.

For example,

URL: UK + universities will find only British universities.

title: 'English language' will find only sites which contain this phrase in their titles.

Tip 9.

AltaVista supports the use of wildcard searches. If you insert a * to the right of a partial word, say hydro*, it will find matches for all words beginning with hydro such as hydrocarbon and hydrofoil. Wildcards can also be used to search for pages containing plurals of the search terms as well as to catch possible spelling variations, for example alumin*m will catch both aluminium (UK) and aluminum (US).

Tip 10.

If you are looking for multimedia files then save yourself time by selecting images, audio or video with the radio buttons on AltaVista's search box and then entering your search:

1) a street map of Edinburgh, Scotland;
2) train times between London and Paris;
3) the exchange rate of your currency against the US dollar;
4) a recipe for chocolate chip or hazelnut brownies;
5) video clips of the Beatles;
6) sumo wrestler competitions in Japan this year;

7) the weather in New York city tomorrow;
8) heart disease amongst women;
9) New Zealand universities which offer courses in computing;
10) Sir Isaac Newton's laws of motion.

EMAIL PROTOCOLS

Although the format of a mail message, as transmitted from one machine to another, is rigidly defined, different mail protocols transfer and store messages in slightly different ways. The mail system you're probably used to employs a combination of SMTP and P0P3 to send and receive mail respectively. Others may use IMAP4 to retrieve mail, especially where bandwidth is limited or expensive.

Simple Mail Transfer Protocol

SMTP is used to transfer messages between one mail server and another. It's also used by email programs on PCs to send mail to the server. SMTP is very straightforward, providing only facilities to deliver messages to one or more recipients in batch mode. Once a message has been delivered, it can't be recalled or cancelled, it's also deleted from the sending server once it's been delivered. SMTP uses 'push' operation, meaning that the connection is initiated by the sending server rather than the receiver. This makes it unsuitable for delivering messages to desktop PCs, which aren't guaranteed to be switched on at all times.

In host-based mail systems, such as Unix and Web mail, SMTP is the only protocol the server uses. Received messages are stored locally and retrieved from the local file system by the mail program. In the case of Web mail, the message is then translated into HTML and transmitted to your browser. SMTP is the only protocol for transferring messages between servers. How they're then stored varies from system to system.

Post Office Protocol

POP is a message-retrieval protocol used by many PC mail clients to get messages from a server, typically your ISP's mail server. It only allows you to download all messages in your mailbox at once. It works in 'pull' mode, the receiving PC initiating the connection. PC-based POP3 mail clients can do this automatically at a preset interval. When you use your Web mail account to access a P0P3 maiIbox, the mail server opens a connection to the POP3 server just as a PC-based application would. The messages are then copied into your Web mailbox and read via a browser.

Since P0P3 downloads all the messages in your mailbox, there's an option to leave messages on тгe server, so that they can be picked up from different machines without losing any. This does mean that you'll get every message downloaded every time you connect to the server. If you don't clean out your mailbox regularly, this could mean long downloads. When using a Web mail account to retrieve P0P3 mail, be careful about leaving messages on the server – if too many build up, each download will take a long time and fill up your Inbox. Many Web mail systems won't recognise messages you've already downloaded, so you'll get duplicates of ones you haven't deleted.

Internet Mail Access Protocol

IMAP is similar in operation to POP, but allows you more choice over what messages you download. Initially, only message headers are retrieved, giving information about the sender and subject. You can then download just those messages you want to read. You can also delete individual messages from the server, and some IMAP4 servers let you organise your mail into folders. This makes download times shorter and there's no danger of losing messages.

A: *Answer the questions:*
1. Name three different email protocols mentioned in the text.
2. Which email protocol is used to transfer messages between server computers?
3. Why is SMTP unsuitable for delivering messages to desktop PCs?
4. Name two host-based mail systems mentioned in the text.
5. Where are email messages stored in an SMTP system?
6. What happens when you use your Web mail account to access a P0P3 mailbox?
7. Give an advantage and a disadvantage of having an option to leave POP3 messages on the server.
8. What are the advantages of using the IMAP4 protocol?

B: *Mark the following statements as True or False:*
a) Different mail systems transfer emails in different ways.
b) IMAP4 requires more bandwidth than the other email protocols.
c) SMTP is used for sending emails from a PC to a server.
d) SMTP delivers messages one at a time.
e) SMTP does not allow a delivered message to be cancelled.
f) SMTP is only one of many protocols used to send mail between servers.
g) POP protocol allows the user to download one message at a time.

C: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) SMTP **b)** 'Push' operation **c)** POP **d)** 'Pull' operation **e)** IMAP	**1.** An email transfer process in which the connection is initiated by the sending computer rather than the receiving computer. **2.** A mail transfer protocol that initially only retrieves the message headers. **3.** An email transfer process in which the receiving computer initiates the connection. **4.** A simple mail transfer protocol that is used to send messages between servers. **5.** A message-retrieval protocol that downloads all email messages at the same time.

UNIT XIV
XML TAKES ON HTML

Standard Generalized Markup Language (SGML) is the language that spawned both HTML (HyperText Markup Language) and XML (extensible Markup Language). SGML is not a true language, it is a metalanguage, which is a language

from which you can create other languages. In this case, it is the creation of a markup language (a system of encoded instructions for structuring and formatting electronic document elements).

HTML is an application-specific derivation of SGML. It is a set of codes, generally used for webpages, that creates electronic documents according to rules established by SGML. HTML is a language that is all about the presentation of your information, not what the actual data is. You can, therefore, say that HTML is a presentation language.

XML is a subset of SGML, but it is also, like SGML, a metalanguage. XML defines a specific method for creating text formats for data so that files are program independent, platform independent, and support internationalisation {able to read different languages, etc.) In fact, because XML is an extensible language, you don't even have to have a browser to interpret the page. Applications can parse the XML document and read the information without any human intervention.

XML, unlike HTML, is concerned with the identity, meaning and structure of data. XML is extensible because it lets website developers create their own set of customised tags for documents. This ability to define your own tags is the main feature of XML and it is what gives developers more flexibility.

By defining your own markup tags, you can explicitly define the content in the document. This makes XML a more intelligent markup language than HTML. For example, in HTML, you could have a paragraph tag <p> preceding a paragraph about baseball. Your Web browser sees this tag and knows to present the following text as a paragraph-All your browser knows about the text, however, is that it is text; it doesn't know that it is specifically about baseball. In an XML document, you could define a <BASEBALL> tag to refer specifically to the text in the paragraph in your document. This way, when your XML browser examines the document, the document knows what data it contains, and that makes the content more intelligent. Search engines that make use of XML data can do a better job of finding the pages you are looking for because of the intelligent nature of XML content.

XML, by design, does not deal with how the data is displayed to the end user. Because HTML is a presentation language, XML documents use HTML tags to help handle the visual formatting of the document. Also, you can use XML in your HTML documents to provide metadata, which is data about data in the document.

XML will do to the Web and e-commerce what HTML originally did to the Internet, XML and its associated applications have the potential to blow the roof off the Internet and how we do business.

A: *Answer the questions:*
1. What languages were derived from SGML?
2. What type of language is used to structure and format elements of a document?
3. Name two metalanguages.
4. What elements of data is XML (but not HTML) concerned with?
5. What is meant by the term 'extensible'?
6. What makes XML a more intelligent language than HTML?

7. What does the HTML markup tag <p> indicate?

8. Why are search engines able to do a better job with XML documents?

9. What type of website is particularly likely to benefit from XML?

B: *Mark the following statements as True or False:*

a) HTML is no longer useful for creating webpages.

b) SGML is more complex than XML.

c) XML files can only be used on Unix systems.

d) XML files can only be read by browser programs.

e) HTML is a markup language.

f) Internet searches will be better with XML files.

C: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Metadata	**1.** Extensible markup language.
b) Metalanguage	**2.** A coding system used for structuring and formatting documents.
c) HTML	**3.** Data about data.
d) XML	**4.** An example of a page presentation language.
e) Markup language	**5.** A language from which you can create other languages.

UNIT XV
BROADBAND COMMUNICATIONS
Integrated Services Digital Network (ISDN)

ISDN services can be carried over existing telephone network infrastructure to terminal adapters (TAs) in the client machine. A common ISDN interface standard has a digital communications line consisting of three independent channels: two Bearer (B) channels, each at 64Kbit/s, and one Data (D) channel at 16Kbit/s. The D channel is used to carry signalling and supervisory information to the network, while the B channels carry the data and can be linked to provide a 128Kbit/s data channel.

Wireless connections

The wireless alternatives come in two forms: satellite and cellular. Satellite systems require the use of a modem to maintain the upload. Downstream bandwidth is provided via a dedicated satellite dish, connector hardware and proprietary software.

Cellular systems use assigned radio frequencies and are based around a network of transmitters that are arranged in a cellular network, much like cellular mobile phone systems.

The cable alternative

Cable companies can also offer affordable broadband services over copper coaxial or fibre infrastructure networks. The connection is shared by several customers on a branch, so actual connection rates are variable, unlike ISDN and DSL.

Digital Subscriber Line (DSL)

DSL technology capitalises on the existing network of copper infrastructure, but allows digital signals to be carried rather than analogue. It allows the full bandwidth of the copper twisted-pair telephone cabling to be utilised.

With splitter-based services, the DSL signal is pulled out from the phone line as it enters your premises and is wired separately to a DSL modem. This involves additional hardware and installation by the service provider at the customer site. The shielded option involves no installation, but the telephone company's equipment and some of your equipment might need upgrading.

With Asymmetric Digital Subscriber Line (ADSL), most of the duplex bandwidth is devoted to the downstream direction, with only a small proportion of bandwidth being available for upstream. Much Internet traffic through the client's connection, such as Web browsing, downloads and video streaming, needs high downstream bandwidth, but user requests and responses are less significant and therefore require less on the upstream. In addition, a small proportion of the downstream bandwidth can be devoted to voice rather than data, allowing you to hold phone conversations without requiring a separate line.

DSL-based services are a very low-cost option when compared to other solutions offering similar bandwidth, so they can be made available to the customer at extremely competitive prices.

A: *Answer the questions:*
1. How many channels does an ISDN system commonly use?
2. What types of wireless systems are named in the text?
3. What do PCs connected to a satellite system use to send data?
4. What types of cables are used in cable network systems?
5. What may need to be upgraded when using a shielded DSL system?
6. Compared to the downstream bandwidth, the upstream bandwidth in an ADSL line is:
   a) larger
   b) smaller
   c) the same
7. Which type of broadband service is the cheapest?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) ISDN b) TA c) Data channel d) Bearer channel e) DSL f) Splitter-based services g) ADSL	1. DSL system that separates the digital signals from the analogue signals. 2. Digital channel used to carry ISDN signalling and supervisory information to the network. 3. Device installed on a PC to allow it to receive ISDN signals. 4. Integrated Services Digital Network. 5. Asymmetric Digital Subscriber Line. 6. Digital channel used to carry ISDN data. 7. Digital Subscriber Line.

C: *Mark the following statements as True or False:*
a) ISDN can only operate over a special digital telephone line.
b) Two ISDN channels can be combined to give the user double the bandwidth.
c) Computers connected to a satellite system do not need a modem.
d) Cellular networks work in a similar way to mobile phone systems.
e) DSL systems require a special digital telephone line.

f) DSL systems use analogue signals.

g) You need a separate line to hold normal phone conversations on an ADSL system.

UNIT XVI
READING HARD DRIVES

Server manufacturers connect hard drives to ensure that data is adequately protected and can be quickly accessed. Computer engineers call such an arrangement a redundant array of inexpensive disks (RAID). By arranging drives in sets, users hope to take advantage of the higher seek times of smaller drives. A special hard disk controller, called a RAID controller, ensures that the RAID array's individual drives are seen by the computer as one large disk drive.

RAID schemes are numbered, with higher numbers indicating more elaborate methods for ensuring data integrity and fault tolerance (or a computer's ability to recover from hardware errors).

	Raid 0	**Raid 1**	**Raid 2-4**	**Raid 5**
Fault tolerance?	No	Yes	Yes	Yes
What does it do?	Called disk striping, RAID 0 breaks data into blocks that are spread across all drives rather than filling one before writing to the next.	Called disk mirroring, RAID 1 uses two identical drives: data written to the first is duplicated on the second.	RAID 2-4 are rarely used and simply enhance the striping provided by other RAID levels.	Called striping with parity, the popular RAID 5 writes error-correcting, or parity, data across available drives.
What are the advantages?	Improved disk I/O throughput – the fastest of all RAID configurations as it distributes read/write operations across multiple drives. Good for imaging and scientific work where speed is important.	If either drive fails, the other continues to provide uninterrupted access to data.	2 enhances 0 by using additional drives to store parity data. 3 enhances 2 by requiring only one error-checking drive. 4 builds on 3 by using larger block sizes, boosting performance.	If one drive fails, its contents are recovered by analysing the data on the remaining disks and comparing it with the parity data.
What are the disadvantages?	The failure of any single drive means the entire array is lost.	Inefficient use of disk space.	Uses dedicated disks to store the parity data used to reconstruct drive contents. Up to 30% more hard disk space needed than 1.	Not as fast as RAID 0.

A: *Answer the questions:*
1. Give two reasons why server computers often have connected hard drives.
2. Why is RAID 0 particularly suited to imaging and scientific work?
3. What is the advantage of using drive mirroring?
4. To store data, RAID levels higher than 1 require:
   a) At least double the disk space
   b) Up to about a third more disk space
   c) Less than half the disk space
5. Where is the backup data stored in a RAID 5 system?
6. Which levels of RAID can reconstruct data lost in failed drives from the backup data spread across the remaining drives in the array?
7. Which level of RAID is the fastest?

B: Match the terms in Table A with the statements in Table B:

Table A	Table B
a) RAID b) RAID controller c) An array d) Striping e) Mirroring f) Check data	1. Information which is used to restore data if one of the RAID drives fail. 2. A process of spreading data across a set of disks. 3. Redundant array of inexpensive disks. 4. A set. 5. A device for controlling a set of hard disks. 6. The technique of writing the same information to more than one drive.

C. *Mark the following statements as True or False:*
a) Small disks tend to have lower seek times than large disks.
b) RAID controllers make one large hard disk act like a set of small disks.
c) In RAID systems, one disk is filled with data before the next disk is used.
d) A higher numbered RAID array uses a more elaborate system to protect the integrity of data.
e) RAIDO provides good data recovery.
f) Small file servers do not usually use RAID level 3.

MODULE V

UNIT XVII
SAFE DATA TRANSFER

Secure transactions across the Internet have three goals. First, the two parties engaging in a transaction (say, an email or a business purchase) don't want a third party to be able to read their transmission. Some form of data encryption is necessary to prevent this. Second, the receiver of the message should be able to detect whether someone has tampered with it in transit. This calls for a message-integrity scheme. Finally, both parties must know that they're communicating with each other, not an impostor. This is done with user authentication.

Today's data encryption methods rely on a technique called public-key cryptography.

Everyone using a public-key system has a public key and a private key. Messages are encrypted and decrypted with these keys. A message encrypted with your public key can only be decrypted by a system that knows your private key.

For the system to work, two parties engaging in a secure transaction must know each other's public keys. Private keys, however, are closely guarded secrets known only to their owners. When I want to send you an encrypted message, I use your public key to turn my message into gibberish. I know that only you can turn the gibberish back into the original message, because only you know your private key. Public-key cryptography also works in reverse – that is, only your public key can decipher your private key's encryption.

To make a message tamper-proof (providing message integrity), the sender runs each message through a message-digest function. This function within an application produces a number called a message-authentication code (MAC). The system works because it's almost impossible for an altered message to have the same MAC as another message. Also, you can't take a MAC and turn it back into the original message.

The software being used for a given exchange produces a MAC for a message before it's encrypted. Next, it encrypts the MAC with the sender's private key. It then encrypts both the message and the encrypted MAC with the recipient's public key and sends the message.

When the recipient gets the message and decrypts it, they also get an encrypted MAC. The software takes the message and runs it through the same message-digest function that the sender used and creates its own MAC. Then it decrypts the sender's MAC. If the two are the same, then the message hasn't been tampered with.

The dynamics of the Web dictate that a user-authentication system must exist. This can be done using digital certificates.

A server authenticates itself to a client by sending an unencrypted ASCII-based digital certificate. A digital certificate contains information about the company operating the server, including the server's public key. The digital certificate is 'signed' by a trusted digital certificate issuer, which means that the issuer has investigated the company operating the server and believes it to be legitimate. If the client trusts the issuer, then it can trust the server. The issuer 'signs' the certificate by generating a MAC for it, then encrypts the MAC with the issuer's private key. If the client trusts the issuer, then it already knows the issuer's public key.

The dynamics and standards of secure transactions will change, but the three basic tenets of secure transactions will remain the same. If you understand the basics, then you're already three steps ahead of everyone else.

A: *Answer the questions:*
1. What does data encryption provide?
  a) privacy
  b) integrity
  c) authentication
2. A message encrypted with the recipient's public key can only be decrypted with

a) the sender's private key

b) the sender's public key

c) the recipient's private key

3. What system is commonly used for encryption?

4. What is the opposite of 'encrypt'?

5. A message-digest function is used to:

a) authenticate a user

b) create a MAC

c) encrypt a message

6. What information does a digital certificate give to a client?

B: *Match the functions in Table A with the keys in Table B:*

Table A	Table B
a) to encrypt a message for sending	**1.** sender's private key
b) to decrypt a received message	**2.** trusted issuer's private key
c) to encrypt the MAC of a message	**3.** the recipient's private key
d) to encrypt the MAC of a digital signature	**4.** the recipient's public key

C: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Gibberish	**1.** Message-authentication code.
b) Impostor	**2.** Principal features.
c) Deciphe	**3.** Meaningless data.
d) MAC	**4.** Person pretending to be someone else.
e) Tenets	**5.** Make unauthorised changes.
f) Tamper	**6.** Convert to meaningful data.

UNIT XVIII
BACKUP HSM AND MEDIA CHOICE

Near-line and offline storage (often called Hierarchical Storage Management) is the modern way of dealing with current storage needs. Hard disks are becoming cheaper, but data storage requirements are higher, so it's better to plan for HSM than assume disks can continually be added to systems.

HSM is essentially the automatic movement of data between media, the media type used depending on when it was last accessed. Many software and hardware vendors have HSM solutions, and all are based on the same basic techniques.

The most common HSM setup is where there's online storage (the hard disk), near-line storage (some sort of fast media from where a file can be quickly retrieved), and offline storage (slower media that might take some time for files to be recovered, but it is cheaper for a long-term storage). This arrangement is the major thrust of today's systems. Most of the time these systems will comprise optical media for near-line and tape media for offline storage.

Data is automatically moved from the online disk to the near-line optical media if it hasn't been accessed for a definable period of time. This is typically three months (depending on your business). This near-line system is likely to be erasable optical disks in some form of jukebox.

The system has to operate on the basis that a user won't know that a file has been moved into near-line storage. Therefore some marker is left in the directory structure on the disk so that the user can still see the file. If the user then tries to open it, the file will automatically be copied from near-line to online storage, and opened for the user. All the user notices is a slight time delay while the file is opened.

Moving data from near-line to offline storage can be done using a similar mechanism, but more often the marker left in the directory for the user to see will just contain a reference. This gives the user the facility to request the file back from the systems administrator, and could have information like 'This file has been archived to offline media' and a reference to the tape number that the file is on. This is then sent to the systems administrator and the file can be recovered from tape in the usual way.

Some modern systems have the ability to keep multiple tapes in a tape changer or jukebox system, so retrieval from offline to online storage can be automatic. However, it is more likely that when a file goes into offline storage it will never be recovered, as it has probably been untouched for several months (again depending on the business). Therefore the requirement to recover from offline to online is reasonably infrequent.

The choice of storage media type is a crucial aspect of HSM. The cheapest is undoubtedly tape (be it digital, analogue or digital linear), so this tends to be used for offline storage. However, tape has no guarantee of data integrity beyond one or two years, whereas optical systems, such as CDs, WORMs and MO disks, have much better data integrity over a longer period of time. Depending on the precise application, archiving systems are usually based on the media type that has the best integrity. The major suppliers within the HSM market are totally open about the media that can be used with their software. Current HSM systems support most hardware devices, so you can mix and match media to suit requirements. Given the fact that media choice depends on the length of time you want your data to remain intact, and also the speed at which you want to recover it, the choice for many system managers is as follows.

Tape is used for backup systems where large amounts of data need to be backed up on a regular basis. Tape is cheap, integrity is good over the short to medium term, and retrieval from a backup can be made acceptable with good tape storage practices.

Near-line storage should be based on erasable optical disks. This is because access is random, so the access speed to find and retrieve a particular file needs to be fast, and data integrity is also good.

Archiving systems should probably be CD- or WORM-based, as again access speeds are good, media costs are reasonably cheap and, importantly, the integrity of the media over the medium to long term is good.

One important thing to remember with archiving systems is the stored data's format. The data might be held perfectly for 10 or 15 years, but when you need to get it back, it's essential that you maintain appropriate hardware and software to enable you to read it.

A: *Answer the questions:*

1. What factor determines which type of storage is used to store a file in an HSM system?

2. Complete the following table using information from the text.

Storage Type	Media	Speed
		very fast with quickest access speed
	optical	
offline		

3. What happens to data that is not accessed for a long time?

4. How does the system record that a file is in near-line storage?

5. What happens when a user tries to access a file in near-line storage?

6. What does the reference to a file in offline storage contain?

7. To whom does the user send a request for the retrieval of a file from offline storage?

8. Name three types of magnetic tape mentioned in the text.

9. Select the correct answers in the following:

   A) How long can data be stored on tape?
   a) 6 months   b) 2 years   c) 10 years
   B) Hard disks are usually used for which type of storage?
   a) offline   b) online   c) near-line
   C) Tape is normally used for which type of storage?
   a) offline   b) near-line   c) online
   D) Files are automatically retrieved from offline storage
   a) always   b) sometimes c) never

10. What two factors determine the choice of storage media used?

11. What items must you remember to maintain while data is stored?

B: *Mark the following statements as True or False:*

a) Hard disks are still very expensive.

b) Near-line storage needs to have a quick access speed.

c) Near-line storage is usually some form of jukebox.

d) Offline storage needs to have a fast access speed.

e) Users are aware that their files have been moved to near-line storage.

f) The movement of files between near-line and online storage is automatic.

g) The user sometimes has to request files from the systems administrator.

h) Files are frequently recovered from offline storage.

I) Tape has much better data integrity than optical media.

j) It is usually possible to use whatever media you want in an HSM system.

UNIT XIX
THE EX-HACKER

Find the answers to these questions as quickly as you can.

1.   Which group hacked into Hotmail?

2.   Who was 'The Analyser' and what did he do?

3.   Which hacker was sent to jail for fraud?

4.   What was the effect of the 1996 raid on Scotland Yard?

5.   Which of the cases reported here involved teenagers?

6.   What did hackers do to the Yahoo! website?

7.   What crime was Raphael Gray accused of?

<div align="center">***</div>

Kevin Mitnick is the hackers' hero. His latest spell in jail was a 46-month sentence for fraud relating to breaking into the systems of several multinational corporations. He was released on condition that he did not have any contact with a computer.

<div align="center">***</div>

In March 2000, a Welsh teenager allegedly stole information from more than 26,000 credit card accounts across Britain, the US, Japan, Canada and Thailand, and published the details on the Internet. FBI agents and British police raided the home of Raphael Gray, 18, and arrested him and his friend. He has been charged with 10 counts of downloading unauthorised information.

<div align="center">***</div>

In 1998 Washington revealed that an Israeli hacker called 'The Analyser' was responsible for 'the most organised attempt to penetrate the Pentagon's computer systems'. He turned out to be Ehud Tenenbaum, 18, who had planted a list of his own passwords in the Pentagon system and passed them to other hackers.

<div align="center">***</div>

In 1997 the son of a fraud squad detective walked free from a court in London after charges of breaching the security of the US air force were dropped. Three years earlier Mathew Bevan, then 19, and a friend, Richard Pryce, 16, used the Internet to gain access to several US military bases. Pryce was fined £1,200 after admitting several other offences.

<div align="center">***</div>

Hotmail, Microsoft's free email service, was hacked into last September, exposing the correspondence of more than 40m users. A group calling itself Hackers Unite posted a Web address with details of how to access any Hotmail account. The service was shut down for five hours.

<div align="center">***</div>

The UK Department of Trade and Industry has twice been prey to hackers, once in 1996 and again in 2000 when a DTI computer was programmed to reroute email. The Home Office investigated nine cases of hacking last year, one of which was the leaking of a report on a murder. In August 1996 hackers ran up a £1m phone bill for Scotland Yard but did not access files.

<div align="center">***</div>

In 1997 hackers got into the Yahoo! website, replacing the homepage with a ransom note demanding the release of their hero, Kevin Mitnick. Unless the demand was met, the note said, a virus would be released in all Yahool's computers. The company dismissed the threat as a hoax, but the 'Free Kevin' slogan continued to appear on other hijacked sites.

UNIT XX
OBJECT-ORIENTED PROGRAMMING

One of the principal motivations for using OOP is to handle multimedia applications in which such diverse data types as sound and video can be packaged

together into executable modules. Another is writing program code that's more intuitive and reusable; in other words, code that shortens program-development time.

Perhaps the key feature of OOP is encapsulation – bundling data and program instructions into modules called 'objects'. Here's an example of how objects work. An icon on a display screen might be called 'Triangles'. When the user selects the Triangles icon – which is an object composed of the properties of triangles (see fig. below) and other data and instructions – a menu might appear on the screen offering several choices. The choices may be (1) create a new triangle and (2) fetch a triangle already in storage. The menu, too, is an object, as are the choices on it. Each time a user selects an object, instructions inside the object are executed with whatever properties or data the object holds, to get to the next step. For instance, when the user wants to create a triangle, the application might execute a set of instructions that displays several types of triangles – right, equilateral, isosceles, and so on.

Many industry observers feel that the encapsulation feature of OOP is the natural tool for complex applications in which speech and moving images are integrated with text and graphics. With moving images and voice built into the objects themselves, program developers avoid the sticky problem of deciding how each separate type of data is to be integrated and synchronized into a working whole.

A second key feature of OOP is inheritance. This allows OOP developers to define one class of objects, say 'Rectangles', and a specific instance of this class, say 'Squares' (a rectangle with equal sides). Thus, all properties of rectangles – 'Has 4 sides' and 'Contains 4 right angles' are the two shown here – are automatically inherited by Squares. Inheritance is a useful property in rapidly processing business data. For instance, consider a business that has a class called

'Employees at the Dearborn Plant' and a specific instance of this class, 'Welders'. If employees at the Dearborn plant are eligible for a specific benefits package, welders automatically qualify for the package. If a welder named John Smith is later relocated from Dearborn to Birmingham, Alabama, where a different benefits package is available, revision is simple. An icon representing John Smith – such as John Smith's face – can be selected on the screen and dragged with a mouse to an icon representing the Birmingham plant. He then automatically 'inherits' the Birmingham benefit package.

A third principle behind OOP is polymorphism.

This means that different objects can receive the same instructions but deal with them in different ways. For instance, consider again the triangles example. If the user right clicks the mouse on 'Right triangle', a voice clip might explain the properties of right triangles. However, if the mouse is right clicked on 'Equilateral triangle' the voice instead explains properties of equilateral triangles.

The combination of encapsulation, inheritance and polymorphism leads to code reusability. 'Reusable code' means that new programs can easily be copied and pasted together from old programs. All one has to do is access a library of objects and stitch them into a working whole. This eliminates the need to write code from scratch and then debug it. Code reusability makes both program development and program maintenance faster.

A: *Answer the questions:*

1. What advantages of using object-oriented programming are mentioned in the text?

2. What are the three key features of OOP?

3. What multimedia data types are referred to in the text?

4. List the different types of triangle mentioned in the text.

5. What feature avoids the problem of deciding how each separate type of data is integrated and synchronized into a working whole?

6. What specific type of rectangle is named in the text?

7. What common properties of a rectangle are mentioned in the text?

8. What features are made quicker by code reusability?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) OOP	**1**. An OOP property that allows data and program instructions to be bundled into an object.
b) Encapsulation	
c) Object	**2.** A list of choices.
d) Menu	**3.** An OOP property that enables different objects to deal with the same instruction in different ways.
e) Square	
f) Polymorphism	**4.** A reusable collection of objects.
g) Library	**5.** A module containing data and program instructions.
	6. Object-Oriented Programming.
	7. A rectangle with equal sides.

C: *Complete the following text using words from the reading text:*

Encapsulation, ____ and polymorphism are key features of ____ programming. Encapsulation allows data and program instructions to be bundled together in ____ called objects. Inheritance means that specific ____ of a class of objects ____ the properties of the class of objects. Polymorphism means that instructions are treated differently by different ____. The combination of these ____ features of OOP means that program code is reusable. This speeds up ____ and ____ of programs.

MODULE VI

UNIT XXI
BECOMING CERTIFIED

Suppose you're a support engineer. You're stuck in a job you don't like and you want to make a change. One way of making that change is to improve your marketability to potential employers by upgrading your skill-set. If you're going to train yourself up however, whose training should you undertake? If you need certificates, whose certificates should they be? Even if you get those certificates, how certain can you be that your salary will rise as a result? One solution is the range of certifications on offer from Microsoft.

Microsoft offers a large array of certification programmes aimed at anyone from the user of a single program such as Microsoft Word, to someone who wants to become a certified support engineer. There are a myriad of certificates to study for

too. If you're the proud holder of any of those qualifications, then you're entitled to call yourself a Microsoft Certified Professional (MCP).

Once you've decided which track you want to take, you should consider just how qualified you already are in terms of experience and knowledge. Will you need to go and take some courses with a training company, or are you the type who can make good use of self-study materials? How much time do you genuinely have to devote towards this? Will your employer pay for your course? Will it grant you leave to go and do the course – assuming you can find one – on either a full-time or part-time basis?

The key question here is experience. This will not only influence the amount of work you'll have to do to get up to speed for the exams, it could also mean the difference between passing or failing the exam.

While you're busy learning all you need to know for your certification, the practice exams are an absolute godsend. They show you the type of questions you'll encounter, and they familiarize you with the structure of the exam. This is essential if you want to pass: the exams have time limits, and you need to get used to answering the requisite number of questions within the allotted time. It's as simple as that.

If you decide a training course will help you out, don't let the title of a course alone convince you that it will be suitable or cost effective. Find out exactly what the course offers and whether there are pre-requisites for attendants. You should also find out what the training company is prepared to do if attendants don't have the minimum knowledge necessary to be on the course.

As exams are replaced by 'updated' ones, you need to upgrade your certification to stay current. Ultimately it's your responsibility to make sure you stay up to date. If you don't, you lose your certification until you take an update.

As a support engineer, you get the satisfaction of knowing that you passed a tough test, and the happy knowledge that your network manager is sweating a bit over the fact that you could be head-hunted at any time.

QUALIFICATIONS

• Microsoft Certified Systems Engineer (MCSE)

MCSEs design, install, support and troubleshoot information systems. MCSEs are network gurus, support technicians and operating system experts.

• Microsoft Certified Solution Developer (MCSD)

MCSDs use development tools and platforms to create business solutions.

• Microsoft Certified Product Specialist (MCPS)

MCPSes know all about at least one Microsoft operating system. Some also specialise in other Microsoft products, development tools or desktop applications.

• Microsoft Certified Trainer (MCT)

MCTs teach others about Microsoft products using the Microsoft Official Curriculum at Microsoft Authorised Technical Education Centres.

A: *Answer the questions:*
1. What advice is given for someone who is stuck in a computing support job?

2. What questions should you ask yourself if you are thinking of getting extra training?

3. What computer program is mentioned in the text?

4. Name two ways of studying that are mentioned in the text.

5. What two factors will be affected by your level of experience?

6. Why is it important to become used to answering exam questions?

7. What factors help you decide whether the course will be suitable or cost effective?

8. What happens if you don't upgrade your certification?

B: *Which qualification would be most useful if you wanted to do each of the following:*

a) be an operating system expert

b) troubleshoot systems

c) teach computing

d) design business solutions

C: *Mark the following statements as True or False:*

a) Microsoft offers a large range of certification programmes to study.

b) You must get an advanced certificate before you can call yourself a Microsoft Certified Professional.

c) All Microsoft training courses involve a period of full-time study.

d) Practice exams allow you to become familiar with the structure of the exams.

e) You can decide on the suitability of a course by its title.

f) It is your responsibility to make sure that your certification is kept up to date.

g) Gaining a certificate is likely to make you more attractive to other employers.

UNIT XXII
BLUETOOTH

As portable computing devices get smarter and more capable, connectivity frustrations increase.

This is where Bluetooth comes in. The brainchild of Ericsson, IBM, Intel, Nokia and Toshiba, Bluetooth is a microwave high-speed wireless link system that's designed to work with portable equipment. To that end, it's low power, very small and very low cost. It uses the same frequencies as existing radio LANs (and, incidentally, microwave ovens) to create a secure 1 Mbit/s link between devices within 10m of each other. These devices can be laptops, PDAs, cellphones, wired telephone access points, even wristwatch devices, headphones, digital cameras and so on. With them, your notebook PC will be able to access your cellular phone — and thus the Internet without your having to take the phone out of your pocket. Files can be exchanged and communications set up for voice and data between just about any device capable of handling the information.

Bluetooth operates in the unlicensed SM (Industrial, Scientific and Medical) band at 2.45GHz, which is globally available for products. There's 89MHz of bandwidth allocated here, and since Bluetooth is very low power, it actually radiates

less than most national and international standards allow non-transmitting devices to leak as part of their normal operation. This is key, as it allows the technology to operate without restriction on aircraft.

As befits their status as radio frequency experts, Ericsson and Nokia developed the RF side of Bluetooth. The link works in a similar way to the IEEE 802.11 wireless networking system, with a packet-switching protocol based on fast-frequency hopping direct sequence spread spectrum. In other words, it constantly switches channel to avoid interference. It changes frequency 1,600 times a second through 79 frequency bands. It's expected that this will be so good at avoiding conflicting signals from other sources that the transmission power can be kept very low.

Security is taken care of through the frequency hopping and 40-bit encryption. As the system uses radio, it can work through some barriers – briefcases, shirt pockets and desktops, for example — but it won't carry through office buildings. The power level of the transmitter can be varied, with feedback from the remote side of the link used to set the output to the lowest level commensurate with error free operation. This saves power and increases the usable density of devices. The device can operate at up to 1mW (an optional power amplifier can increase this to 100mW) and the whole lot consumes between 8mA and 30mA at 2.7V. Various power-saving modes can be used when a device isn't transmitting, trading off speed of response for battery life. These work with current levels between 300pA and 60pA.

Within the 10m radius of a unit, up to 10 independent full-speed piconets can operate, with bandwidth reduced proportionately if more than this is in use. Each can handle up to eight devices, and can be further subdivided into separate services: 432Kbit/s full-duplex data, 721/56Kbit/s asymmetric duplex, or 384Kbit/s third-generation GSM. Each channel can also support three 64Kbit/s full-duplex voice channels. An optional variation in modulation technique would double the basic data rate to 2Mbit/s.

Power consumption and cost were very significant factors in Bluetooth's design, and it was decided not to make the system a fully-fledged LAN. As a result, there's no collision detection. All devices on a piconet are synchronized to a master device and are controlled by it to prevent simultaneous operation on the same frequency. Any device can be a master, and is elected dynamically when the link starts up.

The standard is open and royalty-free to members of the Bluetooth special interest group.

A: *Answer the questions:*
1. What frustrating problem does Bluetooth solve?
2. Who first developed Bluetooth?
3. In what ways is Bluetooth particularly suited to portable systems?
4. What do Bluetooth devices share with microwave ovens?
5. List some devices that are suitable for use with Bluetooth.
6. Why is Bluetooth suitable for use on aeroplanes?
7. What factors provide security for Bluetooth communications?
8. How is the output power level of the transmitter set?

9. Why is there no collision detection in the Bluetooth specification?

10. Why are all devices on a piconet synchronised and controlled by a master device?

11. What are the consequences of Bluetooth having the following characteristics?

a) It is good at avoiding conflicting signals from other sources.

b) The transmitter output level is kept as low as possible.

c) It uses power-saving modes when devices aren't transmitting.

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) Bluetooth	**1.** Radio frequency.
b) SM band	**2.** The number of devices that can be used in the same area.
c) RF	**3.** A microwave high-speed wireless link system designed to work with
d) IEEE 802.11	portable equipment.
e) Frequency hopping	**4.** Very low power network links between Bluetooth devices.
f) Usable density	**5.** An unlicensed frequency range at 2.45GHz.
g) piconet	**6.** A standard for networking systems with a packet-switching protocol.
	7. Constantly switching channels.

C: *Mark the following as True or False:*

a) Bluetooth is an expensive system.

b) Bluetooth devices can communicate at a distance of up to 20m.

c) The SM band is available throughout the world.

d) Bluetooth has a very low radiation level.

e) Each Bluetooth connection operates at one fixed frequency.

f) Bluetooth signals will pass through walls of buildings.

g) The master Bluetooth device is determined when a link is first established.

UNIT XXIII
THE FUTURE OF IT

Read the three opening paragraphs of the text below and answer these questions:

1. How does the author justify his claim that we are 'in the midst of convergence'?

2. What will be the difference between computers and humans after 2015?

3. What does he mean by a 'positive feedback loop' in computer development?

4. Why will knowledge of a major language be the only IT skill needed?

5. Which of the author's predictions do you accept?

The future of Information Technology

We are in the midst of convergence. At the hardware layer, computers, phones and consumer electronics are converging. At the applications layer, we see convergence of information, entertainment, communications, shopping, commerce, and education.

Computers have come from nowhere 50 years ago and are rapidly catching up in capability with the human brain. We can expect humammachine equivalence by about 2015. But after this, computers will continue to get smarter. There is a noticeable positive feedback loop in technology development, with each generation

of improved computers giving us more assistance in the design and development of the next. Ultimately, they will design their offspring with little or no human involvement. This technology development will push every field of knowledge forwards, not just computing. It will be almost as though extraterrestrials had landed in 2020 and given us all their advanced technology overnight.

But we will never get far unless we can solve the interface problem. In the near future we may have electronic pets, with video camera eyes and microphone ears, linked by radio to the family computer. With voice and language recognition we will have easy access to all that the Internet can provide. We can tell the pet what we want and it will sort it out for us. It will be impossible to be technophobic about such an interface, and the only IT skill needed will be to speak any major language.

TEXT A

Telecoms applications will soon be bundled together in much the same way as office application suites are today. A major example is the electronic marketplace, which will bring customers and suppliers together in smart databases and virtual environments, with ID verification, encryption and translation. It will then implement the billing, taxation and electronic funds transfer, while automatically producing accounts and auditing. The whole suite of services will be based on voice processing, allowing a natural voice interface to talk to the computer, all the AI to carry out the request, and voice synthesis and visualisation technology to get the answer out.

Electronic money will be very secure but much more versatile than physical alternatives. E-cash can be completely global and could be used as a de facto standard. It does not have to be linked to any national currency, so can be independent of local currency fluctuations. Its growing use on the Net will lead to its acceptance on the street and we may hold a large proportion of our total funds in this global electronic cash. People will increasingly buy direct from customised manufacturers. Shops will be places where people try on clothes, not buy them. Their exact measurements can be sent instantly to the manufacturer as soon as they have chosen an outfit. The shops may be paid by the manufacturer instead.

TEXT B

Employment patterns will change, as many jobs are automated and new jobs come into existence to serve new technologies. Some organisations will follow the virtual company model, where a small core of key employees is supported by contractors on a project by project basis, bringing together the right people regardless of where they live. The desks they will use will have multiple flat screens, voice interfaces, computer programs with human-like faces and personalities, full-screen videoconferencing and 3D sound positioning. All this will be without any communication cables since the whole system uses high capacity infrared links. The many short-term contractors may not have enough space in their homes for an office and may go instead to a new breed of local telework centre.

Of course, workers can be fully mobile, and we could see some people abandon offices completely, roaming the world and staying in touch via satellite systems. Even in trains and planes there may be infrared distribution to each seat to guarantee

high bandwidth communication. One tool they may have in a few years is effectively a communicator badge. This will give them a voice link to computers across the network, perhaps on their office desk. Using this voice link, they can access their files and email and carry out most computer-based work. Their earphones will allow voice synthesisers to read out their mail, and glasses with a projection system built into the arms and reflectors on the lenses will allow a head-up display of visual information. Perhaps by 2010, these glasses could be replaced by an active contact lens that writes pictures directly onto the retina using tiny lasers.

TEXT C

Finally and frivolously to the very long term. By around 2030, we may have the technology to directly link our brain to the ultra-smart computers that will be around then, giving us so much extra brainpower that we deserve a new name, Homo Cyberneticus. In much the same time frame, geneticists may have created the first biologically optimised humans, Homo Optimus. It would make sense to combine this expertise with information technology wizardry to make something like the Borg, Homo Hybridus, with the body of an Olympic athlete and a brain literally the size of the planet, the whole global superhighway and every machine connected to it. Over time, this new form may converge with the machine world, as more and more of his thoughts occur in cyberspace. With a complete backup on the network, Homo Hybridus would be completely immortal. Ordinary biological humans would eventually accept the transition and plain old Homo Sapiens could become voluntarily extinct, perhaps as early as 2200.

FUTURES

Talking to Professor Cochrane is probably as close as you can get to time travelling without leaving the current dimension, as his vision stretches far into the 21st century and beyond. His seemingly unshakeable conviction is that anything is possible if you really put your mind to it. In fact, BT (British Telecom) is already sitting on a host of innovations poised to blow your mind during this century.

Designed for the 21 st century, Peter Cochrane's signet ring is built around a chip that holds all the details of his passport, bank account, medical records and driving licence. According to Cochrane, it's set to revolutionise shopping. The ring is already a fully operational prototype, but it will be some time before you'll be trading your credit card in for the ultimate fashion accessory.

It's not just jewellery that's set to get smarter.

One of the biggest projects down at the Lab is looking at artificial intelligence as a way of creating software programs, networks, telephones and machines with a degree of intelligence built in. By sensing their environment, they should be able to develop new capacities as demands change. 'I have software that is breeding, which is interchanging genes and creating adaptable behaviour, This means you'll see the network come alive – it will watch what you do and it will adapt'.

It doesn't stop there, though, as BT has taken artificial intelligence one step further and created machines that are solving their own problems. 'We've created solutions that a human being could never have dreamed of. We have solutions, and

although we don't understand how they work, they do work. We're effectively increasing the speed of evolution', says Cochrane.

It's already good to talk, but with artificially intelligent phones on the way it will be even better. Cochrane is at present working on smart phones that can translate English into German, Japanese and French in real-time. 'Some of it's rocket science, but a lot of it's extremely simple. What we've built is a kernel of understanding inside a machine that extracts meaning from the sentence itself – at the moment we can do simple things such as phrase books', he says.

The system uses a non-linear approach that sends the English to the understanding kernel in the machine and then fans it out to all the other languages simultaneously.

There's no doubt that Cochrane is putting a lot of faith in intelligent machines, particularly when it comes to cutting through the deluge of information that he says is the downside of the electronic revolution. BT's solution is the development of intelligent agents that watch, learn and start communicating.

It's not all work down at the Lab, though. BT's also involved in an on-going trial that it claims will revolutionise our leisure time, in particular the way we watch TV. 'We put people on the Internet and broadcast TV at the same time, so that the people at home could actually influence what was happening on their TV sets. As a result, it became interactive and therefore more active.'

BT has its fingers in multiple pies and has made biotechnology another core focus of R&D. 'Personally, I think hospitals are very dangerous places to be. There are lots of viable alternatives. For a start, we can stop bunging up hospital wards by putting people online.' BT has already developed a pack for heart attack victims that monitors their progress and uploads information via a radio link back to the hospital.

So what will the 21st century hold for us if Peter Cochrane and his futurologists have their way? Well, by the year 2015, it's likely that we will be eclipsed by a supercomputer more powerful than the human brain. And if that's got visions of Terminator dancing in your head, don't worry – Cochrane's got it covered. 'I'd really hate one morning to find myself considered an infestation of this planet. Our inclination is to nurture life and not to destroy it. Before we let loose a bunch of artificial intelligence, we ought to be thinking through the necessity of building in a number of rules that hold your life as a human being sacrosanct'.

A: *Answer the questions:*
1. Of what is Professor Cochrane completely convinced?
2. What is stored in the professor's signet ring?
3. What will change dramatically when we start using rings like these?
4. What is the BT lab developing with artificial intelligence?
5. What effect are the professor's AI experiments having on evolution?
6. What does the professor see as the negative side of the electronic revolution?
7. What was the result of combining the Internet with TV?
8. What developments does the professor suggest in the field of biotechnology?
9. According to the professor, what will happen by the year 2015?

B: *Match the terms in Table A with the statements in Table B:*

Table A	Table B
a) BT **b)** Smart phone **c)** Intelligent agent **d)** Rocket science **e)** R&D **f)** Upload **g)** Supercomputer	**1.** A computer program that watches, learns and communicates with the user. **2.** Most powerful type of computer. **3.** Research and development. **4.** Transfer data from a client device to a server computer. **5.** A telephone that can translate English into various languages in real-time. **6.** British Telecom. **7.** Very advanced study.

C: *Mark the following statements as True or False:*

a) BT has a lot of new ideas that will astound people.

b) Jewellery that can store large amounts of personal data has started to replace credit cards.

c) BT's smart phone can only translate English into one other language at a time.

d) Intelligent agents can help users deal with an overload of information.

e) Watching TV will be a more active pastime in the future.

f) The professor thinks that humanity will be destroyed by very powerful computers in the future.

MODULE VII

UNIT XXIV
THE TRUTH ABOUT NOISE

Everybody knows what noise is: noise is an ugly, disturbing and annoying sound, and most of us agree that noise is something that should be suppressed or eliminated. Evidently, there's a lot more to be said about noise than the unsuspecting layman might think.

What Noise *Isn't*

First of all, that neighbour practising bassoon is not producing noise – not in the strict sense of the word. One of the definitions of noise is that it doesn't contain any useful information. While the neighbour's bassoon practising might be highly annoying, out of tune and off-tempo, the sound contains a lot of information in the form of pitch, phrase, direction and amplitude. If you can figure out – by analysing the sound – that it comes from somewhere (your neighbour's apartment, the street, the children's room) and if you can identify that it's a certain type of sound (a bassoon, an internal poker vibrator, a dental drill), then it is not noise – technically speaking, of course.

Then, noise is not only related to sound. Flickering or speckled images on the TV screen, due to bad fine-tuning for example, are a good example for visual noise. In fact, any random fluctuation of any measurable or perceptible entity, such as sound pitch, light brightness, voltage, temperature, colour, content of data, is defined – in a general sense – as noise.

Third, noise is not worthless. Our brains are conditioned to recognize and to process noise better than any supercomputer. Our brains actually expect to get information along with some noise. For that reason, completely noiseless information, an image for example, is often perceived as artificial. It is often convenient to add noise to digitally generated or sampled art, like music or pictures, so that the final product has a more natural texture. There are other more special, scientific and complicated uses for noise, but let us not get lost in details here.

What Noise *Is*

In a mathematical definition noise results from uncorrelated, random events. The sequence of heads and tails in an idealized coin tossing experiment is one simple example for a sequence of uncorrelated, random events. The produced sequence of heads and tails can be considered to be pure noise. Since noise does not contain any information. It is not possible to use it to make predictions or physical statements and it is not possible to figure out by analysing the previous results whether the next is going to be a head or a tail. The impossibility to use a random sequence of heads and tails, or numbers, to produce a statement, doesn't make noise useless. Noise can be used to generate random numbers, as used for example in cryptography – but this is a topic of its own.

While there is large academic interest in noise and randomness in general, there is – using that strict definition – no such thing as pure noise in the real world, with the possible exception of quantum mechanical systems. In a real experiment with coins, to stay in our picture, the outcome could be predicted if one would be able to compute the motion of the coin considering all the involved parameters (the tossing speed, the influence of the air viscosity on the turning of the coin, etc.). The resulting sequence of heads and tails – the 'noise' – is in reality pseudo-noise. In scientific conventions it is possible to hear people muttering about 'deterministic' and 'non-deterministic noise'. But let us forget about that 'pure academic noise' discussion.

Amounts and Flavours of Noise

In a more neutral, or practical definition, noise is statistical, uncorrelated fluctuations of data – if they are due to deterministic processes or not is, for the time being, irrelevant. Using that definition it is possible to analyse and to characterize noise.

Testing Noise

One of the stringent conditions that define noise is that the fluctuations must be uncorrelated. In other words, the sequence of values that make up the fluctuations must not show any patterns in order to be called noise. Sets of data can easily (with the aid of computers this is not a problem nowadays) be checked for repeating sequences or patterns via an autocorrelation analysis. The absence of repeating patterns is one of the necessary criteria for noise.

The second criterion states that fluctuations have to be statistical. In other words, the mean value has to be a constant. A sequence of non-repeating numbers increasing linearly, for example, is not noise (as someone would be able to use the sequence to make predictions). This second criterion is also easily tested. As a consequence, one random number or one measurement alone cannot be considered to be noise – noise will always be a product of a sequence of numbers or measurements.

How Much Noise is in There?

The amount of noise cannot be quantified by itself – this is similar to affirming 'strawberries taste better' (better than what?). As with the taste of strawberries, noise can only be measured in relation to something else that can be quantified, an amount of signal. For this reason noise is quantified as a proportion between signal and noise, which is a quantity called the signal-to-noise ratio (abbreviated SNR). Usually, the higher the SNR the better.

The Different Flavours of Noise

The statistical distribution of the values that make up noise – the spectrum of the noise – can be analysed. (To obtain a spectrum all one has to do is to ask the following question: 'How frequently does a certain value appear in relation to all other values?' This question is asked for every value of interest. If the results are sorted according to the frequency, you get a frequency spectrum.) The spectra can be shown to have different shapes, leading to various types of noise, and descriptions for noise, some of which will be explained in the following.

White Noise: If the frequency spectrum is flat, that is, all values occur in all frequencies, then the noise is called 'white' – in analogy to the spectrum of white light, in which all colours (frequencies) are present with the same intensity. White noise is also the 'pure academic noise', the one and only, real noise we talked about above. All other forms of noise are pseudo-noise. However, it is not possible to obtain true white noise from real life things, because there is no such thing as infinite or zero frequency. In spite of this, noise can be 'white', however, within a certain range of frequencies.

Black Noise: Like 'darkness beams', black noise doesn't exist as such. Black noise is, paradoxically, just a specific form of white noise. It is white noise with opposite signs, it is the noise that cancels out white noise, or in a sense 'anti-noise'. The term 'black noise', however, has found some usage as it can be used to suppress certain ranges of 'noise' (eg, reducing the roar in the passenger cabins of airplanes).

Pink Noise (1/f-noise): In real-life fluctuating things, the frequency of the fluctuations determines the involved energy. If something is fluctuating very rapidly, there's much energy involved, if something is fluctuating slowly, there's little energy involved. With this in mind, it is often more useful to look at a spectrum of 'energy per time', or power-spectrum, instead of the energy spectrum, or frequency spectrum itself (one punch per second hurts more than one soft touch per second – same frequency different power). In order to get a constant power-spectrum, the frequency spectrum decreases with 1/f. In analogy to white noise, this type of noise is called pink, as visible light with that frequency spectrum would be pink. This kind of noise is often found in the world of acoustic gadgets: A pink-noise generator (used to test audio systems), for example, generates random sound pitches with equal power (energy per time).

Other Colours of Noise: Colours of noise are always termed in analogy to the white light spectrum. If within a spectral range of noise the high frequency end is over-represented, the noise becomes blue, if the middle part is over-represented the noise is green or yellow, if the low frequency part is over-represented noise is red. A good place to hear people talking about noise colours is at a 'freelance electronic engineers / radio-amateur' convention.

Brown Noise ($1/f^2$ noise): This is a special form of noise, and is not named after a colour (or digestive sounds), but after botanist Robert Brown (1773 - 1858), of 'Brownian Motion' fame. In this particular case the fluctuations occur like in a 'random walk' or in diffusion: The final result is white noise (the random numbers are everywhere), but for a finite interval of time the numbers have a higher probability to stay close to the previous value than to move far away from it.

Shot-noise: The amplitude of noise often depends on the intensity of the measured signal, because the noise of the background adds up with the noise from the measured property. Shot-noise increases linearly with the square-root of the (signal) intensity. Shot noise plays a key role in the detection of intermittent data, for example laser pulses or sequences of ones and zeroes through a wire. It is called shot-noise in analogy to the distribution of bullet-holes produced by a shotgun.

Glossary

a bassoon – фагот (музыкальный инструмент)
to eliminate – устранить, уничтожить, избавиться от чего-либо
layman – непрофессионал, неспециалист
speckled – рябой, в крапинку
to fine-tune – настраивать, регулировать
fluctuation – колебание, неустойчивость
perceptible – ощутимый, заметный, воспринимаемый
entity – сущность, феномен, единство
voltage – напряжение
random – случайный, беспорядочный
viscosity – вязкость, клейкость, тягучесть
pseudo-… - ложный…
stringent – веский, убедительный, обязательный
the mean value – среднее значение, величина
linearly – линейно
distribution – распределение, распространение
flat – ровный
suppress – подавлять, сдерживать
punch – удар кулаком
diffusion – рассеивание, диффузия
a shot – выстрел
intermittent – скачкообразный

Answer the following questions:
1. What is noise?
2. What characteristics does noise possesses?
3. What types of noise do you know? Describe them.
4. Give any examples of noise.
5. Do the research as your home assignment. What scientists were or are interested in noise?

UNIT XXV
@ - THE HISTORY

The @ symbol has become the emblem of an age. Not only is it the fulcrum of every Internet email address, but also it has been widely co-opted to add the 'Net flavour' to almost any name or <u>trademark</u>. Who would suspect that @ is more than half a <u>millennium</u> old?

Britain's *The Guardian* newspaper recently reported research by Italian academic Giorgio Stabile indicating that @ was created as an indication of weight or <u>volume</u>.

Stabile says that the first known <u>incidence</u> of its use is in a letter written by the Florentine <u>merchant</u> Francesco Lapi on 4 May, 1536. Sent from Seville to Rome, the letter describes the arrival of three ships bearing goods from South America.

In it, the @ sign represents an amphora, <u>a measure of capacity</u> based on the terracotta jars used to transport grain and liquid in the ancient Mediterranean world.

The distinctive loop of the tail of the 'a' is, says Stabile, typical of the mercantile script developed by Italian traders between the Middle Ages and the Renaissance.

Stabile <u>believes</u> that the symbol <u>filtered up</u> the trade routes to northern Europe where <u>accountants</u> began using it as <u>shorthand</u> for 'at the price of'.

It was this <u>application</u> that allowed @ to <u>creep onto</u> the <u>keyboards</u> of typewriters in the early 20th Century and, later, onto keyboards connected to the computers of the 1950s and 1960s. However, <u>given that</u> most of us are not accountants, it languished.

The relative <u>lack of use</u> of the @ symbol in day-to-day communication was a factor for Ray Tomlinson, an American engineer who is one of a select group of men who created what we now know as the Internet.

In March 1972, three years into the life of the first incarnation of the Internet, ARPAnet, Tomlinson completed the email software, which he had designed to allow ARPAnet developers to easily communicate with each other. The move to the use of the network for personal use rather than data transfer or <u>remote computing</u> changed the world we live in.

In defining the way the email software would work, Tomlinson had to pick a character to stand between the user name to the left of an email address and the domain information to the right. He has since explained that he chose @ because it wouldn't be found in a person's name. As the symbol became ubiquitous in the 1990s, its look – in unconscious emulation of that old mercantile script – was even applied to other <u>characters</u>. IBM adopted an 'e' wrapped in its own tall as the brand for its e-business products. Proposed <u>legal action</u> by a hitherto unknown company called E Technologies, which claimed to have begun using the encircled 'e' in April 1997, four months before IBM, fizzled out.

Stabile told *The Guardian* that the 16th Century merchants of the Mediterranean would have considered the modern use of the symbol to be highly appropriate, saying:

No symbol is born of chance, this one has represented the entire history of navigation on the oceans and has come to typify travel in cyberspace.

The professor suspects that even older instances of the symbol's use may be lurking in the archives of Italian banks. He <u>urged</u> the most <u>venerable</u> banks to start looking, pointing that 'the oldest example could be of great value. It could be used for publicity purposes and <u>to enhance</u> prestige of the institution that <u>owned</u> it'.

Yet if the Italian coinage has become a key part of the Anglophone world of the Internet, we speakers and writers of English have failed to come up with a decent name for it. Its formal identity as 'commercial at' is hardly inspiring.

The Spanish have long had a word for it – *arroba*, which in the 16th Century indicated a weight or measure equivalent to 11.3kg (25 pounds) or 22.7 litres (six gallons). Modern Italian Internet users refer to the symbol as *la chiocciola* – the snail, used frequently around the world.

Names other Countries Use to Desribe @

- The Germans call it *klammeraffe* (spider monkey).
- The Dutch, *apestaartje* (monkey's tail).
- Danes <u>refer to</u> it as *grisehale* (pig's tail) or *snabel* (with an elephant's trunk).
- The official Norwegian name is *krøllalfa*. Some people say *alfakrøll. Krøll* means curl, *alf* is alpha hence Curlalpha.
- Finnish people call it *kissanhanta* (cat's tail), which sometimes goes one step further to become *miukumauku* - the meow sign!
- Hungarians see it as the worm or maggot, *kukac*.
- The Thai word translates as 'the wiggling worm-like character'.
- Czechs call it *zavinac*, which is a rollmop herring.
- The Hebrew term is *strudel*, the famous Viennese apple pastry.
- The word *Pita*, a type of bread, is often used in Israel.
- Swedes use *kanelbulle* (cinnamon bun) and *snabel-a* (a with a trunk).
- The French go with *escargot* which translates as snail.

The amazingly useful @ symbol is also used in CAD software to distinguish relative co-ordinate measure from absolute. In AutoCAD it works like this: if you are standing on the point 50,50 and give the command @20,20, you will end up at coordinates 50+20, 50+20 = 70,70. If you just put 20,20 without the @, then you will end up on the point 20,20.

Glossary

<u>fulcrum</u> – точка опоры, центр
<u>terracotta</u> – керамика, глина
<u>a loop</u> – петля
<u>mercantile</u> – коммерческий
<u>to filter</u> – двигаться
<u>to languish</u> – слабеть, увядать, постепенно исчезать
<u>ubiquitous</u> – повсеместный, вездесущий
<u>emulation</u> – эмуляция, копирование, подражание
<u>hitherto</u> – до настоящего времени

to fizzle out – потерпеть фиаско, окончиться провалом
to typify – символизировать, олицетворять
to lurk – прятаться, скрываться
venerable – достойный, почтенный
coinage – новое слово, процес создания нового слова
to come up with sth – придумать (e.g. to come up with solution)
a snail – улитка
a spider-monkey – паукообразная обезьяна
an elephant's trunk – хобот
a maggot – личинка
a rollmop – рольмопс (рулет из селедки)
CAD – computer aided design – проектирование при помощи компьютера

A: *Translate the underlined words. Use them in the sentences of your own.*
B: *Answer the following questions:*
   1. What is the origin of @?
   2. In what ways was @ used according to the text?
   3. Where was @ used with the meaning 'at the price of'?
   4. Why did @ appear on and disappear from keyboards of typewriters?
   5. Why was @ used by Ray Tomlinson?
   6. What names are used in different countries to describe @?

UNIT XXVI
HOW A LASER WORKS

Lasers are widely used in the fields of technology, science and entertainment. Almost everyone has used one in daily life (possibly without knowing – there's one in your CD player), but only a few people know how it works, although it is, to a certain extent, quite simple. The history of the development, the uses and types of laser can be found in the Laser entry.

This entry focuses on the working mechanism of a laser. For a reasonable understanding of the involved mechanisms, a little digression about light-emitting processes is included (the first two sections) and can be skipped – a brief summary is included right after these chapters.

Absorption (or Excitation)

Objects can absorb light, and this is the reason why things look the way they do. Taking a closer look at how light absorption takes place makes the concept of emission more understandable. To make it less complicated, it is best just to accept that certain colours are absorbed better than other colours are.

When a flash of light, or a photon, with the best fitting colour hits a very small piece of matter like a molecule (or an atom) it may be absorbed. Since the energy cannot just be eliminated, the molecule will start behaving differently. Scientists say that the molecule is in an 'excited state' (it can redirect the energy into motion, wiggling about, rotating, sending the electrons into more complicated orbits or whatever). The energy of the absorbed photon is now in the excited molecule (or atom) and the photon is lost. This is absorption.

An example to illustrate this: white light can be analysed using a prism. What one sees is that the white light is composed of all colours of the rainbow. When shining white light through a red-dyed glass it changes its colour. When analyzing this light one will see that the green and blue parts of the spectrum are missing. Why? These components have been absorbed by the dye molecules in the glass.

Relaxation

After the molecule (or atom) has been excited it is in a 'high-energy state'. This energy can dissipate mechanically, causing the material to heat up (this process is called radiationless relaxation), or after a while the molecule can 'decide' to emit a photon (which usually has a lower energy than the original photon used to excite the molecule) and relax. There are two light emission mechanisms:

• **Spontaneous Emission** – After a certain while the photon is emitted in any direction. This process is the one observed for neon lamps. It is not influenced by anything except for the molecule's (or atom's) intrinsic properties, ie how long in average it takes for this process to occur, and how strong it is compared to the radiationless relaxation described above.

• **Stimulated Emission** – Another photon coming from somewhere else can trigger an excited molecule to relax and emit the excitation photon. In order for that to happen, both photons (the triggering one and the one to be released) must have the same energy (i.e. colour). In contrast to the spontaneous emission, the emission is now governed by the incoming trigger photons, and the emitted photon will have exactly the same direction, energy and phase (because the releasing and the triggering occur in a synchronized way) as the incoming trigger photon. This kind of emission is used to generate laser light.

Summary

There are four processes involved in the light emission process:

• The *absorption* of photons by a material (which will be henceforth called the *medium*), which is then in an excited energy-state.

• The *radiationless relaxation.*

• The *spontaneous emission.*

• The *stimulated emission.*

The latter two are responsible for light generation in a laser.

Materials can be analysed or designed to have a good absorption yield, a small radiationless relaxation rate, and a high fluorescence rate (which is the spontaneous and the stimulated emissions together). When this is the case, almost all input energy can be converted into light, and such a material is said to have a good quantum yield (the percentage of the energy that can be converted into light). This can be close to 100% for certain dye molecules.

How Exactly is Laser Light Generated?

The medium where the laser light is going to be generated is typically one with a high quantum yield. This medium can be excited[1] to emit light by many means (applying electric currents, allowing chemical reactions, flashing light into it, etc). Right after the medium is excited for the first time, spontaneous emission will take place: photons are generated and they will fly away in any direction. This procedure

is continuously repeated many millions of times a second, so that one could think of a medium that is constantly in an excited state and at the same time emitting photons.

This medium is placed between two mirrors. Eventually the trajectory followed by one of the many photons that are coming out of the medium will be reflected by one of the mirrors straight back into the medium and to the other mirror. A photon on that trajectory will follow it a few million times before it is scattered away. Such a photon, when passing the medium, will trigger the stimulated emission. The two photons, ie the trigger photon and the emitted photon will have the same direction, energy and phase – the light is therefore called *coherent*.

At this moment there will be two photons on exactly the same path. At the next moment, when the two photons return from a mirror, they will force two more photons onto the same path, next time there will be 8 photons on the path, then 16, 32, 64 and so forth. Eventually one or two photons can be lost[2], so next time there will not be 128 but 126 photons on the path, then 250, 498, 990 and so forth. The number of photons will grow until a certain limit is reached. The limit is reached when the excitation rate is equal to the emission rate minus the loss of photons. The light kept between the mirrors is laser light.

The next stage is to get the light out of the mirror-medium-mirror arrangement, which is called an *optical resonator*[3] in a manner analogous to acoustic resonators. (Sometimes the resonator is also called the 'cavity', which is much shorter, and therefore widely used.) In order to do that, one of the mirrors is designed to reflect only 99% of all the light, so each time 1% of the laser light is let out. That implies that the threshold for laser activity must be lowered accordingly (the 'loss of photons' term).

A further consideration involves the distance between the two mirrors. It must be an integer multiple of the wavelength of the laser light (otherwise the light will annihilate itself due to destructive interference). For that reason, most lasers can be tuned – i.e. the colour coming out of the laser can vary. The tuning range can be very low if the emission band is narrow (e.g. 1nm – no visible colour difference[4]), and it can be wide when the emission band is broad (e.g. 200nm – a very noticeable change). The width of emission bands depends on the medium used, and is, except for gas lasers, usually quite broad.

In order for light to be amplified, there must be more photons coming from the relaxation process (stimulated emission) than being used to excite the molecules (by absorption). For this to happen, the number of excited molecules must be greater than the number of relaxed molecules (otherwise the photon will be absorbed and not used to stimulate emission). This particular situation is called *population inversion* and is easily achieved when the light-emitting relaxation process does not lead directly to the lowest (or ground) state, but to one above that, which is most easily and rapidly depopulated (eg by radiationless relaxation) and therefore almost always empty. This ensures the constant population inversion.

Recap

Roughly how a laser works:

• Light is generated somewhere between two mirrors (which is an arrangement called an *optical resonator*) and kept exactly between them.

• It bounces back and forth and generates ever more light by *stimulated emission*. For that to happen there must be more excited molecules in the medium than relaxed ones (otherwise the photon will be absorbed and not used to stimulate emission), a situation called *population inversion*.

• Light generated by stimulated emission has the same energy, direction and phase as the light that was used to stimulate the emission, and is therefore called *coherent* or laser light.

• If the generation of light is stronger than the loss (by mirrors or air), more and more light will accumulate between the mirrors. One of the two mirrors is designed only to reflect 99% of the light, so every time 1% of the resonating laser-light will be let out.

---

[1] In laser jargon this process is often called *pumping*.

[2] Due to spontaneous emission, absorption or scattering.

[3] The length of typical optical resonators varies from a few millimetres (diode lasers) to one or two metres (dye or crystal lasers).

[4] The visible spectrum ranges from violet (wavelength 400nm) to deep red (wavelength 800nm).

Glossary

absorption - поглощение
excitation - возбуждение
relaxation – ослабление, уменьшение напряжения
to dissipate - рассеивать
radiation - лучеиспускание
emission – эмиссия электронов
spontaneous - самопроизвольный
intrinsic - внутренний
to trigger – приводить в движение, вызывать
to emit - излучать
absorption yield – коэффициент поглощения
fluorescence - свечение
to scatter - рассеивать
coherent – связанный, сцепленный
cavity – полость, впадина
integar – целое число, нечто целое

UNIT XXVII
HI-TECH CRIME

A: *Discuss the following questions:*
1. What do you know about PC security?
2. What is a virus?
3. What is a worm?
4. What have you heard about hackers?

B: *Read the following glossary and try to find equivalents in Ukrainian to basic terms.*

Hi-tech crime: A glossary

ADWARE – Unwanted programs that, once installed, bombard users with unwanted adverts. Often those pushing the aware programs get paid for every machine they manage to recruit.

Some adware poses as fake computer security software. Can be very hard to remove.

BLACKHAT – A hacker that uses his or her skills for explicitly criminal or malicious ends. Has been used to mean the writers of destructive viruses or those that use attacks to knock websites offline. Now as likely to refer to those that steal credit card numbers and banking data with viruses or by phishing.

BOT – The name given to an individual computer in a larger botnet and which is more than likely a home PC running Windows. The name is an abbreviation of "robot" to imply that it is under someone else's control.

BOTNET – A large number of hijacked computers under the remote control of a single person via net-based command and control system.

The machines are often recruited via a virus that travels via e-mail but increasingly drive-by downloads and worms are also used to find and recruit victims.

The biggest botnets can have tens of thousands of hijacked computers in them. Research suggests they can be hired from as little as 4 cents per machine.

BOTNET HERDER – One of the names for the controller or operator of a botnet.

BULLET-PROOF HOSTING – A company that guarantees that its servers will not be shut down even when the request to do so comes from law enforcement agencies.

These hosting companies are often located off-shore or in nations where computer crime laws are lax or non-existent and where extradition requests will not be honoured.

CARDER – Someone who steals or trades exclusively in stolen credit card numbers and their associated information.

CASH-OUT – A euphemism that means to steal money from a bank account or credit card to which someone has gained illegal access.

Hackers who grab credit card data often do not possess the skills or contacts to launder the money they can steal this way.

CHANNEL – A virtual "room" on the IRC text chat system. Most channels are usually dedicated to a single topic.

CROSS-SITE SCRIPTING – A sophisticated phishing attack that exploits weaknesses in the legitimate sites of financial institutions to make attempts to trick people into handing over confidential details more plausible.

A successful use of Cross-site scripting will make it look like all the transactions are being done on the website of the real bank or financial institution.

DEAD-DROP – A hijacked PC or server used to store all the personal data stolen by keyloggers, spyware or viruses.

Criminal hackers prefer to keep their distance from this data as its possession is incriminating. Dead drops are usually found and shut down within a few days of the associated phishing e-mails being sent out.

DDoS – Abbreviation for Distributed Denial of Service. This is an attack in which thousands of separate computers, which are usually part of a botnet, bombard a target with bogus data to knock it off the net.

DDoS attacks have been used by extortionists who threaten to knock a site offline unless a hefty ransom is paid.

DRIVE-BY DOWNLOAD – Malicious programs that automatically install when a potential victim visits a booby-trapped website.

The vast majority exploit vulnerabilities in Microsoft's Internet Explorer browser to install themselves.

Sometimes it is obvious that a drive-by download has occurred as they can lead to bookmarks and start pages of the browser being replaced. Others install unwanted toolbars.

Increasingly criminals are using drive-bys to install keyloggers that steal login and password information.

EXPLOIT – A bug or vulnerability in software that malicious hackers use to compromise a computer or network.

Exploit code is the snippet of programming that actually does the work of penetrating via this loophole.

FIREWALL – Either a program or a feature built into hardware and which sits between a computer and the internet. Its job is to filter incoming and outbound traffic.

Firewalls stop net-borne attacks such as worms reaching your PC.

HONEYPOT – An individual computer or a network of machines set up to look like a poorly protected system but which records every attempt, successful or otherwise, to compromise it.

Often the first hints of a new rash of malicious programs comes from the evidence collected by honeypots.

Now cyber criminals are tuning their malware to spot when it has compromised a honeypot and to leave without taking over.

IP ADDRESS – The numerical identifier that every machine attached to the internet needs to ensure the data it requests returns to the right place. IP stands for Internet Protocol and the technical specification defines how this numerical system works.

IRC – Abbreviation for Internet Relay Chat – one of the net's hugely popular text chat systems.

The technology is also used by botnet herders to keep tabs on and control their flock of machines.

KEYLOGGER – Program installed on a victim's machine that records every keystroke that a user makes.

These tools can obviously be very useful for stealing login and password details. However, the data that is stolen often has to be heavily processed to make it intelligible and to extract names and numbers.

MALWARE – Portmanteau term for all malicious software covers any unwanted program that makes its way on to a computer. Derived from **Mal** icious soft **ware** .

MAN-IN-THE-MIDDLE – A sophisticated attack in which a criminal hacker intercepts traffic sent between a victim's computer and the website of the organisation, usually a financial institution, that they are using.

Used to lend credibility to attacks or simply steal information about online accounts. Can be useful to defeat security measures that rely on more than just passwords to grant entry to an account.

PACKET SNIFFING – The practice of examining the individual packages of data received by a computer to find out more about what the machine is being used for.

Often login names and passwords are sent in plain text within data packets and can easily be extracted.

PHISHING – The practice of sending out e-mail messages that look as if they come from a financial institution and which seek to trick people into handing over confidential details.

Often they direct people to another website that looks like that of the bank or financial institution the e-mail purports to have come from. Anyone handing over details could rapidly have their account plundered.

PORT – The virtual door that net-capable programs open to identify where the data they request from the net should be directed once it reaches a computer.

Web browsing traffic typically passes through port 80, e-mail through port 25.

ROOTS – A slang term for networks that have been hacked into by criminal hackers. Derives from the deep, or root, access that system administrators typically enjoy on a network or computer.

The login details to get root access are often sold to spammers and phishing gangs who then use these networks to send out millions of e-mail messages.

SCRIPT KIDDIE – An unskilled hacker who originates nothing but simply steals code, techniques and attack methods from others.

Many viruses and worms on the web today are simply patched together from other bits of code that malicious hackers share.

SPYWARE – Malicious program that, once installed on a target machine, steals personal and confidential information. Distinct from adware.

Spyware can be contracted many different ways. Increasingly it arrives on a PC via a web download. Often uses a keylogger to grab information. Some are now starting to record mouse movements in a bid to foil the latest security measures. Some fake security programs pose as spyware cleaners.

TCP – Abbreviation for Transmission Control Protocol - the series of specifications which define the format of data packets sent across the internet.

TROJAN – Like the wooden horse of legend this is a type of program or message that looks benign but conceals a malicious payload. Many of the attachments on virus-bearing e-mail messages carry trojans.

VIRUS – A malicious program – usually one that requires action to successfully infect a victim. For instance – the malicious programs inside e-mail attachments usually only strike if the recipient opens them.

Increasingly the word is used as a portmanteau term for all malicious programs - those that users must set off or those that find their own way around the net.

WHITEHAT – A hacker that uses his or her skills for positive ends and often to thwart malicious hackers.

Many whitehat security professionals spend their time looking for and closing the bugs in code that blackhats are keen to exploit.

WORM – Self-propelled malicious program that scours the web seeking new victims – in the past this has been used to distinguish it from a virus that requires user action to compromise a machine.

Worms can infect and take over computers without any help, bar lax security, from a victim.

ZERO DAY – A Zero day vulnerability is one on which code to exploit it appears on the first day that a loophole is announced.

As most of the damage done by exploiting bugs occurs in the first few days after they become public, software firms usually move quickly to patch zero day vulnerabilities.

ZOMBIE – Another name for a hijacked computer that is a member of a botnet.

adware – рекламное ПО (разновидность malware, без согласия пользователя выводит рекламные сообщения, загружает сайты, посвящённые рекламируемой продукции и т.п.)

to pose – представлять из себя

phishing – выуживание, «фишинг» (преступная деятельность интернет-мошенников, действующих под видом благонадёжных компаний и юридических лиц, с целью незаконного получения секретной информации: паролей, данных кредитных карточек, логинов; мошенничество, направленное на получение банковских конфиденциальных данных клиентов с целью хищения денег, как правило, с помощью компьютерных технологий)

botnet – бот-сеть, ботнет (сеть из компьютеров ('зомби'), зараженных ботами, способная управляться удаленно для выполнения массированных действий (рассылка спама, проведение атак отказа в обслуживании и т.д.)

lax – слабый, вялый, неопределенный

plausible – возможный, вероятный

dead-drop – тайник

keylogger – кейлоггер (программа, записывающая нажатые пользователем клавиши, часто с целью кражи паролей и прочих конфиденциальных данных)

spyware – шпионское ПО (разнообразные программы, нелегально собирающие информацию с зараженного компьютера)

shut down – прекращать работу, закрывать(ся)

distributed – распространенный, рассредоточенный

bogus – фальшивый поддельный

extortionist – шантажист, вымогатель

hefty – значительный, обильный, большой

ransom – выкуп

booby-trapped – минированный

vulnerabilities – уязвимость

malicious – злой, зловредный

exploit – эксплойт вредоносный код, эксплуатирующий уязвимости программных компонентов компьютера)

snippet – часть, кусочек

loophole – лазейка (для проникновения в систему)

firewall – шлюз безопасности, система ограничения доступа

honeypot – приманка, «медонос» (незащищенная сеть для изучения приемов хакеров)

malware – вредоносные программные средства, цель которых – нарушение работы ПК

to spot – обнаружить, заметить

tab – учет, счет

a flock – стадо, группа, большое число

portmanteau – слово-гибрид

sniffing – вынюхивание, контроль сообщений, передаваемых по сети связи, с целью получить конфиденциальную информацию

to purport – говорить, иметь в виду, означать

script kiddie – взломщик-дилетант, хакер-дилетант

to foil – отразить нападение, расстроить планы

benign – доброкачественный, хороший

payload – груз, нагрузка, заряд

to thwart – пресекать, мешать, срывать планы

to scour – рыскать

to bar – тормозить, преграждать, мешать

vulnerability – уязвимость, ранимость

C: *Using the glossary do the test on PC security.*

How well do you know PC security?

Is your PC well protected or is it the plaything of malicious hackers the world over?

To find out if you are security savvy or simply a sucker, answer the questions in our quiz and find out how much you know about staying safe when using the web.

Question 1. If you had a zombie in your house, what would you do?

A: Dig out your shotgun.

B: Clean up your PC with an anti-virus scanner – a zombie is a computer hijacked by malicious hackers.

C: Look for the TV cameras - it must be a new reality TV series.

Question 2. What was "Elk Cloner"?

A: The first computer virus seen in the wild – it infected Apple machines.

B: The first computer virus seen in the wild – it infected IBM mainframes.

C: The first computer virus seen in the wild – it infected TRS-80 machines.

Question 3. An e-mail turns up bearing an attachment labelled as video of a nude celebrity. What do you do?

A: Delete it – there's probably a virus in the attachment.

B: Open it and forward it to all your friends so they can enjoy the fun.

C: Sounds good, open it and sit back to watch.

Question 4. Windows is nagging you to update the operating system. What do you do?

A: Ignore it, the updates will just slow down your machine.

B: Install the updates as soon as they become available.

C: Update every six months. Just to keep Microsoft happy.

Question 5. You get an e-mail saying there are problems with your online bank account.

The message does not address you by name. What do you do?

A: Forward it to your bank and then delete it. The message is a phish.

B: This sounds serious. Open it and click on the link in it and login.

C: Withdraw all your money and put it under the mattress where it will be safe.

Question 6. What is a root kit?

A: A software package that helps you draw up your family tree.

B: A way to improve the health of your rose bushes.

C: A very stealthy computer virus that buries itself in your PC's operating system to avoid detection.

Question 7. After downloading a new screensaver you get bothered with lots of pop-up ads, your web browser's start page has changed and any search is re-directed. What do you do?

A: Install a pop-up blocker to get rid of the adverts.

B: Run an anti-spyware package to see if your computer has contracted any of the bothersome bugs.

C: Scan your machine with both anti-virus and anti-spyware software.

Question 8. What is a firewall?

A: The bricks at the back of the hearth.

B: Software that sits between your PC and the net and blocks net-borne attacks.

C: The notice board in the corridor announcing redundancies.

Question 9. You need to choose a password for the account you have set up at an online shop.

What do you do?

A: Pick one that combines letters and numbers that make it hard to guess.

B: Use the word "password" - it's easy to remember.

C: Use the same one as you use on every other site.

Question 10. What is a DDoS attack?

A: Guerilla activism by open source software advocates in which they uninstall Windows on a PC and replace it with Linux.

B: US politicians criticising the US Department of Defense's Office of Security.

C: One that tries to knock a web server offline by bombarding it with huge amounts of data.

MODULE VIII

UNIT XXVIII
TRACKING DOWN HI-TECH CRIME

If every hour a burglar turned up at your house and rattled the locks on the doors and windows to see if he could get in, you might consider moving to a safer neighbourhood.

And while that may not be happening to your home, it probably is happening to any PC you connect to the net.

An investigation by the BBC News website has established the scale of the dangers facing the average net user.

Using a computer acting as a so-called "honeypot" the BBC has been regularly logging how many potential net-borne attacks hit the average Windows PC every day.

Attack traffic

Honeypots are forensic tools that have become indispensable to computer security experts monitoring online crime. They are used to gather statistics about popular attacks, to grab copies of malicious programs that carry out the attacks and to get a detailed understanding of how these attacks work.

To the malicious programs scouring the web these honeypots look like any other PC. But in the background the machines use a variety of forensic tools to log what happens to them.

Perhaps one indicator of how useful these tools have become is seen in the fact that the most sophisticated attackers make their malicious programs able to recognise when they have trespassed on a honeypot.

The BBC honeypot was a standard PC running Windows XP Pro that was made as secure as possible. This ran a software program called VMWare which allows it to host another "virtual" PC inside the host. Via VMWare we installed an unprotected version of Windows XP Home configured like any domestic PC.

VMWare is useful as it makes it easy to pause the "virtual" PC or roll it back to an earlier configuration. This proved essential when recovering from an infection.

This guest machine, once armed with some forensic software, became the honeypot.

When we put this machine online it was, on average, hit by a potential security assault every 15 minutes. None of these attacks were solicited, merely putting the machine online was enough to attract them. The fastest an attack struck was mere seconds and it was never longer than 15 minutes before the honeypot logged an attempt to subvert it.

The majority of these incidents were merely nuisances. Many were announcements for fake security products that use vulnerabilities in Windows Messenger to make their messages pop-up. Others were made to look like security warnings to trick people into downloading the bogus file.

Serious trouble

However, at least once an hour, on average, the BBC honeypot was hit by an attack that could leave an unprotected machine unusable or turn it into a platform for attacking other PCs.

Many of these attacks were by worms such as SQL.Slammer and MS.Blaster both of which first appeared in 2003. The bugs swamp net connections as they search for fresh victims and make host machines unstable.

They have not been wiped out because they scan the net so thoroughly that they can always find another vulnerable machine to leap to and use as a host while they search for new places to visit.

Their impact is limited now because Windows is now sold with its firewall turned on and the patch against them installed. Recently Microsoft said it was cleaning up hundreds of PCs hit by these machines every day.

Many of these worms were launched from different PCs on the network of a French home net service firm but others were from machines as far away as China.

There were also many attempts to probe the BBC honeypot to see how vulnerable it was. Hijacked machines in Brazil as well as at the Indiana offices of a public accounting and consulting firm carried out "port scans" on the BBC honeypot to see if it could get a response that would reveal how vulnerable it was.

Via the honeypot we could see these machines sending test data in sequence to the ports, or virtual doors to the net, that the PC had open.

More rarely, once a day on average, came net attacks that tried to subvert the honeypot to put it under the control of a malicious hacker.

Again these attacks came from all over the world – many clearly from hijacked machines. The BBC honeypot was attacked by a PC at a Chinese aid organisation, a server in Taiwan and many machines in Latin America.

Via the forensic tools installed on the honeypot we could see the booby-trapped data packets these bugs were trying to make our target machine digest.

By using carefully crafted packets of data, attackers hope to make the PC run commands that hand control of it to someone else.

Via this route many malicious hackers recruit machines for use in what is known as a botnet. This is simply a large number of hijacked machines under the remote control of a malicious hacker.

Botnets are popular with hi-tech criminals because they can be put to so many different uses. The slaves or bots in a botnet can be used to send out spam or phishing e-mails.

They can become the seeding network for a new virus outbreak or act as a distributed data storage system for all kinds of illegal data. Spammers, phishing gangs and others often rent a botnet to use for their own ends.

Often once a machine has fallen under someone else's control, a keylogger will be installed to capture information about everything that the real owner does - such as login to their online bank account.

This stolen information is often sold as few of those that steal it have the criminal connections to launder stolen cash.

How the trap was set

The BBC honeypot posed as a normal computer to see what malicious hackers tried to do with it. Here we illustrate what might have happend if it had been hijacked by a worm or virus.
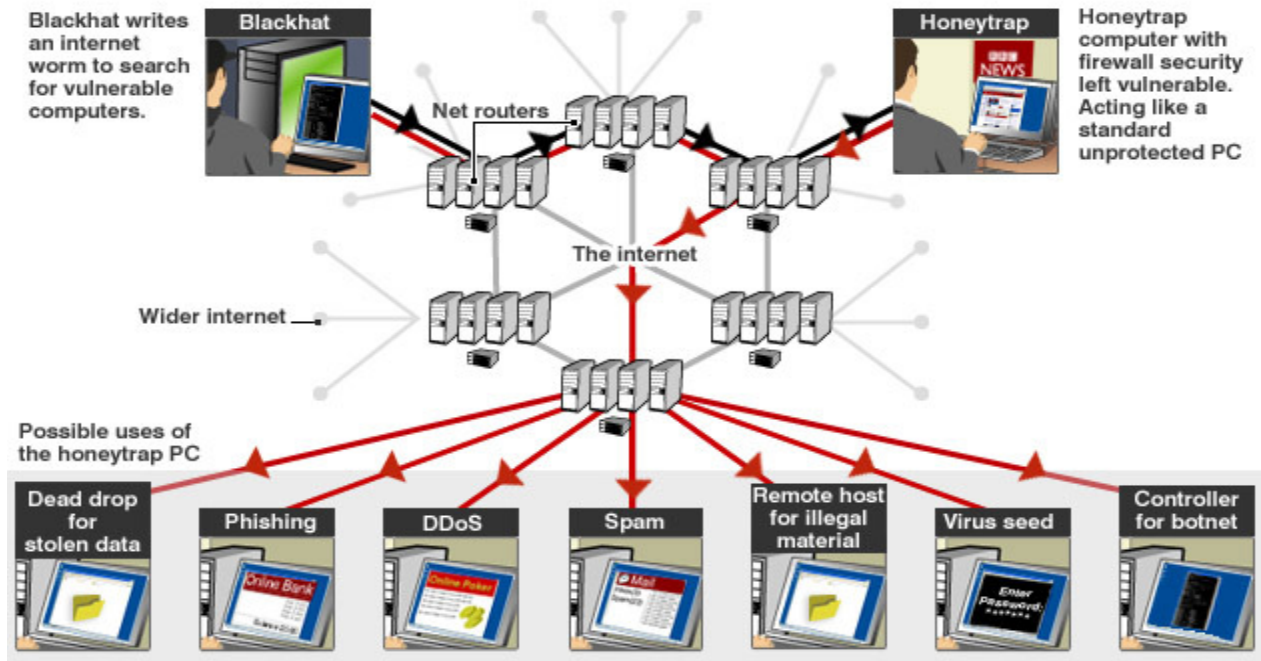
Read the glossary on tracking down hi-tech crime

to track down – выследить, поймать, отыскать

forensic – судебный, судейский

to trespass – совершать проступок, нарушать границы

to host – принимать гостей, быть хозяином

to solicit – подстрекать к совершению преступления, приставать, напрашиваться

nuisance – неприятность, помеха, неудобство

to swamp – заваливать, засыпать

to wipe out – уничтожить, стереть

subvert – свергнуть, подчинить

bona fide – настоящий, честный, без обмана

sneakily – хитро, коварно, исподтишка

unwitting – невольный, непреднамеренный, нечаянный, незнающий

banter – шутливая беседа, шутка

flaming – обман

opaque – непонятный, темный

to hawk – распространять слухи, сплетни

cadre – постоянный состав, кадры

prolly = probably

to stag – спекулировать (ценными бумагами)

to rip off – надувать, обманывать, грабить

to kick up a fuss – поднять скандал, суматоху

A: *Answer the questions:*
1. What is honeypot?
2. Describe the honeypot set by BBC.
3. What kind of attacks did the honeypot set by BBC suffer?
4. What is a botnet? For what purposes can hackers use bots?
5. What is the potential harm of a keylogger?

B: *Give definitions to the following words:*

Adware, phishing, botnet herder, malware, worm, blackhat, script kiddie, firewall, dead-drop, DDoS, spam, virus, whitehat, zombie, port, trojan, honeypot, man-in-the-middle.

UNIT XXIX

TRAPPING HACKERS IN THE HONEYPOT

How the trap was sprung

In this second part of our investigation using the BBC honeypot we recount what happened when we let the machine get infected rather than just log attacks.

It is rare that you would willingly let vandals and burglars into your home but a controlled environment like a honeypot computer lets you do the technological equivalent in relative safety.

The idea of letting the PC get infected was to see exactly what nasty programs hit our machine and how easy it was to recover from infection.

Firstly, we visited a few of the websites mentioned in the many fake security warnings that pop-up unprompted thanks to loopholes in Windows Messenger.

Much of the software available via these bogus warnings turned out to be a nuisance rather than downright malicious.

The programs offered a free scan of the honeypot machine looking for spyware and adware. Every one we installed found a huge amount of spyware lurking on the computer.

This was a surprise: The honeypot machine had only been used to visit the websites from which the bogus software had been downloaded.

Checking the results with a bona fide spyware spotter revealed that most of the spyware identified by the fake software was benign.

If this was not bad enough, all the fake security programs demanded money before they handed over the full results of the scan or tried to fix problems that were not there.

Spyware storm

One of the websites sending out fake security spam looked particularly interesting as it was listed on several "block lists" net service firms use to spot junk mail.
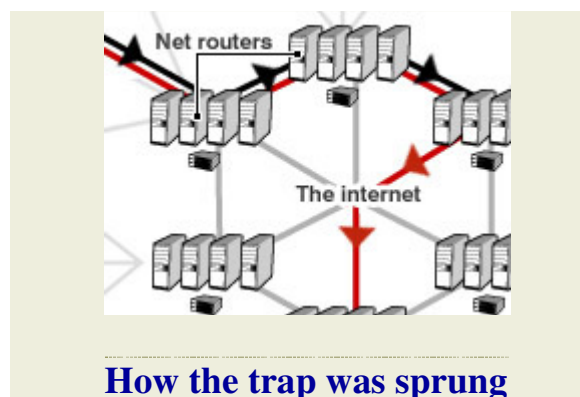
A visit to this website prompted an immediate re-direct to another site which popped up a box asking if we wanted to download the bogus security program.

Sneakily this was an image rather than a Windows dialogue box so clicking anywhere on it, even the "cancel" button, got the download going.

The download installed automatically and kicked off a tsunami of background downloading. The forensic software we had installed on the honeypot saw it connect to three or four other sites and start downloading from them – one was from a Thai hospital that was doubtless acting as an unwitting host.

The software was so sneaky that it tried to stop this traffic being seen by injecting it into the processes usually used by the Internet Explorer. We knew this was the case because IE's homepage had been set to be blank – i.e. when it was running there would be no net traffic.

The result of the installation was new toolbars on the IE browser, a whole list of new unwanted favourites, all web searches were hijacked and redirected plus pop-up adverts populated the desktop.

The machine was becoming unusable because it was so busy so we were forced to cut the net connection.

The bogus download went into overdrive trying to get back online. The meter clocking processor usage zoomed to 100% as it desperately tried to drag more stuff into the PC.

The machine became hard to shut down and we could only shut it off by pulling the virtual plug.

The end result of that single download was a PC that was unusable as it was so clogged with adware and spyware. A quick scan of the machine revealed that seven viruses, mostly trojans, had been installed during the orgy of downloading.

We reverted back to the original configuration of the honeypot machine to get rid of the problems but this particular chunk of spyware was not done yet.

On the honeypot a USB drive was being used to take backups of the attack logs. This had been plugged in to the machine while the fake security program installed itself.

The USB drive had gained a new passenger – the core program of the fake spyware. If we had let this continue, doubtless it would have fired off next time the drive was plugged in to any other machine. It was a close escape.

Cleaning up the PC proved impossible. It was lucky we could just revert to an earlier configuration. If the honeypot had been a home PC almost everything stored on it, pictures, e-mails, might have been lost.

Answer the following questions:

1. What were the purposes to let the computer used by BBC be infected?

2. Describe the results of the experiment carried out by BBC.

3. What piece of advice can you give to a "fresh" Internet user as to computer security.

UNIT XXX
TACKLING THE HACKERS FACE-TO-FACE

I'm lurking on IRC - Internet Relay Chat - the place where lots of net users go to talk via typed text on any and every conceivable topic.

But instead of talking about games, last night's big match or MP3s, I'm on channels with names like cc-visa, ccfull, ccpower and trade-cc.

I'm in bandit country.

The "cc" stands for "credit cards" and these are the virtual markets where thousands of stolen numbers are bought and sold all day, every day.

Card games

In most busy IRC discussion rooms, or channels, the threads of conversations are hard to follow because the typed text flies by so fast. It's like going to a party and being told you can only chat to other people by texting them on your mobile phone.

But in the channels I've joined there is no idle banter, flaming or anyone passing the time of day. It's all business, all the time.

The channels are full of adverts touting stolen goods (credit card numbers), ways to launder the cash extracted from cards and accounts or offering the other services the dedicated cyber criminal needs.

The adverts use jargon that is opaque to anyone who has not been hanging out here for some time.

The jargon reveals how the hi-tech crime world is divided. Typically those involved in net crime do one thing well. Some plunder web shop databases and steal credit card numbers. Some hack business networks so they can be used by spammers. Some are phishers who send out e-mail trying to fool people into handing over their banking details. Others have the bank accounts to help people move cash without being caught.

The hackers lack the skills to do anything with the data they steal and the old-time criminals lack the technical skills to get the data. This is where they meet.

I came across Ess4 hawking login data for the web shops he has hacked, the credit card numbers he has plundered from those sites and a how-to-guide that shows others how to do it.

He said: "i got many shops + tons of daily orders. i hack a shop in 3-4 hours and sell it for 100-500$."

He thanked "stupid admins" for making basic mistakes that let him break in.

Roze, one experienced hand and a spammer, said he exploited "human stupidity" rather than poor security.

He said: "That costs them money :)) I know is not fair .. but it`s the way we make money."

And, he said, when he was not relying on stupidity, he had a cadre of smart hackers working for him to break into networks. Curiously, most of these people were from Romania – a country that comes up again and again on these channels.

He said: "romanian guys are very smart. All the time they come with something new ;) they are the best hackers on earth i think."

Arrest record

These channels on IRC, and in many other places much harder to find, are where the deals are struck. It is where the spammer meets the botmaster or the credit card thief meets the money launderer.

And no one here has any fear of being caught. As one person calling himself Beelze put it: "it is not illegal to be in on an irc server. As well the law does not seem to care about it."

"There are 10.000 + users here, they trade the illegal stuff, NO ONE touches them," he said. "These are bank robberies, prolly in the top 100 biggest ever."

Stano, who I met in one very busy channel, said: "It is very difficult for them to find us, and even if they do, they have no evidence. So ... they go away :)"

He got started as a criminal staging fake ebay auctions and now he's a spammer.

"Now I have made some investments ... and I can live the rest of my life with the money I make without spamming and so on ..but now it is in my Blood," he said.

IRC encourages people to use nicknames and in the card trade channels these change on a regular, often daily, basis. To further hide themselves users join the channel via a machine a long way from their physical location. Look up their net address and you find information about a PC sitting on the domestic network of one of the bigger ISPs - more than likely a bot.

Little communication is done in the channel itself – most happens via private messages sent directly between people.

The big problem that these criminals face is not the police but each other and they are in constant fear of being ripped off by their brethren. There is little honour among these thieves.

For instance, every now and again someone will supply links to software useful to criminals. Programs can be found that crack ebay accounts, that help plan a spam run or supply background information about credit cards if you only have the number.

The vast majority of these programs are booby-trapped with viruses that try to steal the information passing through them.

This lack of trust is widespread. Beelze, who rents networks to scammers, lamented the fact that he had no way to check the reputation of those buying services.

Many pay via cracked Paypal accounts and when the real owner of the account kicks up a fuss the money is taken back. Leaving people like Beelze out of pocket.

Beelze said: "The scammer will still have its service or at least, had, up to the time it got refunded." He said he was losing thousands of euros a month this way. Those with the cracked accounts do not care because they can just use another one. Some have many thousands of cracked accounts.

"Paypal is practicly the most used by criminals," he said.

Answer the following questions.
1. What is IRC?
2. Name some jobs in the world of hi-tech crime.
3. Is it difficult to track down the chatter on IRC?
4. What is Paypal?
5. Describe the behaviour of people from the world of hi-tech crime.

SUPPLEMENTARY READING

COGNITIVE RADIOS

A **Cognitive Radio** (**CR**), as defined by the researchers at Virginia Polytechnic Institute and State University, is "a software defined radio with a cognitive engine brain".

In response to the operator's commands, the cognitive engine is capable of configuring the radio system parameters. These parameters include "waveform, protocol, operating frequency, and networking". It functions as an autonomous unit in the communication environment and frequently exchanges information about the environment with the networks it is able to access as well as with other CRs (Wipro Technologies, 2002). A CR "monitors its own performance continuously, in addition to "reading the radio's outputs"; it then uses this information to "determine the RF environment, channel conditions, link performance, etc.", and adjusts the "radio's settings to deliver the required quality of service subject to an appropriate combination of user requirements, operational limitations, and regulatory constraints". These processes have been described as "reading the radio's meters and turning the radio's knobs".

CR can sense its environment and without the intervention of the user can adapt to the users communication needs while conforming to FCC rules. Conceptually, the amount of spectrum is infinite, practically for propagation and other reasons; it is finite because of the desirability of certain portions of the band. Even the spectrum which is assigned is far from being 100% utilized, hence efficient use of the spectrum is a growing concern. CR offers a solution to this problem. A CR can intelligently detect whether any portion of the spectrum is in use or not, and can temporarily latch into or out of it without interfering with the transmissions of other users thereby efficiently utilizing spectrum. According to Dr.Bruce Fette (2004), "Some of the radio's other cognitive abilities include determining its location, sensing spectrum use by neighboring devices, changing frequency, adjusting output power or even altering transmission parameters and characteristics. All of these capabilities, and others yet to be realized, will provide wireless spectrum users with the ability to adapt to real-time spectrum conditions, offering regulators, licenses and the general public flexible, efficient and comprehensive use of the spectrum".

The phenomenal success of the unlicensed band in accommodating a range of wireless devices and services has led the FCC to consider opening further bands for unlicensed use. In contrast, the licensed bands are underutilized due to static frequency allocation. Realizing that CR technology has the potential to exploit the inefficiently utilized licensed bands without causing interference to incumbent users; the FCC released the Notice of Proposed Rule Making to allow unlicensed radios to operate in the TV broadcast bands. The IEEE 802.22 working group formed in November/2004 is equipped with the task of defining the air interface standard for Wireless Regional Area Networks based on CR sensing for the operation of unlicensed devices in the spectrum allocated to TV service.

STORAGE GROWTH SETS A FAST PACE

A decade ago a 500 megabyte (MB) photo collection was something <u>to boast</u> about. Nowadays it is more likely be a collection measured in the gigabytes.

But as our appetite for storage continues to grow thankfully so does the <u>capacity</u> of our hard drives. Hitachi has unveiled a drive which has reached the new heights of one terabyte (TB). Its drive looks like any other, but uses perpendicular magnetic recording to make space for all that data.

"The previous generation of recording technology was called longitudinal and it basically recorded the bits laying down, now we're recording the bits standing up," said Kelly O'Sullivan from Hitachi. "So if you think of it that way, you're stacking a lot more data in a shorter area, therefore you get a terabyte."

With so much data being written to the hard drive, <u>wear and tear</u> is <u>inevitably</u> a concern. So the Hybrid Storage Alliance is promoting a new laptop unit with a <u>built in</u> flash chip that stores all the data you are currently calling on. That reduces disk spinning time, increases <u>longevity</u> and has other <u>benefits</u>.

"A hybrid solution will extend your battery life. If you're on a plane for two or three hours and you don't want to stop working on a project you want to keep going - so battery is really important in a laptop PC," said Joni Clark, chair of the Hybrid Storage Alliance.

Flash memory

Some storage firms, such as SanDisk, <u>are doing away with</u> the mechanical hard drive completely and are opting for an all flash solution. Its flash drive is due out in spring.

Using flash memory has many advantages. A modified laptop using only flash memory can start up faster than an ordinary one; is less of a drain on battery power and is far less likely to suffer data loss when dropped. However, the biggest it can currently get is 32GB which says something about its target market.

"If you look at my kid, he will never use it as he is downloading movies every day," said Amos Marom, general manager of SanDisk Corporation's Computer Solutions Division. "But if you look at myself I am a road warrior, I work in airports, in aeroplanes, on trains and in hotel rooms. I am consuming about 20GB today, that's all.

Gadget friendly SD flash memory cards are also advancing <u>in leaps and bounds</u>. They come in high-capacity varieties up to a <u>staggering</u> 8GB hence SDHC – as in Higher Capacity. Those planning to use them should be aware that they run at a variety of speeds and can only be used in compatible SDHC hardware.

For reliability and <u>endurance</u>, optical storage is considered one of the best options. Holographic disks start at 300GB capacity and store data all the way through the disk rather than just on the surface. Data is written using a split <u>laser beam</u> which creates holograms in <u>the light sensitive material</u> of the disk at the point of <u>intersection</u>.

But even if you wanted to buy a holographic <u>burning kit</u> you cannot – at least not in the shops.

"The reason that it's not entering the consumer market initially is because of fairly high pricing," said Elizabeth Murphy of holographic storage maker InPhase Technologies. "The drive will be $18,000 (£9,135) list price, so that's a little bit outside the average consumer's price range. And then the media will be $180 for one disk. That's quite a bit of money, but on a cost per gigabyte perspective it's very, very attractive."

Still the cheapest is the traditional hard drive, which now comes in a new form – this is an external Serial ATA drive - the same kind that sits inside your PC. This is an improvement because it does not use the slower types of connections your computer supports.

"USB really was made for keyboards and mice and it's not really made for storage, neither was Firewire," said Conrad Maxwell, chairman of the SATA-IO Marketing Work Group. "They both require protocol translations to make them work and the drives come out with SATA, so direct SATA is faster and you get six times faster performance."

While hard drive advances are impressive, losing 1TB of data is not likely to be much fun in the future. That is why devices built around a technology known by the fearsome name of Redundant Array of Independent Disks (RAID) are becoming more popular. One such is Seagate's 1.5TB device that is actually made up of two 750GB drives. A continuous backup is created by the same data being written to both drives simultaneously. It might well save your life. Well, your digital one.

SD – super density

Firewire – последовательная шина сверхбыстрой (до 400 Мбит/с) передачи данных

SATA – serial advanced technology attachment – последовательный интерфейс ATA

Redundant Array of Independent Disks – избыточный массив из независимых дисков, RAID-массив

REMOTE ACCESS KEEPS YOU IN TOUCH

Imagine you are miles from home and you suddenly realise you have forgotten to send an important document stored on your computer. What can you do?

It is an increasing problem because we are now far more dependent on our computers than ever before - in fact a lot of us can't do our jobs or even live our lives without our PC. In pre-worldwide web times, sharing information remotely was close to a black art. Networking was in its infancy and we used floppy disks to transfer most of our data – at that time swapping files between computers was something you did with both PCs in the same room.

One of the first types of remote access was called Laplink. It enabled you to plug two computers into each other with a serial lead. It was like plugging into a modem or a printer. You could look at the files on the other computer and move them across. It was essentially a transfer facility and not much more than that.

Laplink is one of the few products that has ridden the technology wave and managed to survive the transition from MS DOS to Windows XP. Now it is the

internet that has been pressed into service to make our life easier. Today there are a host of services that allow you to go online and connect to a computer far away.

One of them is LogMeIn which allows you to access your computer from any web browser anywhere in the world. It creates a virtual desktop that you can access, display and use in a web browser.

Your remote computer contacts your home computer, wakes it up and promptly takes it over. The remote machine completely controls the home machine, but the only information being sent across the internet is the mouse, keyboard and screen data. This also means you can use any of the applications already on your home computer, remotely.

Michael Simons of LogMeIn says: "You may have a contract on a USB stick, you're in an airport lounge and it doesn't have Microsoft Word but you have it on your home or office computer. With our product you can simply plug the USB stick into the computer you're sitting at and then use Word on the remote machine."

You view the data on the home computer until you are finished and then you break the connection – the only downside is that your home computer is still connected to the internet. For some people this creates security worries.

Rupert Goodwins, Technology Editor of ZDNet UK says: "If you're going to have to access your computer remotely then that computer has to be there all the time. So the internet's on, the computer's on – there's a way into your computer. It's got security, so it's not an open door, but if you do not set it up properly it can be quite a security gap".

Microsoft built remote access into Windows XP. It will also be part of Vista and the forthcoming version of Mac OS X for Apple users.

Mr Goodwins says once people start using remote access it becomes addictive. "We're going to start to get good internet bandwidth and infrastructure everywhere we go, because we won't be able to work without it. So if we go to places that don't have internet infrastructure they'll suddenly be provided with all the things we've got access to. This could be one of the big things that breaks down the digital divide."

Bandwidth – полоса (диапазон частот, передаваемых через устройство или среду)

RADAR

The term 'radar' was coined in the 1930s and is an abbreviation for *RAdio Detection And Ranging*. The initial purposes of detecting objects and range measurements nowadays are only part of a radar's function, as radars also serve for tracking an object's movements and whereabouts, its identification and the determination of certain properties.

The Principle In A Nutshell

Radars consist of a transmitter, a receiver, one or two antennae and lots of signal-processing circuitry. This is a basic overview of how the principle of radar works:

1. The transmitter produces a signal which is radiated through the antenna.
2. The signal is an electromagnetic wave which is capable of propagating through space.

3.   If an object happens to be in the way then part of the signal is reflected and finds its way back to the radar.

4.   The receiver picks up this echo, using the transmit antenna or a dedicated receiving antenna.

5.   The signal processor detects the echoes, sorts them out from among noise and other types of interference, takes measurements with regard to the object's location in space, its speed and perhaps some more characteristics, and prepares them for output to a display or some remote command post.

The principle can be compared to finding one's way through a forest at night with the help of a torchlight. The torchlight contains the light bulb (the transmitter) and a reflector (the transmit antenna) which is used to shape the beam and direct it into the area of interest. The 'signal' is the beam of light which is capable of propagating through the atmosphere. Objects like trees and grass reflect the light, and part of it is picked up by the eye (the receiver). Finally, the brain controls the whole process, performs the signal processing and avoids its owner tripping over a fallen tree.

General Aspects

Behind the scenes, radars are rather complex devices which bring together scientific areas like mathematics, electronics, optics, mechanics, fluid dynamics and many more. Main application fields for radars include weather forecasting, air surveillance, navigation and collision avoidance, air traffic control, law enforcement and warfare, astronomy, geodesy and ecology.

Within a single radar, the units of measure usually stretch over tens of orders of magnitude. The transmitter may operate at megawatts of power for the duration of a microsecond whereas the receiver measures picowatts. The signal in the air can have a frequency of several hundred GigaHertz while distances in the millimetre range are being measured.

The radar principle is also used in optics and acoustics (e.g: LIDAR, laser radar) and sonar (acoustic-sounding). Lidar finds its most prominent application in detecting chemical substances in the atmosphere. Sonar[1] is used by navies and commercial fleets all over the world for finding underwater targets and fish. Ultrasonic devices used in medical diagnostics also employ the radar principle in order to produce images of a baby within the mother's womb or a Doppler profile of the bloodstream within a vessel.

The signals used in radars are electromagnetic waves just like light. There are only two major distinctions which make it hard for the lay person to gather the similarity:

• The wavelengths are different. Light has a wavelength of some minute fraction of a millimetre, whereas radars use wavelengths between 1mm and 100m.

• Humans don't have sensors for these wavelength bands. Our senses only cover the optical band (which is perceived as light) and the far infrared which is perceived as heat. Radar wavelengths are some 10 orders of magnitude greater than those of infrared radiation. In order to be able to *see* a radar signal, our eyes would have to grow by the same factor. Eyes this big might prove a little cumbersome - even perhaps impractical.

Apart from these two points, radar signals share the same properties as light. They propagate through space and Earth's atmosphere, are absorbed by different kinds of matter, get reflected from other kinds of matter and undergo diffraction at objects of particular shapes and dimensions. The entries Over The Horizon Radar, How Stealth Works and Advanced Electronic Countermeasures look into some interesting consequences of this.

However, one distinctive difference between light and typical radar signals is that longer wavelengths can easily propagate through precipitation. Hence, radars are able to look through fog, clouds and snow. Some wavelengths do exhibit significantly stronger attenuation in the atmosphere, especially when molecular resonances of oxygen or water molecules are excited. But even these areas of the electromagnetic spectrum are used by radars: weather radars and wind-profiling radars use them in order to look out for clouds and to track hurricanes. Radars can also take a look *into* the earth – although not very deep –to detect buried mines.

All radars are composed of the items listed below. Their operation is organised in a processing chain and hence it is the weakest part that defines the systems capabilities.

The Transmitter

Transmitters are built around semiconductors (often contained in MMICs, millimetre-wave integrated circuits) or powerful vacuum tubes. The latter are rather complicated and sophisticated devices and often carry weird names ending in '-tron', such as Amplitron, Magnetron, Carcinotron, Stabilitron or Klystron.

Owners of a microwave oven are also owners of a magnetron. The fact that microwaves can heat up food was discovered by serendipity, when during the 1940s a radar researcher was astonished to see that a chocolate bar was melting in his trouser pocket while he was performing experiments with an unshielded magnetron[1].

The Antenna

The radar antenna serves as the coupling element between the wiring in the radar hardware and free space. Radar antennae can be as small as a thumbtack or as big as a 30-storey building, depending on their operating frequency and beamwidth.

The Receiver

The receiver's task is to pick up the echo that was bounced off a target, filter out unwanted parts outside the radar's bandwidth, amplify the rest and feed it into the signal processor for further analysis. A good receiver is a radar's best defence against *noise*, its toughest enemy.

A receiver must be very sensitive in order to pick up weak echoes from far away. But usually it is located near the transmitter which can easily 'blind' or even destroy it by 'spillover' leaking into the receiver's input circuitry. In a pulsed radar, damage can be avoided by using a Transmit/Receive-Switch or *T/R switch* that disconnects the receiver's input from its antenna while the transmitter is operating. In a Continuous Wave Radar, the transmitter operates all the time and receiver protection is only feasible by blocking the frequency that is currently used. Both measures do fulfil their purpose but at the same time they introduce some problems of their own: they produce blind ranges and blind speeds.

Until not long ago, travelling wave tubes (TWT) were the mainstay of receiver construction. Like the -tron devices mentioned above, their inner workings are rather complicated as they are built around some chamber or structure where strong magnetic fields or electron beams interact with low power, high frequency signals. During the 1980s, TWTs were gradually replaced by semiconductors.

The Signal

The signal is what the radar transmits into space. A wide variety of types is available, and perhaps more than all the hardware components, the signal is what determines the quality and capabilities of a radar. The most powerful radar, equipped with an ultra-low sidelobe antenna of incredibly high gain can be *blind* at the most important range or target speed if the signal was chosen wrong. Some signals are likely to produce 'angels' and 'ghosts' on a screen – things that really make a radar operator's life interesting. More often than not, a single type of signal will not meet all the requirements, and fierce discussion about necessary expenditures ensues between manufacturer and customer.

The Signal Processor

The Signal Processor is the central element of a radar. It has to decide whether an echo really *is* an echo and whether or not it is worth being reported and displayed. This is not a simple task, as there is much natural noise around, and in the case of military applications there is man-made interference too.

The System

A collection of sophisticated components is a precondition, but not a guarantee, for a good radar. The first step during the design phase is to determine which part of the electromagnetic spectrum is to be used, followed by the selection of the signal that is most appropriate for the purpose in question. All this needs to be composed into a system that is more than the sum of its parts. There are only a few things that a radar *cannot* do, and the easiest way to find these is to look into the requirement specifications written by the customer.

RADAR TECHNOLOGY - SIGNAL PROCESSING

The main task of a radar's signal processor is *making decisions*. After a signal has been transmitted, the receiver starts collecting returns, with those originating from near objects arriving first because time of arrival translates into target range. The signal processor places a raster of *range bins* over the whole period of time, and now it has to make a decision for each of the range bins as to whether it contains an object or not.

This decision-making is severely hampered by noise. Atmospheric noise enters into the system through the antenna, and all the electronics in the radar's signal path produces noise too. The common metaphor is to speak of a 'noise carpet', 'noise floor' or 'grass' and it is easy to understand the metaphor by taking a look at a radar scope.

Even if atmospheric attenuation can be neglected, the return from a distant object is *incredibly* weak. Target returns are often no stronger than twice the average noise level, sometimes even buried under it. It is quite a problem to define a threshold for the decision whether a given peak is noise or a real target. If the threshold is too high then existing targets are suppressed –that is, the probability of detection P_D will

drop. If the threshold is too low then noise peaks will be reported as targets and the probability of false alarms P_{FA} will rise. A common compromise is to have some 90% probability of detection and a false alarm rate of 10^{-6}. This means that a real target will be detected in 9 out of 10 attempts, and that the radar is allowed to produce a single false alarm over a period of 24 hours.

A clever means to maintain a given P_{FA} is known as CFAR, for *Constant False Alarm Rate*. Rather than keeping the threshold at a fixed point, CFAR circuitry inspects one range bin after the other and compares the signal level found there with the signal levels found in its neighbouring bins. If the noise level is rather high in all of them (because of precipitation) then the CFAR circuit will raise the threshold accordingly.

Further tasks of the signal processor are:

• **Combining information**. Secondary Surveillance Radars like those located on airports can ask an aircraft's transponder for information like height, flight number or fuel state. Pilots may also issue a *distress* signal via the transponder. The ground radar's signal processor combines this data with its own measurements of range and angular direction and plots them all together on the appropriate spot on the scope.

• **Forming tracks**. By correlating the data sets which were obtained in successive scan cycles, the radar can calculate a *flight vector* which indicates an aircraft's speed and expected position for the next scan period. Airport radars are capable of tracking hundreds of targets simultaneously, and flight safety depends heavily on their reliability. Military tracking radars use this information for gun-laying or guiding missiles into a calculated collision point.

• **Resolving ambiguities** in range or Doppler measurements. Depending on the radar's pulse repetition frequency (PRF), the readings for range, Doppler, or even both, are ambiguous. The signal processor is aware of this and selects a different PRF when the object in question is measured again. With a suitable set of PRFs, ambiguities can be eliminated and the true target position can be determined.

• **Ground Clutter Mapping**. Clutter is the collective term for all unwanted blips on a radar screen. Ground clutter originates from buildings, cars, mountains and so on, and a clutter map serves to rise the decision threshold in areas where known clutter sources are located.

• **Time and power management**. Within a window of some 60°x40°, phased array radars can instantly switch their beam position to any position in azimuth and elevation. When the radar is tasked with surveying its sector and tracking dozens of targets at the same time, there is the danger of either neglecting part of the search sector or losing a target if the corresponding track record isn't updated in time. Time management serves to maintain a priority queue of all the tasks and to produce a schedule for the beam-steering device.

Power management is necessary if the transmitter circuitry runs the danger of overheating. If there's no backup hardware then the only way of continuing regular operation is to use less power when less power is required, say, for track confirmation.

• **Countering interference**. Interference can be a) natural, or b) man-made. Natural interference can be heavy rain or hailstorms, but also weird propagation

conditions like *ducting*. Ducting is the same to a radar as is a *mirage* to some lost soul in a desert: the radar beam bounces off the boundary between two layers of air at different temperatures.

Man-made interference, if created on purpose, is also called *jamming* and is one of the means of Electronic Countermeasures. Unintentional man-made interference is a problem when radars of the same type are deployed without proper planning and their signals get into each other's ways. In particular, Automotive Radars have to deal with the latter type of interference.

In summary, the signal processor is the *brains* of a radar. Usually, it is represented by a very capable computer with Megabytes of software and as the above list shows, a lot of things keep it busy.

THE HISTORY OF RADAR

The early history of radar is closely connected with warfare - only relatively recently have civilian applications stimulated development of radar technology and attracted some public attention.

The Very, Very Early Days

The oldest radar system was developed *millions* of years ago and is still used worldwide: it is the ultrasonic sensor of a bat. Bats emit a short 'cry' from their noses, receiving the echo with a set of two antennae which happen to be ears. True, a bat's radar doesn't use electromagnetic rays, but the working principle is the same as that of a modern radar, with a chirped signal, target-tracking by Doppler estimation, PRF agility, terrain avoidance function, and fine angle measurement based on the monopulse principle.

The oldest radar warning device also was developed millions of years ago. Tiger moths (which frequently appear on bats' menus) are equipped with ears that can detect and jam the ultrasonic signal of a bat, and they have also developed tactics to evade a bat's attack. Thus, Electronic Combat also came into being a long time ago.

The Early Days: Experiments and Discoveries

Mankind first became involved in this radar business around the beginning of the 20th Century. In 1904, Christian Hülsmeyer (1881–1957) received a German patent (as well as others in the UK, the USA and elsewhere) for the *Telemobiloskop*, or Remote Object Viewing Device. The device achieved ranges of 3000m against ships, even before amplifier tubes were invented. It was offered as an application to prevent ship collisions, but didn't attract any customer interest and fell into oblivion. Thus, radar was invented earlier than Sonar (the acoustic equivalent used in seafaring), which was developed in the aftermath of the Titanic catastrophe of 1912.

RC Newhouse of Bell Labs got a patent in 1920, and his experiments performed throughout the decade eventually led to the radio altimeter which became operational in 1937.

In 1922, Guglielmo Marconi gave a speech which demonstrated that he had a clear idea that it was possible to detect remote objects by radio signals. But it was not before 1933 that he was able to show a first working device.

In 1925/26, the American physicians Breit and Tuve, as well as the British researchers Appleton and Barnett, performed measurements of the Earth's ionosphere, using a pulsed radio transmitter which could be described as a radar.

It was 1928 when HM Signal School of the UK received the first patent on Radio Location, credited to L. S. Alder.

In 1930, a team of engineers from the US Naval Research Lab performed measurements of a radio antenna, and more or less by serendipity they independently discovered radar. Their radio link happened to stretch across an aircraft landing strip, and the signal quality changed significantly when an aircraft crossed the beam.

In 1933 when Hitler took over power in Germany, the German Kriegsmarine (Navy) started research into what they called *Funkmesstechnik*, or remote radio measuring technology.

Research in Russia began in 1934, but was somewhat hindered by quarrels between different authorities. However, one of the earlier devices was a success, with a 70km detection range against aircraft.

In 1935, Sir Robert Watson-Watt (1892–1973) sucessfully demonstrated the detection of an aircraft by a radio device, during the so-called Daventry Experiment. An order for full scale development of radar was issued later that year, after it was realised that sound locators (which at the time were the only means of detecting inbound bombers) could not provide adequate reaction time. This was the starting point of the world's first operative radar network, called Chain Home or *CH* in short. The Chain Home became operational in 1937, well before the war broke out. Bombers could be detected at ranges of 150km and more. Sir Watson-Watt has often been credited with the invention of radar – something which is obviously, at best, debatable.

Also in 1935, a French ship was equipped with a collision avoidance device of local fabrication. A land-based device, the *barrage electronique* was tested in 1936 and was used in the early days of WWII.

By 1939, the following countries had more or less rudimentary, but operational radars in their inventories: Britain, France, Germany, Hungary, Italy, Japan, the Netherlands, Russia, Switzerland and the USA. To some extent, the technology behind these devices can be described in terms of today's buzzwords, such as Continuous Wave Doppler, conical scan, Bistatic and Spread Spectrum radars.

World War II

During the Battle of Britain (1939–1941), significant success was attributed to the Chain Home network which detected incoming air-raids and provided information to guide interceptors to home in on the bombers. Detection reports were sent via landline to 'filter rooms' which coordinated the efforts of the short supply of interceptors and thus made up a formidable force multiplier. The CH was never really understood by the Germans, and no serious attempt to jam or destroy the whole system has been reported. The radar on the Isle of Wight was a part of the system.

In 1941, radar missed a chance to significantly change history. There was an initial system deployed on a hill on the pacific island of Hawaii, close to Pearl Harbour. The operators actually detected the Japanese attack squadrons and reported their observation, but none of their superiors believed them because they were deemed inexperienced[1]. Had the reports been acted upon then the whole attack could have been turned into a failure.

On 17 February, 1942, a <u>raid</u> was undertaken to capture the essential parts of a German Würzburg radar located near Bruneval, Normandie. The parts were evaluated and showed that the device could only work in a narrow frequency range. Further reconnaissance revealed that all German radars were operating in no more than three major frequency ranges, and thus were prone to jamming. The first operational use of *chaff* (aluminium strips which are precisely cut to a quarter of the radar's wavelength) took place in July 1943, when Hamburg was subjected to a devastating bombing raid. The radar screens were cluttered with reflections from the chaff and the air defence was, in effect, completely blinded. Chaff (also called 'window' by the RAF, or *Düppel* in German) had been discovered independently by the British and the Germans – neither side knew of the other side's knowledge. The Germans were aware of their vulnerability but found themselves incapable of making their radars tunable within reasonable amounts of time, and they hoped that refraining from using Düppel themselves would enable it to be kept secret.

<u>Stealth Technology</u> was invented in the 1940s, when German submarines suffered severe losses because they were detected by airborne radars once they were on the surface. Technicians found that a mixture of graphite and rubber could substantially weaken the radar echoes if it was applied as a 'Schornsteinfeger' ('chimney sweep') coating on the submarine's hull. However, this only worked while the subs were in the dry dock. Once the anti-reflective coating was wet from sea water, it was the water and salt layer which reflected the radar signals.

During the war, higher and higher frequencies of the electromagnetic spectrum were put to use. Researchers started with the first experiments at some 10MHz, the Chain Home operated around 20MHz (with later extensions up to 70MHz), and the bulk of air surveillance and tracking radars worked between 200MHz and 800MHz. The refinement of 1921's cavity magnetron transmitter device by Randall and H. Boot in 1940 was a significant breakthrough. The <u>magnetron</u> was the heart of the American H2S bombing radar which operated at 3GHz. Its Plan Position Indicator (PPI) screen showed a map of the underlying terrain with a resolution that was hitherto unheard of. This type of magnetron wasn't known in Germany, and 3GHz was far beyond the frequency range of their interceptor and warning devices. In fact, a conference between Hitler's top military ranks and some researchers had come to the conclusion that 800MHz was enough and that it was questionable whether signals at frequencies above 1GHz could propagate through the atmosphere at all. Rated 'top secret', the H2S radar was not to be used over Germany, for fears that its carrier might be shot down, letting the magnetron fall into hostile hands.

But then in spring 1943, a bomber was shot down near Rotterdam and the H2S radar with its magnetron was a big surprise to the Germans. Significant effort went into the repair, study and reproduction of the device, but only a few examples of what they called the 'Rotterdamgerät' became operational by the end of 1944.

At the end of the war, most of today's technologies had already been put to use, although they relied on contemporary technical means. There was a chirp radar in production, the monopulse principle was invented and even a <u>Synthetic Aperture Radar</u> already existed. The Chain Home was used to detect the V2 <u>rockets</u> after they left their launch sites, hence it can also be called the world's first Anti-Ballistic

Missile (ABM) radar system. Among the few ideas which were born later than 1945 are the phased array antenna technology and the concept of multistatic radar.

After WWII

Having lost the war, Germany was ejected from the radar business. Until 1950, any research into the field of radar was forbidden. Lots of researchers emigrated, following in the footsteps of Wernher von Braun and others.

Radar was kept highly secret throughout WWII, and only in 1946 was it published that an American device had successfully measured the distance to the moon, which is a round trip of some 770,000km. Even later, it became known that a Hungarian device had already done the same thing in 1944.

It is very hard to find any remaining WWII radar equipment in museums today. Even though radars aren't as impressive as 50-ton battle tanks, every single radar had an influence comparable to a whole battleship, so some sense of the impact and significance of radar has been lost. The Online Air Defense Radar Museum features a good selection of American radars. The Historical Electronics Museum, Linthicum, Maryland (close to Baltimore Washington International Airport) has inter alia an SCR-584 tracker like the ones used to down the majority of V1 flying bombs. It also has an SCR-270 like the one that detected the Japanese assault force on Pearl Harbour. The Imperial War Museum in London has a single exposure of a German Würzburg tracking radar. The Deutsches Museum in Munich as well as the Musee Radar at Douvres, France, feature a Giant Würzburg. The *Auto- und Technik-Museum* in Sinsheim-Steinfurt (close to the A6 near Heidelberg, Germany) features none, and so does the National Air Museum at Wright Paterson, Dayton, Ohio. There may be displays in other museums, but this researcher is not aware of them.

The Cold War (1945–1989)

The Vietnam War (1961–1975) saw the first use of Anti-Radiation Missiles (ARM) which were carried by the F-105 Thunderchief, also affectionately known as 'Thud' or *Wild Weasel*. Once a radar warning receiver inside the aircraft detected the signal from a ground-based acquisition or missile guidance radar, the seeker-head of the ARM was cued – and after lock-on, the missile would home in on the source of the signal (the radar itself) and destroy it.

Desert Storm (1991)

Suppression of Enemy Air Defense, or SEAD was the first mission to be carried out by coalition forces in order to drive out Iraqi forces from occupied Kuwait. These SEAD missions employed the whole spectrum of Electronic Combat measures in order to pave the way for bombers and ground forces.

Modern Days

The layperson may know radar only as an invisible threat when speeding on a motorway, because police radars are employed as a means to enforce law. However, radar is also on its way to be used to their advantage as automotive radars are now entering the market. They are used to automatically keep a set distance from the car in front, and to warn the driver when obstacles are encountered in his lane.

These days, no major airport can be operated without a radar. Flight controllers in the tower use radar to keep track of dozens of aircraft which are circling in the waiting loop and to schedule them for landing. The public is only made aware of this

when a radar is defective and hundreds of flights are cancelled or redirected to other airports and local hotels are unable to accommodate any more guests as a result.

The Future

Many of the first devices that researchers played with were bistatic radars (this is when the transmitter and receiver do not share the same location but are set up at two different places). These bistatic radars are getting new attention, obviously with much more highly-developed <u>signal processing</u> working behind the scenes. The extension of the principle, using a transmitter plus several interconnected receiving sites, is called <u>Multistatic Radar</u> and is also subject of ongoing research.

At the time of writing, <u>Passive Radar</u>, imaging radar and *Multi-coloured* radars are the latest buzzwords that are circling around developers' laboratories. Passive radar relies on background illumination by whatever source happens to be there. Imaging radar is what the name implies – the results are displayed as if they had been gathered by a camera and with comparable resolution. Multi-coloured radar is another word for ultra-wideband radar which is able to extract much more information out of the scene it sees – it is rather like how colour television must have seemed to a world familiar with only black-and-white.

However, these current cutting-edge activities are also mankind's first steps to imitate the capabilities of sensors that nature developed millions of years ago.

GREEN PIGMENT SPINS CHIP PROMISE

An unpopular pigment used by artists in the 18th Century could lead to more energy efficient, faster computers.

Cobalt green, as it is known, has been tested by a US team who believe it could be used in "spintronic" devices. Spintronics involves manipulating the magnetic properties of electrons to do useful computational work. Cobalt green may be useful for building working devices as it can be used at room temperature, unlike many other materials which must be supercooled.

"The big challenge is to develop materials that can perform these kinds of functions not just at cryogenic temperatures but at practical temperatures," said Professor Daniel Gamelin of the University of Washington in Seattle, one of the team that carried out the work.

Cobalt green, sometimes known as Rinmann's green, is a mixture of zinc oxide and cobalt. The semi-transparent pigment was developed by the Swedish chemist Sven Rinmann in 1780. The colouring never found favour with artists as it was expensive and created relatively weak colours. However, the material could be useful in spintronic devices because of its magnetic properties. Conventional electronics rely on the movement and accumulation of electrons to carry out calculations or to store data. In addition, spintronics uses the spin of electrons – detected as a weak magnetic force – to increase the computational power of a device. Spintronic devices, in theory, should be much quicker than conventional electronics and require much less power. The technology is already used in some hard discs and could eventually be used for sensors and computer memory.

A goal of spintronics is to develop a semiconductor that can manipulate an electron's magnetism. Semiconductors are used to manufacture microchips, at the

heart of all computers and many other electronic devices. As computers have become faster, chips have become smaller. But manufacturers recognise that conventional chip fabrications techniques will eventually reach a physical limit. Spintronics offers a potential solution. To create a useful spintronic device the semiconductor must be magnetised and remain stable at room temperature. Researchers have proposed that the best way to create material like this is to incorporate a magnetic element into a traditional semiconductor such as silicon. Until now, most attempts to do this have only shown useful spintronic properties at low temperature, typically around minus 200C. This is much too cold to be useful in a working device. Cobalt green appears to work at more useful temperatures.

"The breakthrough with the materials we tested is that they exhibit their magnetic properties at room temperature," said Professor Gamelin.

To test the antique pigment the researchers processed zinc oxide, a simple semiconductor material, so that some of the zinc ions were replaced with ions of magnetic cobalt. The process is known as "doping". The cobalt ions were then aligned by exposing the semiconductor to a zinc metal vapour. The alignment causes the material to become magnetic. The magnetism continued when the material was warmed to room temperature and when the exposure to the zinc metal vapour was stopped. When the material was heated further the magnetic properties disappeared.

"This work shows there is a real effect here, and there is promise for these materials," said Professor Gamelin.

However, the research is still in its early stages. To be of use to chip-makers the technique must be shown to work using common semiconductor material.

"The next step is to try to get these materials to interface with silicon semiconductors."

YAHOO TELLS MICROSOFT: 'BUY US'

Yahoo said the "For Sale" sign is still on its front lawn and that Microsoft should buy the company.

The internet portal's co-founder and CEO Jerry Yang made the comment despite the fact Yahoo rejected a $33 (£21) a share offer from Microsoft back in May. Mr Yang's suggestion also came hours after Google pulled out of an internet advertising partnership with Yahoo.

"To this day the best thing for Microsoft to do is buy Yahoo," said Mr Yang. "I don't think that is a bad idea at all, at the right price whatever that price is. We're willing to sell the company," he told a packed ballroom at the Web 2.0 summit in San Francisco.

During the on stage conversation in front of a standing-room only crowd, Mr Yang was asked why the company did not take the $33 a share offered back in the summer. The company's share price closed Wednesday below $14 (£8.80) a share.

"They walked away from a public offering and we were ready to negotiate. We wanted to negotiate a deal. We felt we weren't that far apart. At the end of the day, they withdrew and they have since been clear about not wanting to buy the company," explained Mr Yang in a rare public appearance.

Microsoft did however come back and offer to buy the search part of Yahoo, but a deal was never struck. Again Mr Yang said the offer then was not good enough but he still remained open to persuasion.

"As far as a search deal goes, we are open-minded about it. The last time we felt the deal was not a good one for the company but that doesn't mean we won't do one."

When asked if any negotiations were pending with the software giant, Mr Yang said "There is no new news."

Microsoft declined to comment. And when quizzed about a possible deal with AOL, Mr Yang played coy with his host John Battelle.

"Buying AOL? I can't talk about that, John. If I told you I would have to kill you."

While Yahoo is still holding the door open to Microsoft, Google closed one earlier in the day on a deal the two companies had struck up over search advertising. After four months of scrutiny from the Department of Justice, Google decided to back out of the agreement it had made to provide advertising around the internet portal's search results. It had been estimated that the venture would have been worth around $800m (£500m) a year to Yahoo.

"Pressing ahead risked not only a protracted legal battle but also damage to relationships with valued partners," said Google's chief counsel David Drummond.

Mr Yang said he was "disappointed that they [Google] didn't want to defend this deal." But he felt that in his mind, the government scuppered it.

"I really thought the government in this case does not understand our industry. They have a market definition that I think is too narrow and I think things like this tend to have unintended consequences for our entire industry. So I clearly don't agree with what the viewpoint is, but they are the government and they can decide on these things."

Mr Yang pointed out that the Google partnership was not crucial to its bottom line and that it was "incremental" to its overall growth plans.

A HANDS-ON PREVIEW OF WINDOWS 7

Microsoft has released an early preview copy of its new operating system, Windows 7.

The release follows in the wake of Vista, which has been subject to fierce criticism from a number of users. When Vista launched in January 2007, many complained that it ran slowly and failed to work at all with some programs and devices. Corporate customers have been slow to switch from Windows XP to Vista, although Microsoft said that the operating system had an unfair press, and that it enjoyed record sales.

Despite this Microsoft has extended the life of Windows XP so PC makers can continue selling it to those that do not want to upgrade. Windows Vista took more than five years to develop but Windows 7 is likely to arrive within a couple of years.

Microsoft's VP, Steven Sinofsky, described Windows 7 as an "exciting new version" and claimed it would deliver a more personalised experience. With Windows 7, Microsoft has added a range of new functions including:

- A new taskbar to give more rapid access to files and programs.

- A feature called HomeGroup, allowing users easy sharing of data across PCs and other devices in the home.

- Support for devices such as cameras, printers, and mobile phones with a product called Device Stage offering a single window to manage tasks for each device.

- Windows Touch - software for touch screen devices that enables users to use different gestures to perform tasks.

- Improvements to some applications, such as MS Paint, and Calculator.

Microsoft's chief software architect Ray Ozzie said Windows 7 would be evolutionary rather than revolutionary. The new operating system is scheduled for release in 2010 and the advance code still had limited functionality. A widely released public trial, or beta, version is expected to be available in early 2009.

To test Microsoft's claims BBC News gave a copy of the early version of Windows 7 to Alex Watson, editor of Custom PC. The early version made a good impression on Mr Watson, who described it as "quick, snappy, and reliable".

Given the popularity of Windows XP and the plethora of issues that came with the launch of Windows Vista, Microsoft may have a tough job persuading users to upgrade - noted Kelvyn Taylor, editor of Personal Computer World.

"The problem is that they [Microsoft] have to overcome the damage that Windows Vista caused. And that will be an uphill struggle. People are comfortable with XP, so there will have to be something significant in Windows 7 to persuade people to migrate over, " he said.

"Pricing, response time, and reliability are all issues that will need to be addressed. If Microsoft does that, then they're in with half a chance. Otherwise Windows 7 will end up as little more than Vista 2 Mark II."

THE GAME GIRL

Nancy Smith, who got her career break as the "token woman," is now riding high in a world dominated by men.

For Ms Smith it has mostly always been so as she worked her way up the ladder from selling spreadsheets and word processing packages to becoming one of the most influential women in video gaming. She has a track record going back nearly a quarter of a century with Electronic Arts (EA), one of the most dominant players in the gaming space. Her time with the company has included executive roles in publishing, sales, and distribution as well as that of vice president and president of the The Sims Label, the best selling PC franchise of all time with over 100 million sales. Just last month she embarked on a new, as yet undefined, path within the company. While that is being fleshed out she will look after special projects for The Sims, which lets users create and control the lives of simulated people.

"I was in the business application area when Electronic Arts launched. It was then I became interested in the idea of entertainment and games and frankly it wasn't a hard decision to make: games or spreadsheets?"

The decision was made even easier by her upbringing. "I grew up in a family that played a lot of games, but it was board games and card games," she said. But in

those early days selling spreadsheets, she found herself involved in very different games – a community that was almost illicit in its nature. "In the 70's in San Francisco I had several good friends who were in the tech business and they were selling mainframe computers. At lunch we would go over when the mainframes where shut down from all the accounting processes and we'd bring our lunch and play games. It was the same programmers and analysts who were running payroll for Wells Fargo bank that were creating these games we would play."

Today she can hardly believe how far the industry has progressed since 1984, when she started at EA as Western Regional sales manager.

"It was all independent dealers. The first year we started shipping games, there were 5,000 independent mom and pop dealers. No one even owned two stores at that time. Then retailers like Babbages started to grow with multiple store locations. In that retail climate, our customers were those store managers and store owners who played our games and sold to the converted."

Slowly the industry evolved and bigger retailers started to spring up. That then presented other hurdles.

"When it got really challenging I was six or seven years into it. It was when the industry started moving into mass merchants and different types of retail record stores where you were dealing with traditional retail buyers who were looking for specific business metrics. The problem was they really didn't have a sense of who the customer was. They had to believe that we as an industry would drive consumers to their stores."

Of course, Ms Smith noted that today the business of selling games is a lot easier, with third quarter sales up 60% on last year. "For many years now it has been one of the fastest growing aisles in Wal-Mart, in Target, in Best Buy. So those retailers understand how valuable game entertainment is to driving footsteps and driving growth and profit for them."

While the sales figures have changed much, the demographics haven't. The face of the industry today remains largely male with just 20% of females making up the workforce and only 3% employed as game programmers according to Game Developer Magazine. When Ms Smith first started out, that figure was a lot less.

"I spent the first 15 years of my career being the only woman in every meeting I ever attended whether it was with external partners, art, retail, licensing groups, design meetings outside of EA. There were just not a lot of women in the business."

That turned out to be a boon for getting her first job, in the American Express card division.

"They were given a mandate that they had to hire one woman and one minority," she said. "I was the woman they hired and I joined with a black man who was the minority candidate for them."

Far from being insulted, Ms Smith used the situation as an ice-breaker.

"It was a wonderful jumpstart for my career. I would embrace the opportunity and I would introduce myself as 'I'm Nancy Smith, the token woman in the Western Region of American Express card division.'"

So what of the future? For Ms Smith it's a new executive position within Electronic Arts as it downplays talk of a takeover following a dismal share price amid

a gloomy economy. For The Sims label, it is a new version of the game which is expected next year along with a Hollywood movie. For the industry as a whole, Ms Smith sees a major shift that was started by The Sims.

"It's about connecting consumers. It's not just creativity, but it's the community element that has always been there with The Sims. Now people want that in all their entertainment. They want to be connected. They want to play with other people. They want to share. And I think that is really transforming the gaming business and the entertainment business."

FERRARI TEST DRIVES SUPERCOMPUTING

As computer power goes up and costs come down more and more firms are turning to small-scale supercomputers to help them get the job done. David Reid visited Ferrari's headquarters in Maranello, Italy as it put Microsoft's high performance software through its paces.

Supercomputers are traditionally thought of as a bookish breed, hiding themselves away in universities puzzling over astronomical data or decoding genomes. But in 2000 the list of the world's leading supercomputers revealed an interesting trend. More than half of the top 500 supercomputers in the world were in the service of businesses. The trend appears to be continuing, so much so that Microsoft has moved into the market with a version of Windows for what it calls High Performance Computing (HPC).

Microsoft has teamed up with high performance car manufacturer Ferrari to promote the software giant's goal of bringing supercomputing to the masses.

"Traditionally, HPC has been utilised by the most specialised markets and specialised users," said Vince Mendillo, director of HPC marketing at Microsoft.

"By having a common platform like Windows, that is capable of doing this high performance computing and number crunching and dealing with large data sets," he said. "Now more and more computer problems can be solved by a larger population of people who traditionally wouldn't have access to that technology."

Windows HPC Server 2008 already runs on the Cray's CX1 hardware that was unveiled in September. It is reported that units from HP, IBM and Dell will follow. Supercomputing software delegates, distributes and schedules complex calculations across the stacks of processors.

Microsoft's declared aim is not to compete with Linux as the supercomputer operating system, but to offer the market an OS that works well with the Windows customers are likely to be already using.

Ferrari is keen to use the smaller supercomputers because it hopes they will help it speed up car production. Like so many products, high performance cars were once handcrafted and took an age to get through the processes of design, testing and manufacture. Now the design process is streamlined by high performance computers which speed the pathway from drawing board to road or race-track. This means car designers can increase turnover and profits by using computer simulation in place of research tools such as wind tunnels, which can cost a fortune in time, manpower and money.

"We simulate the flow of the wind outside the car and the engine simulation, so the flow of the gases inside the engine," said Piergiorgio Grossi, head of IT at Ferrari.

"We want to do more with less, even in Formula One, because budgets are not increasing, and you know about the financial crisis," he said. "We want to carefully use all of the resources that we have to do as much as we can."

THE PITFALLS OF BIOMETRIC SYSTEMS

How easily do biometric ID systems fall down, and can they be fooled completely? Dan Simmons asks if being unique is enough to keep us safe.

Biometric ID systems rely on one central idea - that we are all unique. That notion appeals to our own vanity. It is tempting to think biometric systems are the perfect way to identify us. But it is not that straight-forward. Consider fingerprints. Manual workers can have theirs rubbed off and swimmers need to wait until their fingertips dry out to be identified. It is also possible to lift and copy prints.

There are cultural concerns too. In Japan people tend to dislike the idea of touching something, so some Japanese ATMs analyse the palm of the hand while it is held over a scanner.

The introduction of face recognition scanners at Manchester Airport in August in a trial to speed up passport queues revealed some of the shortcomings of relying on biometrics. Face recognition uses the contours of the face and the relative distance between the eyes and nose to spot people.

"You can tune the system so it's less fussy about getting an exact match to the biometric data on record," said Ant Allan of analysts Gartner. "Or you can make it demand a more exact match, so you can make it stronger security. That means that users probably have to provide a number of samples, which reduces the convenience. There is the potential for error and user frustration because of that."

The most common error biometrics systems make is when they say "no" instead of "yes" – a false negative. Far more dangerous is a false positive, where the system gives a thumbs-up to an imposter.

"Some of the technologies are known to be vulnerable," said Ant Allan adding that there had been reports of iris recognition systems being fooled by digital photographs. "I think this stresses the sensitivity that this kind of technology has".

"That might depend upon the complexity of the system," he said. "The higher-end systems certainly have techniques where they wouldn't be fooled by that, but there are certain systems deployed in commercial and government use where these kinds of attacks can succeed."

The latest iris and fingerprint systems now look for live subjects and are much harder to dupe.

Voice identification is also catching on fast. It has been used in court cases for some years and Canadian stockbroking firm TD Waterhouse is using it to automatically verify its customers before they start trading – completely automating the system. In Spain, Bankinter runs the Kivox voice recognition system created by voice experts, Agnitio. It is used internally to verify the ID of staff. Agnitio expects other banks in the UK and Europe to start using its service within the next 12 months. But just how unique is our voice? We took the chance to test the Kivox Authenticator.

Dan Simmons made two telephone calls saying clearly 10 sets of four numbers, so the system could build a voice profile and recognise him when he called back. And sure enough when he did, it let him in, although he did get a few false negatives. It did not like the throaty tones of his voice in the morning, or when background noise was too high. All the attempts we made to fool the system failed.

Agnitio were so confident, the company offered to introduce us to a pair of identical twins in order to test it. Unfortunately, when we agreed the pair were unavailable for filming. So Dan asked his brother to try and break into the system. He did it with comparative ease.

In a statement, Agnitio said: "Agnitio's Kivox demo system is a basic tool to show how voice biometrics works. It has not been calibrated to a real live scenario. We have set the demo's False Rejection Rate very low to make it more accessible. Consequently, the False Acceptance Rate increases. For a 'live system' we will always bring the False Acceptance Rate down, as required by our customers. Please note, there will always be false positives."

Said Ant Allan: "There is work to be done. Even if the technology itself is sound and even if in other situations it works well, or well enough, I think this stresses the sensitivity that this kind of technology has, on the way it's used, how the system is set up, on the circumstances, the environment and so on. It's interesting, given the problems that we've seen with small-scale implementation of biometric projects, these large scale implementations are really opening themselves up to significant failures. That's not necessarily likely, but it's certainly a possibility."

HOW BIOMETRICS COULD CHANGE SECURITY

Recent losses of personal data held on discs, laptops and USB keys by governments and companies have highlighted the need for better security. Here Dan Simmons looks to see if biometrics can help.

As the name implies biometrics is all about using a measurable biological characteristic, such as a fingerprint or iris pattern, to identify an individual. And the field is not confined to gross physical characteristics such as facial features, more subtle measures – such as the way a person walks – can also be used to identify individuals.

Researchers at the University of Southampton have won funding from UK and US governments to establish a new form of biometrics. They claim their gait recognition system is 99% accurate when identifying people.

"From a picture, we take the human body silhouette, and we get a set of measurements which describe the subject's shape," said Prof Mark Nixon, head of the gait research group at Southampton. "We also get a set of measurements which describe the movement, and together, those are used to recognise the person. The alternative to that is to use a model, and so we model the movement of parts of the body like the thorax and limbs. The motion of the model gives us the set of numbers that we then use to recognise you," he said.

To collect data the team has designed a tunnel employing eight cameras that feeds data to sophisticated modelling software that collects data. Through this work, researchers have been able to analyse variables in the real world, such as different

surfaces and shoes, and how these might affect the way people walk. Prof Nixon's database currently stands at 100 students, but the technology is already being used outside the labs too.

Automatic gait recognition on public CCTV images has been admitted as evidence in UK courts for the first time. One man was convicted of a burglary after podiatrists compared CCTV images of him on his way to commit a crime with images of him in custody. The CCTV pictures were grainy and made identification difficult, but the 35-year-old's distinctive swagger gave him away to experts.

Prof Nixon hopes to automate this type of video matching, but recognised that walking styles can be affected – or not work at all if the person is covered up or trying to hide their usual walking style. But, he said, some elements of an individual's movement did not change and the advanced modelling his group uses could factor out problems.

As the pen and signature are slowly replaced by the computer and keyboard, security companies are now offering software that recognises a user by the way they log into a computer. The tech measures the time between keystrokes, how long each key is held down, and total time taken to do tasks. Some companies have turned to typing recognition to stop staff sharing passwords.

A less tested form of biometrics is odour recognition, which is being studied to see if sensors can tell people apart by the way they smell. Apparently, not even a strong curry can hide personal odour, but the tech required is expensive and has not been tested outside the labs.

Despite these advances, the physical biometric in widest use is the fingerprint. Fingerprint readers have been built into laptops, and some banks are looking at using these devices to secure cash machines and online banking. Tech giant Siemens has helped develop what it calls an "Internet Passport" that presents users with a flashing barcode when they visit a bank or shopping site. A device held up to the computer screen read the information encrypted in the flashing image and deciphers it. Users then swipe a finger on the device, and after verification, are shown a decoded string of numbers needed to access the website.

Jonathan Haywood, from Siemens, says the company is in talks with a couple of banks in the UK, Germany and Switzerland.

"The device stores 128 possible accounts, you can then use this substitute all of your credit cards, or store cards, you can use it for loyalty schemes," said Mr Haywood. "So you don't have to have a big wallet full of things, you can have just this, and it will handle all of the security for you."

The company believes this device will stop fraud, but it involves the user doing more of the work, and costs US$100 (£61) a unit.

MICROSOFT TO BATTLE IN THE CLOUDS

Microsoft has unveiled a cloud computing service, in which data and applications will not be stored on individuals' computers.

The new platform, dubbed Windows Azure, was announced at Microsoft's Professional Developers Conference in Los Angeles. The platform was described by Microsoft's chief software architect Ray Ozzie as "Windows for the cloud". The framework will be offered alongside the next Windows release, Windows 7.

The move sees Microsoft taking on established players like Google and Amazon in the rapidly growing business of online software. The aim is to allow developers to build new applications which will live on the internet, rather than on their own computers. Microsoft believes consumers will also want to store far more of their data – from letters to photos to videos – on the servers in its "cloud" of giant data centres around the world, so that it can be accessed anywhere, from any device.

The term cloud computing has become increasingly fashionable, as companies with large data centres start renting out space to businesses wanting to build rapidly growing online applications without needing to invest in more servers as traffic grows. For consumers, there is the prospect of a future where much of their data and many of the applications they use could be stored online "in the cloud".

Microsoft, which still reaps huge profits from its Windows and Office products, is now moving into territory where it has so far struggled to make an impact.

Google, dominant in search and in online advertising, already has a suite of online applications living in the "cloud". Sam Schillace, who runs Google Docs, says he is not worried by the arrival of a big new rival.

"Competition, even stiff competition from Microsoft doesn't bother us because it will either make the internet as a whole better or it will be irrelevant to making it better."

Without naming Microsoft, Mr Schillace drew a contrast between the old model of "bloaty" software and a more open future where online applications would be updated virtually every week.

"The way people work and the way people communicate, openness and velocity and nimbleness and focus are much more valuable and I think that's a very big shift."

Amazon, with big data centres handling millions of e-commerce transactions, has been another pioneer in this field, with its Elastic Cloud Service. Using the spare capacity on its servers, it allows a range of customers big and small – from Facebook application developers to the Washington Post – to build applications which can cope with a sudden rush of demand.

In his speech in Los Angeles, Ray Ozzie said he "tipped his hat" at Amazon for its work in this field, saying "we are all standing on their shoulders."

Microsoft is taking a different approach from some of its rivals, insisting that its customers still want to be able to choose to have their software offline, on their own computers, as well as online in the web cloud. "We believe deeply in on-premises software and we believe deeply in this new world of software in the cloud," said Ray Ozzie.

It's a strategy which rivals will say is designed to protect the profits from its existing software products. But the scene is set for a battle in the clouds between the few big companies wealthy enough to be able to build the huge data centres on which this new form of computing will depend.

CLEANING UP IN 'FAB WORLD' BY PETER WILSON

The process of making silicon chips is as complex as the chips themselves. Each manufacturing plant, or "fab", may cost billions of dollars and is a triumph of engineering. But working inside these hi-tech plants can be a surreal experience, says Dr Peter Wilson of the University of Southampton.

"Fab world" is like no other place on earth. Its pristine white walls, secure air locks, sterile air and ethereal yellow lighting makes it seem like you have arrived in the belly of an orbiting space station. I can still remember the first time I went there. It was set in classic "tumbleweed" territory – a small town in Arizona with just one road and the factory. The temperature was over 100 degrees outside, with dust everywhere, but when you crossed the threshold into the plant, the air-conditioning kicked in and you felt like you were in a different world. This is a common experience to anyone who works in the silicon manufacturing sector. The world outside and the fab world inside are on two different planes. The boundary can transcend geographic and political boundaries – it can become impossible to tell which country you are in, when everyone is wearing a mask, and is dressed head to foot in shapeless, white hooded-suits.

Outside, we worry about dirt on our shoes and wipe our feet, or perhaps wipe some dust off our laptop screen. In fab world, we worry about a few atoms contaminating the environment. If dust falls on the delicate silicon wafers on which chips are printed it can render them useless. Modern transistors – the tiny switches at the heart of these devices – are described in terms of the smallest feature sizes that can be made, such as a 45 nanometres, or 45 billionths of a meter. To put this in perspective, the average human hair will be between 20 and 100 micrometers across – over a thousand times larger – and a typical dust particle will be anything from 1 to 100 micrometres. Dust and contaminants must be kept out!

The fab is a place for chips, not for people. As a result, only the pure and the clean are given permission to penetrate its' inner chambers. Anyone that enters must go through a strict set of procedures. All of the trappings of the outside world must be left behind, whether clothes, jewellery or even make-up. A series of ante-chambers serve as prep rooms where workers change into a series of gowns and gloves, collectively known as a "bunny suit". Sticky floors make sure that no one treads in any contaminants and an air shower before entry makes certain that any loose particles are stripped away. Skin flakes, lint, hair and anything else gets sucked into the grate in the floor. And then it's onwards into the hum of the clean rooms. Stark white walls reflect the yellow sodium lights from above and a constant breeze blows down from the ceiling taking any particles through the gridded floor. In modern fabs, ultra high tech chips are manufactured in what are known as class 1 rooms that contain just one tiny particle per metre cubed. In contrast, a room where open heart surgery takes place may have as many as 20,000. Everything taken in either needs to be cleaned with alcohol or specially designed. Even the paper we use to take notes is designed from a special lint-free material.

Inside, humans very rarely come into contact with the rainbow-streaked discs of reflective silicon on which the chips are cut. Instead, they are there to trouble-shoot and monitor that everything goes correctly. The silicon wafers are handled on

monorails that move above the fab floor and the processing is done by complex vacuum sealed robots. The wafers enter one end of the line costing a couple of hundred dollars and appear at the other – weeks later – patterned with billions of transistors and worth tens of thousands of pounds. The silicon itself is not made at the fab – the ultra pure ingots (up to 99.99999999% pure) are produced and cut by specialist companies and sold to the chip makers. The fab world's magic is creating the incredibly complex patterns of wires and circuitry on chips the size of a postage stamp time and time again. That alchemy can cost billions of dollars. Each layer of a processor is constructed using a mask which is like a stencil, to highlight the areas to be deposited, etched or doped. Doping involves adding impurities to the silicon to change its electrical characteristics – something which has to be done with astonishing precision. Each mask used to cost several thousand pounds but as the complexity of chips has increased, and the smallest possible feature size has reduced, the number and intricacy of these masks has increased. In addition, the size of individual features is now smaller than the wavelength of light that used to be used to pattern them, which means the use of some clever optics is required.

The yellowish lights used inside the fab are to make sure that they do not interfere with this process.

The result of all of this is that an individual silicon integrated circuit may require masks that cost hundreds of thousands of pounds, or perhaps even millions of pounds, to produce and machines that cost a similar amount. Fab world is an expensive place and, hence, it never stops. The plants churn out chips every single day of every year. So called giga-fabs may process more than 100,000 wafers every month, each containing hundreds of chips. Each one of the 10mm by 10mm silicon squares is a triumph of design. As a chip designer, the impact of the incredible complexity of fab world has led to an amazing transformation in what we can do on a single chip. The products of this strange and surreal place have burst out of its confines and have pervaded every facet of the outside world from computers and mobile phones to aircraft and microwave ovens.

Yet, incredible as it is to visit, fab world is also a place that is blissful to leave. At the end of the day there's no better feeling than being able to rip off the itchy bunny suit, step outside into the searing heat and once again get dirty.

FUTURE DIRECTIONS IN COMPUTING

Silicon electronics are <u>a staple</u> of the computing industry, but researchers are now exploring other techniques to deliver powerful computers.

Quantum

A quantum computer is a theoretical device that would <u>make use</u> of the properties of quantum mechanics, the <u>realm of</u> physics that deals with energy and matter at atomic scales. In a quantum computer data is not processed by electrons passing through transistors, as is the case in today's computers, but by caged atoms known as quantum bits or Qubits.

"It is a new paradigm for <u>computation</u>," said Professor Artur Ekert of the University of Oxford. "It's doing computation differently."

A bit is a simple unit of information that is represented by a "1" or a "0" in a

conventional electronic computer. A qubit can also represent a "1" or a "0" but crucially can be both at the same time – known as a superposition. This allows a quantum computer to work through many problems and arrive at their solutions simultaneously.

"It is like massively parallel processing but in one piece of hardware," said Professor Ekert.

This has significant advantages, particularly for solving problems with a large amount of data or variables.

"With quantum computing you are able to attack some problems on the time scales of seconds, which might take an almost infinite amount of time with classical computers," Professor David Awschalom of the University of California, Santa Barbara told the BBC News website recently.

In February 2007, the Canadian company D-Wave systems claimed to have demonstrated a working quantum computer. At the time, Herb Martin, chief executive officer of the company said that the display represented a "substantial step forward in solving commercial and scientific problems which, until now, were considered intractable." But many in the quantum computing world have remained sceptical, primarily because the company released very little information about the machine. The display also failed to impress.

"It was not quite what we understand as quantum computing," said Professor Ekert. "The demonstrations they showed could have been solved by conventional computers."

However, Professor Ekert believes that quantum computing will eventually come of age. Then, he said, they will not be used in run-of-the-mill desktop applications but specialist uses such as searching vast databases, creating uncrackable ciphers or simulating the atomic structures of substances.

"The really killer application will probably be in designing new materials or complex systems," he said.

Light

Computers exploit the movement or accumulation of electrons to do useful calculations. These movements down tiny wires are the reason why PCs become so hot.

"We are dissipating huge amounts of power in chips right now," said Professor Stan Williams of computer firm Hewlett Packard.

And the problem will get worse as the components become smaller, making chips even more inefficient, he said.

"If we could find new ways of moving information around a chip, we could significantly reduce the amount of power that is dissipated."

A potential solution would be to use particles of light – photons – instead of electrons to move information around and between chips.

"Electrons will still be doing the computing but photons will be doing the communicating," he said.

"It sounds a little bit complex but you find that that baton pass [of data between the electrons and photons] can be far more efficient, in terms of electrical power required than just using electrons."

It is similar to the technology that is used to move data around the internet today but at a much smaller scale. The technology could be key for transferring data between massively multiple core chips – devices with several linked computing engines. But some researchers would ultimately like to skip this baton pass and use photons to manipulate and store data, rather than just transmit it. Experiments are going on in academic institutions, firms such as IBM and even the American space agency Nasa. Several of the individual components needed to build an optical computer have been demonstrated and even put together into a working machine. However, it may be some time before optical components compete with silicon because of a fundamental barrier.

"The reason it is not in circuits today is essentially cost," said Professor Williams.

Spin

Spintronics, also known as magnetoelectronics, is a technology that <u>harnesses</u> the spin of particles, a property ignored by conventional electronics.

"Until now, electronics has worked by moving electrons around or moving charge around and that takes work," said Kevin Roche of computer giant IBM. "The most obvious example of that is that if you have a laptop that runs faster, it runs hotter."

But, by using the spin of particles – detected as a weak magnetic force – scientists believe they can unlock almost infinite computing power.

"It is called spin because the maths for dealing with it is similar to the maths for a spinning ball," said Mr Roche. "An electron always has spin and it can be spinning one of two different ways: up or down."

These two different states can be used to represent a "1" or a "0" – the bits of information used by all computers. Basic spintronic devices are already used in today's computers. For example, most hard drives today use a "spin valve", a device that reads information off the individual disks or platters that make up a hard drive. But researchers at firms such as Intel and IBM are hoping to take this one stage further.

"We are hoping to use it to store data, to transmit data; to do all the things we do now with charge but to use the spin property of the electron instead," said Mr Roche.

Chips exploiting spintronics would in theory be able to transmit data with spin using a lot less charge.

"So power costs go down," said Mr Roche.

IBM has already shown off a prototype spintronic device known as "racetrack memory", a device that could increase storage density by up to 100 times.

Other researchers are working on spin-based transistors, which unlike conventional transistors would not require the application of an electric current to work. According to many researchers, spintronics could be the next big change in computing in the coming decades.

"The conventional microelectronics industry and the magnetic storage industry are approaching their limits very fast. Spintronics might offer a way out," Dr Yongbing Xu of the University of York told the BBC earlier this year.

Chemicals

Chemical computing is an unconventional approach to computation that uses a "soup" where data is represented by different concentrations of chemicals. Chemical computers can exploit several different kinds of reaction to carry out the computation. For example, so-called conformation computers use polymer molecules that change shape in response to a particular input. Metabolic computing exploits the kinds of reactions typically found inside a living cell.

Dr Andrew Adamatzky of the University of West England works on another type.

"I am dealing only with reaction-diffusion computing," he explains.

This type of computation exploits waves travelling through a <u>beaker</u> of chemicals to carry out useful calculations. These waves are <u>the information carriers</u> in the computer. They are created by triggering chemical reactions in the soup at specific points. As waves propagate from different areas they <u>collide</u> and interact – effectively processing the information they hold. At the site of their interaction a point with a new chemical concentration is created, which is in effect an answer. With a beaker full of thousands of waves travelling and interacting with each other, complex computational problems can be solved. Although the process sounds complicated and esoteric it can be applied to almost all computational problems.

"Reaction-diffusion processors are universal computers, they can solve all types of problems," said Dr Adamatzky.

As a result, computer giant IBM is already interested in the technology.

Although slower than silicon, its key advantage is that it is cheap to produce and incredibly <u>robust</u>.

Working with chemist Ben De Lacy Costello, Dr Adamatzky has already produced logic gates using the technique that can be used to make chemical "circuitry".

"Ultimately, we will produce a general purpose chemical chip," he said. The chip would be capable of mathematical operations such as adding and multiplying numbers, he said. However, he believes he can take the research even further to create intelligent, amorphous robots. In these, he said, silicon circuitry would be of no use.

"Assume we have fabricated an artificial amoeba, gel-based robot, without any fixed shape, and capable for splitting into several smaller robots," he said. "Conventional silicon circuits will not work because they have rigid architecture." But as chemical computers are an amorphous blob they could be cut in half and both would continue functioning independently. "You can not cut your laptop in half and expect both parts to function properly; you can do this with reaction-diffusion processors," he said.

DNA

DNA computing, commonly called biomolecular computing, is an <u>emerging</u> field that uses DNA and biochemistry instead of silicon-based electronics. The first proof-of-concept use of DNA to perform computation was carried out by Professor Leonard Adleman at the University of Southern California in 1994. The original goal

of the field was to use biomolecules to beat electronic computers at solving large complex problems.

"Today, most people believe that biomolecular computing will not beat electronic computers in the <u>foreseeable future</u>," admitted Professor Ehud Shapiro of the Weizmann Institute of Science in Israel. Instead, said Professor Shapiro, the new goal is to try to use DNA computing to do things that traditional silicon cannot.

"What we offered in our work was a different vision," he said. In particular he is trying to develop smart drugs that are capable of computation.

"You want a drug that can sense the biochemical environment, analyse it and, in response, release a molecule which is the appropriate drug for that particular situation," he said.

In 2002, Professor Shapiro unveiled a programmable molecular device composed of enzymes and synthetic strands of DNA. Two years later, the same team showed off another DNA computer so small that roughly a trillion of them could fit into a microlitre (a millionth of a litre). The device was able to detect signs of cancer, and release drugs to treat the disease.

"This soup of DNA and enzymes implements a well know mathematical model of computation known as finite automaton," he explained. "This finite automaton knows how to do very simple computation such as recognising whether a list of zeros and ones has an even number of ones."

In the case of his 2004 computer this method of computation was used to analyze ratios of specific molecules related to prostate cancer and a specific type of lung cancer. The "computer" consisted of a chain of three segments of DNA and an enzyme which could cut the strands. If the first segment of the DNA detects ratios of certain molecules that indicate the presence of cancer, it tells the second segment to release the third segment, which is an anti-cancer drug. Since then, other researchers have shown off new computational systems that make use of enzymes that naturally occur in a living cell, whilst Professor Shapiro has attempted to make a more practical device.

"We have continued working in this direction trying to make this molecular system to work in living cells," he said.

Plastics

Silicon is expensive and complex to produce, requiring clean rooms and precise manufacturing techniques in plants that can cost billions of dollars.This means they are currently out of reach for low-cost products. But organic polymers, a class of substances that are used to make everything from bin bags to <u>solar panels</u>, could offer a solution.

"It really opens up a whole new set of options for what you do with electronics," said Professor Art Ramirez of Bell Labs.

Highly conductive polymers were first discovered in the early 1960s and are already used in some electronic devices. In 2004, electronics giant Philips announced a concept flexible display, while other companies such as Cambridge Display Technology use them to manufacture organic <u>light-emitting diodes</u> (LEDs).

Earlier this year, UK firm Plastic Logic said that it would build the world's first factory to produce plastic electronic circuits. Although, circuits made of polymers are much slower than silicon devices, they have one significant advantage: they can be printed using techniques similar to those used to mass produce magazines and wallpaper.

"Using big drums of substrate you can put down one chemical after the other and build up something that looks like a circuit," said Professor Ramirez. This means they are cheap and easy to produce. And as the polymers can be printed onto flexible substrates they can also be used in totally new types of device, such as large-scale billboards or electronic newspapers.

"If you can integrate that with very simple wireless connectivity one can imagine, instead of picking up the New York Times each morning, picking up a plastic sheet," said Professor Ramirez.

GLOSSARY
of computing terms and abbreviations

A

(Microsoft) Access /'ækses/ noun U – a database program developed by the Microsoft Corporation.

account /a'kaunt/ noun C – a registration for a user of a network system. It is used for controlling access to the system.

active window /'æktiv ˌwindəu/ noun C – the window in a WIMP system that is currently being used. It is usually on top of any other open windows.

address bus /ə'dres bʌs/ noun C – the set of conductors that carry the memory address signals between different parts of a computer system.

ADSL /ei di: es 'el/ noun U – abbreviation for asymmetric digital subscriber line. A form of DSL that has a different bandwidth for the upstream and the downstream.

AGP /ˌei dʒi: 'pi:/ noun U – abbreviation for accelerated graphics port. A video bus interface that allows the use of a fast video card and allows the use of three-dimensional graphics.

AI /ei 'ai/ noun U – abbreviation for artificial intelligence.

algorithm /'ælgəriðm/ noun C – a set of precise rules or instructions for solving a problem.

Alt (key) /'ælt, 'plt ki:/ noun C – the alternative key on a computer keyboard that changes the function of the other keys when it is held down.

ALT text caption /'ælt, 'plt tekst ˌkæpʃn/ noun C – text displayed in a webpage as an alternative to a graphic when the facility for displaying graphics is not available or is switched off.

AltaVista /ˌælta'vistə/ noun U – the name of a well-known search engine website.

analogue signal /'ænəlpg ˌsignəl / noun C – a type of signal that can take any value between a maximum and a minimum.

analyst programmer /'ænəlist ˌprəugræmə/ noun C – a person whose job is a combination of systems analysis and computer programming.

anorak /'ænəræк/ noun C – a slang term for an eccentric socially inept person with little or no fashion sense and having an obsessive interest in a hobby or subject.

anti-static /ænti 'stætik/ adj – prevents the build up of static electricity.

anti-virus (program or software) /ˌænti 'vairəs/ noun C/U – a computer program or set of programs used to detect, identify and remove viruses from a computer system.

Apple /'æpl/ noun U – the common name for Apple Computer Incorporated, a well-known producer of computers that introduced the WIMP interface on computers such as the Apple Macintosh.

Apple Macintosh /æpl 'mækintpʃ/ noun C – a family of personal computers produced by Apple Computer Inc.

applet /'æplət/ noun C – a very small self-contained computer program.

application layer /æpli'keiʃn ˌleiə(r)/ noun C – the only part of a network communications process that a user sees. It prepares a message for sending over a

network by converting the message from human-readable form into bits and attaching a header identifying the sending and receiving computers.

application port /ˌæpli'keiSn po:t/ noun C – a path available for a particular type of application data to enter or leave a network system.

application service provider /.æpli.keiSn 'sW:vis praˌvaidə(r)/ noun C – a company that makes applications programs available over the Internet usually charging a fee for access to programs.

applications (program or software) /æpli'keiSnz/ noun C/U – a computer program designed to be used for a particular purpose, e.g. a wordprocessor spreadsheet or database program.

applications programmer /æpli'keiSnz ,prəuɡræmə(r)/ noun C – a person who writes applications programs using a computer language.

architecture /'a:kitekCə(r)/ noun C – the general specification of a system.

archive bit /'a:kaiv bit/ noun C – a digital bit stored with a file indicating if the file has been backed up since it was last edited.

archiving system /'a:kaiviN .sistəm/ noun C – a system used for storing infrequently-used data in a way that does not provide the user with immediate access.

artificial intelligence /a:tifiSl in'telidZəns/ noun U – an area of computing concerned with developing computer programs that perform tasks that can normally only be done using human intelligence.

ASCII /'æski/ noun U – acronym for American Standard Code for Information Interchange. A standard character encoding scheme.

ASP /ˌei es 'pi:/ noun C – abbreviation for application service provider.

assembly language /ə'sembli .læŋgwidZ/ noun C – a low-level computer language that uses mnemonics rather than only numbers making it easier than machine code for humans to read and write.

asymmetric /.eisi'metrik/ adj – having a different signal bandwidth in each direction, i.e. the bandwidth for sending is different from the bandwidth for receiving.

asynchronous /ei.siNkrənəs/ adj – not synchronised, i.e. occurring at irregular intervals.

AT&T /ei ti: ən 'ti:/ noun U – abbreviation for American Telephone and Telegraph Company. One of the world's largest IT suppliers.

ATI (Technologies) /ei ti: ai/ noun U – the name of a well known company that produces computer graphics cards.

ATM /ei ti: 'em/ noun C – common abbreviation for automatic teller machine. The type of machine used by banks for enabling customers to withdraw money from their bank accounts.

authentication /O:Tenti'keiSn/ noun U – a process that checks the identity of a user or an object.

avatar /'ævəta:(r)/ noun C – a graphical icon that represents a real person in a cyberspace system.

B

B channel /'bi: Cænəl/ noun C – the common name for a bearer channel in an ISDN system.

backup /bæk Ap/ verb – to store a copy of data on a storage device to keep it safe.

backbone /'bækbəun/ noun C – the main transmission path handling the major data traffic connecting different LANs together.

backend /'bækend/ noun C – the server part of a client-server configuration that provides a service on a network at the request of a client.

backup /'bækAp/ noun C – the process of storing a copy of data on a storage device to keep it safe / the term used for the copied data.

bandwidth /'bændwidD/ noun C – the range of frequencies that can be transmitted over a communications channel.

barcode /'ba:koud/ noun C – a sequence of vertical parallel lines used to give items a unique identification number.

barcode reader /'ba:koud ri:də/ noun C – an optical input device that uses the reflection of a light beam to read barcode labels.

BASIC /'beisik/ noun U – acronym for Beginners' All-purpose Symbolic Instruction Code.

batch mode /'bæC məud/ noun U – a process in which all the data is collected and processed together in a batch rather than one at a time as they become available.

BBC micro /ˌbi: bi: si: 'maikrəu/ noun C – the name of one of the first microcomputers produced in the United Kingdom and used in schools. Its development was sponsored by the British Broadcasting Corporation.

bearer channel /'beərə ˌCænəl/ noun C – the common name for the part of an ISDN line that carries the data.

Beginners'All-purpose Symbolic Instruction Code /biˌginəz O:l ˌpWpəs sim.bolik in'strAkSn kəud/ noun U – a simple high-level computer language often used for teaching programming.

B-frame /'bi: freim/ noun C – the common name for a bi-directional frame in an MPEG compressed file.

bi-directional frame /bai də.rekSənl 'freim/ noun C – a type of image frame used in MPEG compression. It is situated between I and P frames and stores the differences in the image compared with the I or P frame both before and after it.

binary /'bainəri/ noun U – a number system that only uses two digits, i.e. 1 and 0.

biometric device /ˌbaiəmetrik di'vais/ noun C – a security device that measures some aspect of a living being, e.g. a fingerprint reader or an eye scanner.

BIOS /'baios/ noun C – acronym for Basic Input Output System. A part of the operating system stored on a ROM chip that controls the input and output of data to peripherals.

biotechnology /.baiəutek'nolədZi/ noun U – the industrial application of biological science techniques.

bit /bit/ noun C – a small unit of storage capacity. One of the eight binary digits that make up a byte. The term comes from an abbreviation of binary digit.

bitmap compression /ˌbitmæp kəmˌpreSn/ noun C – a way of reducing the size of a stored image where different digital bits or collections of bits are used to describe each element of an image.

(data) block /blok/ noun C – a collection of data stored together and treated as a single unit.

Bluetooth /'blu:tu:T/ noun U – the name of a high-speed microwave wireless network system developed by a group of companies consisting of Ericsson, IBM, Intel, Nokia and Toshiba. It is used with portable equipment.

bookmark /bukma:k/ verb – to store a link to a webpage to make it easier to find in the future.

boot /bu:t/verb – to copy a part of the operating system into memory to allow a computer to start up.

boot sector virus /bu:t sektə 'vairəs/ noun C – a self-replicating program that stores itself in the part of a disk containing the programs used to start up a computer.

bracketing /brækətiN/ verb – to set the boundaries of a message or part of a message by marking its beginning and its end with special control bits.

bridge /briG/ noun C – a hardware and software combination used to connect the same type of networks or to partition a large network into two smaller ones.

broadband /'bro:dbGænd/ adj – able to carry signals transmitted over a wide range of frequencies.

broadcast /bro:dka:st/ verb – to transmit signals that can be picked up by a large number of receivers.

browse /brauz/ verb – to move from webpage to webpage using a Web browser program.

(Web) browser /'brauzə(r)/ noun C – a program used for displaying webpages.

BT /bi: 'ti:/ noun U – abbreviation for British Telecom. The organisation that provides the telephone system in Great Britain.

buffering /'bAfəriN/ noun U – a process of temporarily storing data from a fast source so that it can be fed at a steady rate to a slower system.

bug /bAg/ noun C – a fault in a system.

bulletin board /'buletin bo:d/ noun C – an electronic noticeboard system that enables users to display messages for other users to read.

bus /bAs/ noun C – a set of conductors that carry signals between different parts of a computer.

byte /bait/ noun C – a unit of storage capacity. A byte is made up of eight bits and stores one character, i.e. a letter, a number, a space or a punctuation mark.

C

C /si:/ noun U – a general purpose computer programming language that was originally designed for writing Unix systems programs.

C drive /'si: draiv/ noun C – the first hard disk in a personal computer.

C++ /si: plAs 'plAs/ noun U – an object-oriented superset of the C programming language commonly used for writing applications programs for the Microsoft Windows operating system.

cache /kæS/ verb – to temporarily store frequently-used data in fast memory so that it can be accessed more quickly.

cache /kæS/ noun C – fast memory used to temporarily store frequently-used data to allow it to be accessed more quickly.

cache coherency /kæS kəu'hiərənsi/ noun U – a system that ensures that any changes written to main memory are reflected within the cache and vice versa.

cache controller /kæS kontrəu1ə(r)/ noun C – the set of electronic logic circuits that control the operation of cache memory.

cache hit /kæS 'hit/ noun C – the process of successfully finding the required data stored in cache memory.

callback system /кL1bæк ˌsistəm/ noun C – a system that automatically disconnects a telephone line after receiving a call and then dials the telephone number of the system that made the call to reconnect the line. It is used in remote access systems to make sure that connections can only be made from permitted telephone numbers.

cathode ray tube /ˌkæTəud rei 'tju:b/ noun C – a display device that uses an electron gun to fire a beam of electrons at a phosphor-coated screen.

CCNA /si: si: en 'ei/ noun U – abbreviation for Cisco Certified Network Associate. A starting level networking qualification offered by Cisco, a major network equipment vendor.

CD (-ROM) (disk) /si: 'di:/ noun C – abbreviation for compact disk read only memory. A read only storage device in the form of a disk that is read using laser light.

CD-ROM drive /si: di: 'rom draiv/ noun C – a storage device for reading CD-ROM disks.

CD-RW (drive) /si: di: a: 'dAbl ju:/ noun C – abbreviation for compact disk rewritable. A storage device use for reading from and writing to a special type of CD known as a re-writeable CD.

cellphone /'selfəun/ noun C – the common name for a cellular phone.

cellular network /seljələ ˌnetwWk/ noun C – a radio communications systems that divides a region into cells so that each region becomes a network with every point connected to a local transmitter within the cell.

cellular phone /.seljələ 'fəun/ noun C – a cellular telephone. A mobile telephone that communicates with a local transmitter located within a small geographic area called a cell.

central processing unit /.sentrəl 'prəusesiN ˌju:nit/ noun C – the electronic processor at the centre of a computer. The term is sometimes used to refer to the combination of the processor and the main memory.

channel /'Cænəl/ noun C – a path for the transmission of data.

chat room /'Cæt ru:m/ noun C – a virtual space on a website where online discussions organized around specific interests are held in real-time by users typing text messages.

check data /'Cek deitə/ noun U – information written to disks in a RAID system which is used to restore data if one of the array drives fail.

checksum /'CeksAm/ noun C – a calculated value that is stored with data to detect any errors that may occur when the data is copied or transmitted.

chip /Cip/ noun C – common name for a microchip. An electronic integrated circuit in a small package.

Cisco /'siskəu/ noun U – the name of a company that makes networking system hardware such as that used to operate the Internet.

class /kla:s/ noun C – the term used for a collection of objects in object oriented programming.

cleanse /klenz/ verb – a term used in data mining meaning to remove duplicate information and erroneous data.

(left) click /klik/ verb – to press and release the (left-hand) button on a mouse.

client /'klaiənt/ noun C – a network computer used for accessing a service on a server.

client-server application /klaiənt 'sWvər ˌæpli'keiSn/ noun C – a program that is accessed from a client computer but most of the processing is carried out on a server computer.

clipart /'klipa:t/ noun U – professionally-prepared graphical images stored on a computer system.

Clipboard /'klipbLd/ noun U – the name used in Microsoft Windows for the section of memory that temporarily stores data while it is being copied and pasted.

clock /klOk/ noun C – the set of electronic circuits used to control the timing of signals and synchronise different parts of a computer system.

cluster /'klAstə(r)/ noun C – a term used in data mining meaning a group of data that has similar features or is based on a limited data range.

clustering /'klAstəriN/ noun U – a method used in data mining that divides data into groups based on similar features or limited data ranges.

CMC /ˌsi: em 'si:/ noun C – abbreviation for computer mediated communication, i.e. the transfer of messages using a computer system.

CNE /ˌsi: en 'i:/ noun U – abbreviation for Certified Novell Engineer. A qualification aimed at people interested in installing and planning the rollout of Novell based networks.

coax(ial) (cable) /'kəuæks/ noun C – a type of shielded cable for carrying signals. It is often used with radio frequency and video signals.

COBOL /'kəubol/ noun U – acronym for Common Business-Oriented Language.

code /kəud/ noun U – a piece of program text written in a programming language.

code /kəud/ verb – to write the text of a program or part of a program using a computer language.

COM program /'kOm ˌprəugræm/ noun C – a DOS program with a .com filename extension that loads and runs in 64 kilobytes or less of memory.

command interpreter /kəma:nd inˌtWpritə(r)/ noun C – the part of an operating system that processes commands that are part of a program or are input using a keyboard.

Commodore 64 /.komədo: ˌsiksti 'fo:(r)/ noun U – the model name of one of the first popular personal computers to be made available in the United Kingdom. It had a very good graphics system and was particularly suited to running computer games programs.

Common Business-Oriented Language /.komən .biznis ,o:rientid 'læŋgwidZ/ noun U – a high-level computer programming language. It is the principal transaction processing language used to process the records of large organisations on mainframe computers.

compatible /kəm'pætəbl/ adj – able to operate on the same type of system or run the same software.

compile /kəm'pail/ verb – to convert a program written in a high-level language into machine code using a compiler.

compiler /kəm'pailə(r)/ noun C – a program that converts the whole of a program into machine code before the program is used.

compress /kəm'pres/ verb – to reduce to a much smaller size.

compression (scheme) /kəm'preSn/ noun C – the process used for reducing a file to a much smaller size.

computer /kəm'pju:tə(r)/ noun C – a general purpose machine that can be programmed to process data in a variety of ways.

computer consultant /kəm'pju:tə kən.sAltənt/ noun C – a person who is paid to advise on computing system issues.

computer engineer /kəm'pju:tə enGiˌniə(r)/ noun C – a person who designs and develops computer systems.

computer lab /kəm'pju:tə læb/ noun C – a room full of computers used for study.

computer language /kəm'pju:tə 1æNgwiG/ noun C – a language used for writing computer programs.

computer operator /kəm'pju:tə ,Opəreitə(r)/ noun C – a person whose job it is to operate part of a computer system.

computer salesperson /kəm'pju:tə 'seilzpWsn/ noun C – a person whose job it is to sell computers.

computer science /kəm'pju:tə saiəns/ noun U – the study of computers and their use.

computer services engineering technician /kəm'pju:tə sWvisiz enGi'niərN tekˌniSn/ noun C – a person who provides a service of maintaining and troubleshooting computers.

computer-aided design /kəm'pju:tə eidid di'zain/ noun U – the process of designing using a computer program.

computer-aided manufacture /kəm'pju:tə eidid mænjə'fækCə(r)/ noun U – the process of manufacturing goods using a computer.

computerised /kəm'pju:təraizd/ adj – changed so that it can be operated or controlled using a computer.

computer-mediated communication /kəm'pju:tə mi:dieitid kəˌmju:ni'keiSn/ noun C – a process of transferring messages using computers.

computing /kəm'pju:tiN/ noun U – the theory and practice of computers.

computing science /kəm'pju:tiN 'saiəns/ noun U – see computer science.

computing support /kəm'pju:tiN sə'pLt/ noun U – a field of work that provides a service including setting up, maintaining and troubleshooting computing systems and providing technical advice to users.

computing support officer /kəm'pju:tiN sə'po:t ˌOfisə(r)/ noun C – a person whose job it is to provide support to computer users including setting-up, maintaining and troubleshooting computer systems and giving technical advice.

configure /kən'figə(r)/ verb – to adjust the settings.

connectivity /konek'tivəti/ noun U – the characteristic of being connected.

control bit /kən'trəul bit/ noun C – a data bit used to mark parts of a transmitted signal so that the transmission can be controlled, e.g. a 'start' bit marks the beginning of a character and a 'stop' bit marks its end .

control bus /kən'trəul bAs/ noun C – the set of conductors that carry the control signals between the Control Unit and other parts of a computer.

corrupt /kə'rApt/ verb – to damage in such a way that prevents normal use.

cp /si: 'pi:/ noun U – a Unix command for copying a file.

CPU /si: pi: 'ju:/ noun C – abbreviation for central processing unit.

crack /kræk/ verb – to break into a computer system in order to steal information or cause damage.

crash /kræS/ verb – to fail suddenly and completely usually referring to the failure of a hard disk.

CRT /si: a: 'ti:/ noun C – abbreviation for cathode ray tube.

Ctrl + Alt + Del /kəntrəul plAs ælt plAs di'li:t/– noun U – set of symbols that signify pressing the combination of the control-alternative and delete keys on a computer keyboard at the same time.

cursor /'kE:sə(r)/ noun C – a symbol on the monitor screen that indicates the point on the screen that is being used.

cut and paste /kAt ənd 'peist/ verb – to remove some data from a file and temporarily store it in the computer's memory then insert a copy of the data in another position in the same or in another file.

cyberbabe /'saibəbeib/ noun C – a digital image of an attractive female that is used in programs on the Internet.

cybernetics /.saibə'netiks/ noun U – the study of control and communication in animals and machines. It is used in the design of robots.

cyberspace /'saibəspeis/ noun U – the combination of all the data on all the computer networks throughout the world accessed using the Internet.

cyborg /'saibo:g/ noun C – a man-machine system or a person made superhuman by a machine or external system that changes the way the body functions.

D

D channel /'di: Cænəl/ noun C – the common name for a data channel in an ISDN system.

data /'deitə/ noun U – the information processed by a computer.

data bank /'deitə bænk/ noun C – a large collection of data that can be accessed by many users and enables them to copy or store data on a particular topic.

data bus /'deitə bʌs/ noun C – the set of conductors that carry the data signals between different parts of a computer.

data centre /'deitə sentə(r)/ noun C – a facility for storing large amounts of information.

data channel /'deitə Cænəl/ noun C – the common name for the part of an ISDN line that carries signalling and supervisory information to the network.

data communications /deitə kamju:ni'keiSnz/ noun U – the transmission and reception of data signals using a communications network and appropriate protocols.

data integrity /deitə in'tegrəti/ noun U – a measure of how resistant a system is to causing corruption in data while it is being stored or transferred.

data mart /'deitə ma:t/ noun C – a storage system that archives large amounts of data in a way that makes it easy to access.

data mining /'deitə mainiN/ noun U – a process of analysing a large amount of stored data to find new useful information.

data stream /'deitə stri:m/ noun C – the flow of data.

data warehouse /deitə 'weəhaus/ noun C – a computing centre that provides a large collection of data gathered from different sources for data mining.

database (program) /'deitəbeis/ noun C – a type of applications program used for storing information so that it can be easily searched and sorted.

data-delivery system /deitə di'livəri .sistəm/ noun C – a system for transmitting data from one computer to another.

data-link layer /'deitə link leiə(r)/ noun C – the part of a network communications system that supervises the transmission. It confirms the checksum then addresses and duplicates the packets. This layer keeps a copy of each packet until it receives confirmation from the next point along the route that the packet has arrived undamaged.

date /deit/ noun U – a Unix and MS-DOS command for displaying the current date.

debug /di:'bʌg/ verb – to find and fix faults in a program or system.

DEC VAX /'dek væks/ noun U – a range of computers produced by the Digital Equipment Corporation using their Vax range of processors.

decipher /di'saifə(r)/verb – to change coded information into normal text.

decision table /di'siZn .teibl/ noun C – a type of grid used in computer program design to show what actions should be taken by the program under different conditions.

decision tree /di'siZn tri:/ noun C – an Al technique used in data mining that separates data into subsets then further divides the subsets into smaller subsets until the subsets are small enough to allow the mining process to find interesting patterns and relationships within the data.

decode /di:'kəud/ verb – to decide what a program instruction means.

decompress /di:kəm'pres/ verb – to remove the compression, i.e. to expand to its original size

decrypt /di:'kript/ verb – to recover the original text from an encrypted message.

defacing /di'feisiN/ noun U – a computer crime that involves changing the information shown on another person's website without permission.

default /di'folt/ noun C – an initial setting that can be changed by the user.

denial of service attack /di‚naiəl əv 'sE:vis ə‚tæk/ noun C – a type of computer crime that involves swamping a server with large numbers of requests.

desktop /'desktop/ noun C – the main graphical user interface background screen that displays icons for other programs.

desktop (PC)/(computer) /'desktop/ noun C – a personal computer that is designed to be used on an office desk.

desktop application /'desktop .æpli'keiSn/ noun C – a computer program designed to be used on a desktop computer.

desktop organiser /'desktop 'o:gənaizə(r)/ noun C – a small computer providing a variety of tools for organising work, e.g. a calendar, to do list, diary, address list, calculator, etc.

development life cycle /di.veləpmənt laif saikl/ noun C – the phases a software product goes through from when it is first thought of until it becomes obsolete. This typically includes: requirements analysis, design construction, testing (validation), installation, operation, maintenance and retirement.

DHTML /di: eiC ti: em 'el/ noun U – abbreviation for dynamic hypertext markup language. A development of HTML that allows the creation of more dynamic and user-interactive web pages.

dial-up networking /dail Ap 'netwE:kiN/ noun U – a communications system that allows computers to connect together using a telephone line.

differential backup /.difərenSl 'bækAp/ noun C – a type of backup that copies all the selected files on a system that have been changed since the last time a full backup was carried out.

digital /'diGitəl/ adj – an electronic system that has only two states, e.g. off or on.

digital camera /.diGitəl kæmərə/ noun C – an input device for taking pictures. It has an electronic lens and uses electronics for storing the images rather than chemical film.

digital cash /.diGitəl 'kæS/ noun U – electronic currency that is stored on electronically sensitive cards or exists in cyberspace and is used for making electronic purchases over the Internet.

digital certificate /.diGitəl sə'tifikət/ noun C – an electronic message used to show a transaction is trustworthy. It contains information about the company processing the transaction including their public key and is electronically 'signed' by a trusted digital-certificate issuer.

digital subscriber line /.diGitəl səb'skraibə lain/ noun U – a broadband communications system that allows digital signals to be transferred across an ordinary analogue telephone line.

directory /də'rektəri, di-, dai-/ noun C – a storage area used for grouping files so that they can be easily located. A directory is sometimes called a folder.

disk /disk/ noun C – a flat circular storage device.

disk drive /'disk draiv/ noun C – a storage device for reading from and writing to disks.

divider /di'vaidə(r)/ noun C – a vertical bar that divides a Windows Explorer window into two parts. One part shows the drive folders and the other part shows the filenames of the files in the selected folder.

DNS /di: en 'es/ noun C – abbreviation for domain name system.

domain name /də'mein neim/ noun C – an identifier used on the Internet in place of the numerical Internet address. It identifies the host, the type and the country code, e.g. holyrood.ed.ac.uk.

domain name server /də'mein neim sE:və(r)/ noun C – a network server computer used for operating and controlling the domain name system.

domain name system /də'mein neim ˌsistəm/ noun C – a system of associating the name of a device on a network such as the Internet with its numerical address so that the name can be used by the user and the numerical address can be used by the network system.

dot-matrix printer /dot 'meitriks printə(r)/ noun C – a printer that prints by hammering pins onto an inked ribbon.

doubleclick /dAbl 'klik/ verb – to press and release the left-hand button on a mouse two times in rapid succession.

download /daun'ləud/ verb – to copy a file from a server to a client computer in a network.

download /'daunləud/ noun C – a process of copying a file from a server to a client computer in a network.

downstream /'daunstri:m/ noun U – the signal path for receiving communications from a server to a client computer in a network.

drag and drop /dræg ən drop/ verb – to move data from one location to another with a mouse. Holding down the mouse button while moving the mouse moves the selected data. Releasing the mouse button drops the data in the new location.

drive array /'draiv aˌrei/ noun C – a set of hard disks that are used in a RAID system.

driver /'draivə(r)/ noun C – a systems program that controls a peripheral device.

DSL /di: es 'el/ noun U – abbreviation for digital subscriber line.

DTP /di: ti: 'pi:/ noun U – abbreviation for desktop publishing. A process of designing documents for publishing using a computer system.

dumb terminal /dAm tE:minəl/ noun C – a network device with a keyboard and display screen that is used for sending and receiving data but does not do any processing.

duplex /dju:pleks/adj – able to transfer data in both directions, i.e. can send and receive data.

DVD (-ROM) /di: vi: di:/ noun C – abbreviation for digital versatile disk read only memory. An optical disk storage device that can hold a large amount of video data.

E

EAN /i: ei 'en/ noun U – abbreviation for European Article Number system. The European price and item codes commonly used in barcode systems.

earphone /'iəfəun/ noun C – sound output device that fits into the ear of the user.

earth /ɜːT/ noun U – a common name for an electrical ground point or zero voltage point.

ebook /'iːbuk/ noun C – common name for an electronic book.

ebook reader /'iːbuk riːdə(r)/ noun C – common name for an electronic book reader.

e-business /'iːbiznis/ noun U – common term for electronic business, i.e. business that is carried out using the Internet.

e-cash /'iːkæS/ noun U – common name for electronic cash.

ECC memory /i: si: si: 'meməri/ noun U – abbreviation for error code correcting memory. A type of memory often used in server computers that automatically fixes simple memory errors without requiring the rebooting of the computer.

e-commerce /'i: kəmE:s/ noun U – the business of buying and selling goods and services on the Internet.

editor /'editə(r)/ noun C – a computer program for making changes to text in computer programs or data.

edutainment /.edju'teinmənt/ noun U – a system that has both educational and entertainment value.

EIDE /i: ai di: 'iː/ noun U – abbreviation for extended integrated device electronics. A type of hard disk control system where most of the control electronics is built into the drive itself. Extended IDE allows the use of multiple drives of more than 528 megabytes.

electronic (book) reader /elekˌtronik 'riːdə(r)/ noun C – a computing device that displays the text and images of an electronic book.

electronic book /elekˌtronik 'buk/ noun C – a book that is displayed using a computing device instead of being printed on paper.

electronic cash/money /elekˌtronik 'kæS, 'mAni/ noun U – data that represents real money that is stored and transferred on computing devices connected to the Internet in e-commerce systems.

electronic publisher /elekˌtronik 'pAbliSə(r)/ noun C – an organisation that produces ebooks.

electronic virtual assistant /elek.tronik vE:Cuəl ə'sistənt/ noun C – a computer program represented by an animated screen image that is used to help the user perform particular tasks such as searching the Internet for useful data.

email /'iːmeil/ noun C – the common name for an electronic mail message, i.e. a text message sent electronically using a computer.

email /'iːmeil/ verb – to send an email message.

email address /'iːmeil ə.dres/ noun C – the unique address code used to contact someone using electronic mail.

email attachment /iːmeil ə.tæCmənt/ noun C – a file that is attached to an email message.

112

email program /'i:meil ˌprəuɡræm/ noun C – a computer program used for reading and sending email.

email service /i:meil ˌsE:vis/ noun C – an Internet service that allows user to send and receive emails.

encapsulation /en.kæpsju'leiSn/ noun U – a key feature of object-oriented programming that bundles data and program instructions into modules called objects.

encode /.en'kəud/ verb – to write information in a coded form.

encoder /en'kəudə(r)/ noun C – a computer program that converts WAV files into MP3 files or vice versa.

encrypt /en'kript/ verb – to transform data into coded form to make it secure.

encryption /.en'kripSn/ noun U – the transformation of data into coded form to make it secure.

Enter (key) /'entə(r)/ noun C – another name for the RETURN key on a computer keyboard. Pressing the ENTER key inserts the data into the memory of the computer.

enterprise resource planning tool /.entəpraiz riˌzo:s 'plæniN tu:l/ noun C – a type of computer program for planning and organising business functions in an enterprise. It can help companies manage everything from sales and marketing to human resources.

EPOS till /'i:pos til/ noun C – acronym for electronic point-of-sale till. A computerised cash register that edits records in sales and stock control databases.

e-publishing /'i: pAbliSiN/ noun U – the production of ebooks.

erasable optical disk /i.reizəbl optikl 'disk/ noun C – a CD that allows data to be deleted and new data to be recorded on it.

ERP /i: a: 'pi:/ noun U – abbreviation for enterprise resource planning.

e-solution /'i: səˌlu:Sn/ noun C – common term for electronic solutions, i.e. ways of solving a problem or providing a service using the Internet.

ethernet /'i:Tənet/ noun U – a widely-used local area network standard that broadcasts packets of data that are addressed to particular devices on the network. Each device on the network reads the address and passes it on to the correct device.

(Microsoft) Exchange /iks'CeinG/ noun U – a Microsoft Windows program that includes an email program, a calendar task list and address list.

exe program /eks'i: .prəuɡræm/ noun C – an MS-DOS executable program that has an .exe filename extension. It can use more than 64 kilobytes of memory and can be located anywhere in the memory.

executable /eksi'kju:tEbl/ adj – containing instructions that can be run or executed by the processor.

execute /'eksikju:t/ verb – to perform a computer operation by processing a program instruction.

expansion card /ik'spænSn ka:d/ noun C – an electronic circuit board used for adding facilities to a computer.

expansion slot /ik'spænSn slot/ noun C – a long thin connector that is used for adding additional electronics in the form of expansion cards.

expert system /'ekspE:t .sistəm/ noun C – an artificial intelligence program that collects and uses human expertise to allow non-experts to solve specialised problems.

extensible /ik'stensəbl/ adj – able to be added to, e.g. in an extensible language a developer can add their own terms.

extensible markup language /ik.stensəbl 'ma:k ʌp .læNgwiG/ noun U – a metalanguage that allows developers to create their own set of customised tags that identify the meaning and structure of data. It is used for creating files that are program-independent, platform-independent and able to be used with different languages.

F

FAQ /ef ei 'kju:/ noun C – acronym used on websites for frequently-asked question.

fault tolerance /'folt .tolərəns/ noun U –a computer's ability to recover from hardware errors.

fetch /feC/ verb – to go and get the next instruction or piece of data from memory.

field /fi:ld/ noun C – a section of a database where an item of data is Stored.

file /fail/ noun C – a computer program or data stored on a storage device.

file server /fail ˌsE:və(r)/ noun C – a main computer that provides a storage area for data files on a network.

file transfer protocol /fail trænsfɜ: 'prəutəkol/ noun U – an Internet service that allows users to transfer files from one computer to another.

file virus /'fail ˌvairəs/ noun C – a virus that attaches itself to a program file.

filestore /failstE:(r)/ noun C – a collection of computer files stored centrally on a network server.

firewall /'faiəwLl/ noun C – a combination of hardware and software used to control the data going into and out of a network. It is used to prevent unauthorised access to the network by hackers.

flag /flæg/ verb – to mark in a way that indicates that a particular condition has occurred.

flat file database /.flæt fail 'deitəbeis/ noun C – a simple database in which all the data is stored in one table which is not related to any other table.

floppy (disk) /flopi/ noun C – a magnetic storage device in the form of a small plastic disk. Also known as a diskette.

floppy (disk) drive /'flopi draiv/ noun C – a common magnetic storage device that reads and writes data on a floppy disk. Also known as a diskette drive.

flowchart /'fləuCa:t/ noun C – a kind of diagram used by programmers to show the logical steps in a program or by systems analysts to show logical steps in the design of a system.

folder /fəuldə(r)/ noun C – see directory.

FORTRAN /'fo:træn/ noun U – acronym for Formula Translator. A high-level computing language that was designed by scientists in 1954 and is oriented toward manipulating formulas for scientific, mathematical and engineering problem-solving applications.

forward /'fLwəd/ verb – to pass on without changing the content, e.g. a received email can be passed on to or forwarded to another address.

frame /freim/ noun C – a section of a webpage that acts as an independent browser window. Clicking on a link in one frame can cause a webpage to be displayed in another frame, e.g. a menu in one frame can provide links to webpages that are displayed in another frame.

Free Software Foundation /fri: softweə faun'deiSn/ noun U – an organisation that is dedicated to producing software that can be used by anyone who wants to use it at no cost. It depends on the voluntary effort of a large number of programmers throughout the world creating and improving programs and making their work freely available to others.

free up /fri: 'Ap/ verb – to make space available, e.g. by deleting files on a hard disk.

freeware /fri:weə(r)/ noun U – computer programs that are made available to anyone who wants to use them at no cost to the user.

frequency band /fri:kwənsi bænd/ noun C – a set of frequencies that are used together to provide a path for the transmission of signals.

frequency display /fri:kwənsi di.splei/ noun C – an electronic device for showing the frequency of a signal.

frequency hopping /fri:kwənsi ˌhopiN/ noun U – a process of changing frequencies within a fixed bandwidth during a transmission so that other transmissions can use the same bandwidth at the same time without interfering with each other.

FTP /ef ti: 'pi:/ noun U – abbreviation for file transfer protocol.

full backup /ful bækAp/ noun C – a type of backup that copies all the selected files on a system whether or not they have been edited or backed up before.

full-duplex /'ful ˌdju:pleks/ adj – able to transfer data in both directions simultaneously, i.e. data can be transmitted and received at the same time.

futurologist /fju:Cə'roləGist/ noun C – a person who studies and predicts what technology will be like and what effects it will have in the future.

G

games console /'Geimz .konsəul/ noun C – an electronic device used for playing computer games.

gateway /'Geitwei/ noun C – an interface that enables dissimilar networks to communicate such as two LANs based on different topologies or network operating systems.

Gb/GB /'Gigəbait/ noun C – abbreviation for a gigabyte.

geek /Gi:k/ noun C – although it was originally a derogatory term used for an expert lacking in social skills, it is now used in computing to mean a dedicated expert.

general packet radio service /ˌGenrəl ˌpækit 'reidiəo ˌsE:vis/ noun U – a GSM data transmission technique that transmits and receives data in packets.

general-purpose language /ˌGenrəl ˌpE:pəs 'læNgwiG/ noun C – a computer language that can be used to write different types of programs.

get listed /ɡet 'listid/ verb – to register the Web address of a website on an Internet search engine

GHz /'ɡiɡəhE:ts/ noun C – abbreviation for gigahertz.

gigabit /'ɡiɡəbit/ noun C – a unit of storage capacity equal to 1 073 741 824 bits.

gigabyte /'ɡiɡəbait/ noun C – a unit of storage capacity equal to 1 073 741 824 bytes.

gigahertz /'ɡiɡəhE:ts/ noun C – a unit of frequency equal to one thousand million hertz (cycles every second).

global positioning system /ɡləubl pə'ziSniN .sistəm/ noun C – a system that determines the user's location by comparing radio signals from several satellites.

Gnome /ɡə'nəum/ noun U – a project to build a complete user-friendly Unix-^ke desktop system based entirely on free software. It is part of the GNU project and part of the OpenSource movement.

GNU /ɡə'nu:/ noun U – a freely distributed portable Unix compatible software system.

GPRS /Gi: pi: a:r 'es/ noun U – abbreviation for general packet radio service.

GPS /Gi: pi: 'es/ noun C – abbreviation for global positioning system.

graphic equaliser /.ɡræfik 'i:kwə.laizə(r)/ noun C – an electronic device that uses slider controls to adjust the frequency response of an audio system.

graphical (user) interface /ɡræfikl 'intəfeis/ noun C – the part of an operating system that allows the user to interact with a computer using graphic images and a cursor.

grep /ɡrep/ noun U – a Unix command for searching through one or more text files for a specific text string.

GUI /'ɡu:i/ noun C – acronym for graphical user interface.

H

hack /hæk/ verb – to gain unauthorised access to a network system.

hacker /'hækə(r)/ noun C – a skilled programmer who attempts to gain unauthorised access to a network system.

half-duplex /'ha:f ˌdju:pleks/ adj – able to transfer data in both directions but only in one direction at a time, i.e. data can be transmitted or received but not at the same time.

handheld (computer) /'həndheld/ noun C – a small portable computer that can be held in one hand.

hang /hæN/ verb – to suddenly and unexpectedly stop processing during the execution of a program.

hard (disk) (drive) /ha:d (disk) (draiv)/ noun C – a common magnetic storage device that reads and writes data on metal disks inside a sealed case.

hardware /'ha:dweə(r)/ noun U – the physical components of a computer system.

(disk drive) head /hed/ noun C – the part of a disk drive that reads and writes data to the disk.

header /'hedə(r)/ noun C – the first section of a message that contains information about the content and transmission of the message including the sending and destination addresses.

headphone /'hedfəun/ noun C – sound output device that fits over the ears of the user.

help-desk/helpline /helpdesk, 'helplain/ noun C – a telephone service for helping users solve problems that occur on computer systems.

hierarchical storage management /haiəˌra:kikl 'sto:riɡ .mæniɡmənt/ noun U – a system of automatically moving files to different storage media depending on how often the files are used, i.e. the least used files are gradually archived. The less a file is used the more difficult it becomes to access it in the archive.

high-end package /hai end .pækiɡ/ noun C – a set of computer programs with a wide variety of complex features.

Higher National Certificate /haiə ˌnæʃənl sə'tifikət/ noun U – a British college qualification that can be gained through part-time or full-time study. It is usually obtained before studying for an HND.

Higher National Diploma /haiə ˌnæʃənl di'pləumə/ noun U – a British college qualification that usually requires a period of full-time study. It is more advanced than an HNC and not as advanced as a degree.

high-level language /.hai ˌlevəl 'læŋgwiɡ/ noun C – a programming language closer to human language than low-level computer languages such as machine code or assembly language.

high-level program /hai ˌlevəl 'prəugræm/ noun C – a computer program written using a high-level language.

highlight /'hailait/ verb – to select by marking on the display screen.

hijacking /'haiɡækiɴ/ noun U – a computer crime that involves redirecting anyone trying to visit a certain website elsewhere.

HNC /eiɕ en 'si:/ noun U – abbreviation for Higher National Certificate.

HND /eiɕ en 'di:/ noun U – abbreviation for Higher National Diploma.

Home button /'həum ˌbʌtən/ noun C – the button icon on a Web browser program that takes you to the starting webpage.

homepage /'həumpeiɡ/ noun C – the main start page of a website.

host /həust/ noun C – a computer that provides a service on a network / a program that carries a virus.

hot plug /'hot plʌg/ verb – to attach a device to a system without switching the system off and without causing problems to the system.

hover /'hovə(r)/ verb – to hold a cursor over an icon for a short period of time.

HSM /eiɕ es 'em/ noun U – abbreviation for hierarchical storage management.

HTML /eiɕ ti: em 'el/ noun U – abbreviation for hypertext markup language. A page description language that uses a system of tags for creating web pages.

hub /tʌb/ noun C – an electronic device at the centre of a star network topology.

humanoid /'hju:mənoid/ noun C – a robot with human characteristics.

hyperlink /'haipəlink/ noun C – a text or image in a webpage that causes a related webpage to be displayed or another program to be started when the user clicks on the hyperlink using the mouse.

hypertext markup language /.haɪpətekst 'maːkʌp .læŋgwɪg/ noun U – a page description language that has a set of tags that can be inserted into a document to make it act as a webpage. The tags determine how the document is displayed on the screen and marks the position of hyperlinks.

I

I/O /ai 'əu/ noun C – abbreviation for input/output.

IBM /ai bi: 'em/ noun U – abbreviation for International Business Machines, the largest computer company in the world. It launched the first personal computer called the IBM PC which quickly became the standard.

IC /ai 'si:/ noun C – abbreviation for integrated circuit. A complete electronic circuit built on a single silicon chip.

icon /'aikon/ noun C – a small picture used in a WIMP system to represent a program folder or file.

IEEE802.1l /ai i: i: 'i: ˌeit au ˌtu: point wAn 'wAn/ noun U – a wireless networking system standard approved by the American regulating organisation called the Institute of Electrical and Electronic Engineers.

I-frame /'ai freim/ noun C – the common name for an intra frame in an MPEG compressed file.

image editor /'imiG ˌeditə(r)/ noun C – a computer program that allows the user to make changes to images.

image map /'imiG mæp/ noun C – a graphic image with separate areas that contain hyperlinks to different parts of a website.

IMAP /'aimæp/ noun U – acronym for Internet mail access protocol.

inbox /'inboks/ noun C – the folder in an email program where emails are stored when they are first received.

incremental backup /ˌinkrəˌmentəl bækAp/ noun C – a type of backup that copies all the selected files that have been changed since the last full differential or incremental backup.

industrial scientific and medical band /in.dAstriəl (ˌsaiəntifik ənd 'medikl bænd/ noun U – a set of radiowave frequencies centred around 2.45GHz used for industrial scientific and medical devices and for Bluetooth devices.

information superhighway (the) /.infə.meiSn 'su:pəˌhaiwei/ noun U – an informal term for a global high-speed network providing communication services that are freely available to everyone, i.e. a highly-developed Internet system.

information technology /.infə.meiSn tek'noləGi/ noun U – the study and practice of techniques or use of equipment for dealing with information.

inheritance /in'heritəns/ noun U – a key feature of object-oriented programming that allows specific instances of a class to inherit all the properties of the class, e.g. squares are a specific instance of rectangles and inherit all the properties of rectangles.

in-house /in haus/ adj – done by employees of an organisation rather than people outside the organization.

initialise (the hard disk) /i'niSəlaiz/ verb – to reboot or restart the computer.

input /'input/ verb – to put data into a system.

input /'input/ noun U – data put into a system.

input device /'input di.vais/ noun C – a piece of equipment used for putting data into a computer.

instruction /in'strAkSn/ noun C – one line of a computer program.

integrated services digital network /.intiɡreitid ˌsE:visiz .diGitəl 'netwE:k/ noun U – a broadband network communications system that allows the ordinary analogue telephone system to carry digital signals including voice, data, text, graphics and video.

Intel /'intel/ noun U – the American company that designs and produces the electronic processors used in most of the computers in the world.

intelligent agent /in.teliGənt 'eiGənt/ noun C – a computer utility program that uses artificial intelligence to perform tasks for the user such as retrieving and delivering information and automating repetitive tasks.

interactive /intə'ræktiv/ adj – allows two-way communication so that the user can respond or interact with the system.

interface /'intəfeis/ noun C – the hardware or software that connects two systems and allows them to communicate with each other.

Internet (protocol) address /'intənet əˌdres/ noun C – a 32-bit code number assigned to every node on the Internet. It consists of a series of numbers that identify the major network and the sub-networks to which a node is attached and provides a path that gateways can use to route information from one machine to another.

(Microsoft) Internet Explorer /ˌintənet ik'splo:rə(r)/ noun U – a free browser program developed by the Microsoft Corporation.

Internet mail access protocol /ˌintənet ˌmeil .ækses 'prəutəkol/ noun U – a set of standards for accessing email messages stored on an email server. Initially only message headers are retrieved. Users can then organise or delete messages on the server and download individual messages.

Internet protocol /.intənet prəutəkol/ noun U – the basic set of standards for enabling computers to communicate over the Internet.

Internet service provider /ˌintənet 'sE:vis prəˌvaidə(r)/ noun C – an organisation that provides Internet connections for a fee.

Internet (the) /ˌintənet/ noun U – the connection of computer networks across the world.

interpreter /in'tɜ:pritə(r)/ noun C – a program that converts other programs into machine code line by line as the programs are being used.

intra frame /'intrə freim/ noun C – a type of image frame used in MPEG compression which contains only information in the picture itself.

intranet /'intrənet/ noun C – a computer network that is internal to an organisation and uses the TCP/IP protocol in the same way as the Internet.

IP /ai 'pi:/ noun U – abbreviation for Internet protocol. A part of the TCP/IP protocol used on the Internet.

IP address /ai 'pi: ə.dres/ noun C – abbreviation for Internet protocol address.

IP-layer /ai 'pi: ˌleiə(r)/ noun C – the IP part of a TCP/IP system.

IRC /ai a: 'si:/ noun U – abbreviation for Internet relay chat. An Internet service that allows user to have a conversation by sending text messages to each other in real-time.

iris recognition /'airis rekəg.niSn/ noun U – a process of identifying a user by scanning their eyes.

IS Manager /ai 'es ˌmæniGə(r)/ noun C – an abbreviated form of information systems manager. A person who manages a computer-based service that provides information that is useful to a particular organisation.

ISDN /ai es di: 'en/ noun U – abbreviation for integrated services digital network.

isolation adapter /.aisə'leiSn əˌdæptə(r)/ noun C – an electronic device that isolates a network system from high voltages and allows it to use the mains electricity cables for connecting computers together and transferring data.

ISP /ai es 'pi:/ noun C – abbreviation for Internet service provider.

IT /ai 'ti:/ noun U – abbreviation for information technology.

iteration /itə'reiSn/ noun C – a process that is repeated as long as certain conditions remain true.

J

Java /'Ga:və/ noun U – an object-oriented computer programming language that was developed by Sun Microsystems in the mid 1990s. Programs written in Java can be used on a wide range of operating systems. It is widely used for developing interactive applications for the Internet.

JavaScript /'Ga:vəskript/ noun U – a scripting language that allows simple programs to be embedded into HTML documents.

JPEG /'Gei peG/ noun U – abbreviation for joint photographic expert group the committee that devised a common standard for image file format and compression. JPEG compression is commonly used for photographic images in webpages because it creates very small files.

jukebox /'Gu:kboks/ noun C – informal name for an optical disk drive that stores many optical disks. The disks are loaded into the drive when required by the host computer.

JUMP command/instruction /GAmp kəˌma:nd, in.strAkSn/ noun C – a programming instruction that causes a program to change its normal sequence.

junk email /GANk 'i:meil/ noun U – unwanted and unsolicited email that is normally advertising or trying to sell something.

K

Kb/KB /'kiləbait/ noun C – abbreviation for a kilobyte. A unit of storage capacity equal to 1024 bytes.

Kbit/s /'kiləbits/ noun C – abbreviation for kilobits per second. A unit of signal speed equal to 1024 bits every second. A more common form is kbps.

kbps /.kiləbits pə 'sekənd/ noun C – abbreviation for kilobits per second. A unit of signal speed equal to 1024 bits every second.

KDE /kei di: i:/ noun U – a graphical user interface used with the Linux operating system.

kernel /'k3:nəl/ noun C – the lowest level layer at the core of an operating system. It deals with allocating hardware resources to the rest of the operating system and the application programs.

keyboard /'ki:bo:d/ noun C – the main electronic input device that has keys arranged in a similar layout to a typewriter.

keystroke /'ki:strəuk/ noun C – the process of pressing and releasing a key on a keyboard.

keyword /'ki:wE:d/ noun C – a word used to categorise documents or records in a file. Keywords can be used by a search engine to find relevant links on the Internet.

kHz /'kiləhE:ts/ noun C – abbreviation for kilohertz. A unit of frequency equal to 1000 cycles every second.

killer application /'kilər .æplikeiSn/ noun C – an application program that is particularly useful and popular, making a computer system very successful.

knowledge base /'noliG beis/ noun C – a collection of information that can be easily modified, revised and manipulated to enable the user to solve particular problems.

L

LAN /læn/ noun C – acronym for local area network.

language processor /'læNgwiG .prəusesə(r)/ noun C – software that performs computer language translation.

laptop (computer) /'læptop/ noun C – the largest type of portable computer.

laser printer /leizə ˌprintə(r)/ noun C – a printer that prints using toner powder and laser light on a photosensitive drum.

LCD /el si: 'di:/ noun C – abbreviation for liquid crystal display. An electronic display device that uses liquid crystal cells to control the reflection of light.

leased line /li:st 'lain/ noun C – a cable connection that is rented for use in a communications system.

library /'laibrəri/ noun C – a set of programmed functions that are made available for use by any program.

line driver /'lain ˌdraivə(r)/ noun C – an electronic circuit that provides high currents or voltages to other electronic circuits.

line size /'lain saiz/ noun C – the amount of date transferred eaih Lime there is a transfer between the main memory and cache memory.

link /liNk/ noun C – a common term used for a hyperlink, i.e. the connection of a webpage to another webpage or file.

Linux /'lainAks/ noun U – a clone of the Unix operating system created by Linus Torvalds for use on personal computers.

Linux distribution /1ainAks distri.bju:Sn/ noun C – the Linux-user term for a complete operating system kit complete with the utilities and applications needed to make it do useful things, e.g. command interpreters, programming tools, text editors, typesetting tools and graphical user interfaces.

load /ləud/ verb – to copy a program from a storage device into the computer's memory.

local area network /ləukl ˌeəriə 'netwE:k/ noun C – computers connected together over a small area such as a company department.

log /loG/ verb – to record the time that an event happened.

log /loG/ noun C – a record of when an event happened.

logon /loG 'On/ verb – to connect to a network system account normally using a password.

logic bomb /'loGik bom/ noun C – destructive code introduced into a program that is triggered by some event taking place on the computer system at a later time.

logic circuit /'loGik ˌsE:kit/ noun C – a digital electronic circuit that compares two or more inputs and gives an output according to a particular rule of logic.

look-up table /luk Ap teibl/ noun C – a method by which a program uses two sets of related records to find a required value. It is quicker than calculating the value using a formula but takes up more memory space.

loop structure /'lu:p ˌstrAkCə(r)/ noun C – see iteration.

low-level language /ləu levəl 'læNgwiG/ noun C – a computer language such as machine code or assembly language that is closer to the form that a computer understands than to that of a human language.

loyalty card /'loiəlti ka:d/ noun C – an electronic card that gives the owner discount on purchases at a particular store depending on how much they spend.

lpr /el pi: 'a:(r)/ noun U – a Unix command for printing a file.

ls /el es/ noun U – a Unix command for displaying a list of files in a directory.

LVD /el vi: 'di:/ noun U – abbreviation Low Voltage Differential. The interface used in Ultra2 and Ultra3 SCSI.

M

m /em/ noun C – abbreviation for metre. An international unit for distance.

mA /'miliæmp/ noun C – abbreviation for milliamp. A unit of current equal to one thousandth of an amp.

(Apple) Mac /mæk/ noun C – the common name for the Apple Macintosh range of computers. A type of personal computer manufactured by Apple Computer Incorporated.

MAC /mæk/ noun C – acronym for message-authentication code.

machine code /mə'Si:n kəud/ noun C – a computer language that consists entirely of a combination of Is and Os.

machine intelligence /mə'Si:n in'teliGəns/ noun U – another name for artificial intelligence.

Mac OS /mæk əu 'es/ noun C – the family of operating systems used on the Apple Macintosh range of computers.

macro virus /'mækrəu ˌvairəs/ noun C – a virus program in the form of a macro program.

magnetic tape /mæg.netik teip/ nounU – a magnetic storage medium in the form of a thin plastic ribbon wound on a reel or a cassette. It is commonly used for backing up data.

mail bombing /'meil .bomiN/ noun U – a computer crime that involves inundating an email address with thousands of messages slowing or even crashing the server.

mail client /'meil .klaiənt/ noun C – an email program that connects to an email server to send and receive email.

mail server /'meil ˌsE:və(r)/ noun C – a network service that stores email messages and enables email clients to send and receive emails.

mailbox /'meilbɒks/ noun C – a folder used by an email server to store a user's emails.

mailmerge /'meilmɜ:ɡ/ noun C – a wordprocessing facility that causes a mailing list to be automatically combined with a standard letter to produce a separate copy of the letter addressed to each person on the mailing list.

main memory /mein 'meməri/ noun – the electronic memory that holds the programs and data being used.

mainframe (computer) /'meinfreim/ noun C – the largest and most powerful type of computer. It is operated by a team of professionals.

mains line /'meinz lain/ noun C – the main electricity supply.

man /mæn/ noun U – a Unix command for viewing the online manual pages on a Unix system.

markup language /'ma:kʌp .læŋgwiɡ/ noun C – a set of tags that can be inserted into a document to indicate its layout and appearance.

massively parallel /ˌmæsivli 'pærəlel/ adj – being part of a system in which an application is processed by up to 200 or more processors at the same time. Each processor using its own operating systems and memory and working on a different part of the program.

Mb/MB /'meɡəbait/ noun C – abbreviation for a megabyte.

Mbit/s /.meɡəbit pə 'sekənd/ noun C – abbreviation for megabit per second. A unit of signal speed equal to 1 048 576 bits every second.

Mbps /.meɡəbits pə 'sekənd/ noun C – abbreviation for megabits per second. A unit of signal speed equal to 1 048 576 bits every second.

megabyte /'meɡəbait/ noun C – a unit of storage capacity equal to 1 048 576 bytes.

megahertz /'meɡəhɜ:ts/ noun C – a unit of frequency equal to 1 million cycles every second.

megohm /'meɡəum/ noun C – a unit of electrical resistance equal to 1 million ohms.

memory /'meməri/ noun U – the electronic part of a computer system that is used for temporarily storing the programs and data that are being used by the processor.

menu /'menju:/ noun C – a list of options displayed on a computer screen.

menu bar /'menju: ba:(r)/ noun C – a row of icons on a display screen that open up menus when selected.

message-authentication code /.mesiɡ ɔ:ˌṭenti'keiʃn kəud/ noun C – a number produced by a message-digest function that is used to make a message tamper-proof and provide message integrity.

message-digest function /.mesiɡ 'daiɡest .fʌnkʃn/ noun C – a program function that processes a message to produce a number called a message-authentication code. This number is then used to make a message tamper-proof.

message-integrity scheme /.mesiɡ in'tegrəti ski:m/ noun C – a system that allows the receiver of a message to detect whether someone has tampered with the message in transit.

metadata /'metədeitə/ noun U – data about data in a document.

metalanguage /'metəlæNgwiG/ noun C – a language from which you can create other languages.

MHz /'meɡəhE:ts/ noun C – abbreviation for megahertz.

microchip /'maikrəCip/ noun C – an electronic integrated circuit in a small package.

microcomputer /'maikrəukəmˌpju:tə(r)/ noun C – a personal computer. Smaller and less powerful than a mainframe or a minicomputer.

microprocessor /ˌmaikrəu' prəusesə(r)/ noun C – the main electronic chip in a computer. It can be thought of as the 'brain' of the computer because it does the main processing and controls the other parts of the computer. It is sometimes called the CPU.

Microsoft /'maikrəsoft/ noun U – the common name for the Microsoft Corporation. The company founded by Bill Gates that developed the MS-DOS and Windows operating systems and a variety of software commonly used on desktop computers.

microwave /'maikrəweiv/ noun C – a high-frequency electromagnetic wave used in data communication systems.

MIDI /'midi/ noun U – acronym for musical instrument digital interface. A standard for connecting musical instruments to computer systems.

minicomputer /'minikəm.pju:tə(r)/ noun C – a computer that is slightly less powerful and a little smaller than a mainframe.

Minix /'miniks/ noun U – a compact Unix clone written as a teaching aid by Professor Andy Tannenbaum.

mirroring /'mirəriN/ noun U – a technique used in RAID 1 systems where at least two hard disks are paired in such a way that the hard disk controller writes each byte of data to both disks. This ensures that a backup exists should the primary disk drive fail.

misdirection routine /misdə'rekSn ru:ˌti:n/ noun C – the part of a computer virus that enables it to hide itself by altering the normal sequence of instructions in another program.

mixing desk /'miksiN desk/ noun C – an electronic device used in audio recording that allows a number of audio inputs to be mixed together.

mkdir /em kei 'diə(r)/ noun U – a Unix and MS-DOS command for creating a directory.

MO /'em əu/ adj – abbreviation for magneto-optical. Used to describe storage devices that use a combination of magnetism and laser light.

mobile phone /.məubail 'fəun/ noun C – a wireless telephone that operates over a wide area

modem /'məudem/ noun C – short for modulator/demodulator. An electronic device that converts signals to enable a computer to be connected to an ordinary telephone line.

modulation /.modju'leiSn/ noun U – a process of combining a data signal with a carrier wave by causing the data signal to modify the amplitude frequency or phase of the carrier wave.

monitor /'monitə(r)/ noun C – the main output device used to display the output from a computer on a screen. See VDU.

MOO /mu:/ noun C – acronym for multi-user object oriented. An Internet virtual environment developed from multi-user adventure games that allows many users to interact.

motherboard /'mADəbO:d/ noun C – the main electronic circuit board inside a computer that holds and connects together all the main electronic components.

mouse /maus/ noun C – a common cursor control input device used with a graphical user interface. It commonly has two or three button switches on top and a ball underneath that is rolled on a flat surface.

mouse button /'maus .bAtən/ noun C – a switch on a mouse that is pressed to select an object on the screen.

mouse pointer /'maus ,pointə(r)/ noun C – a cursor image in the shape of an arrow that is controlled by a mouse and is used for pointing and selecting icons on the screen.

MouseKeys /'mauski:z/ noun U – a Microsoft Windows operating system feature that changes the function of the numeric keypad keys on a computer keyboard so that they can be used to control the screen cursor.

MP3 /em pi: 'Tri:/ noun U – abbreviation for MPEG Audio Layer 3. A Motion Picture Experts Group standard for audio compression.

MPEG /'empeg/ noun U – a standard video compression scheme. The term is an acronym for Motion Picture Experts Group a committee that develops standards for audio and video file formats and compression.

MS-DOS /em es 'dos/ noun U – abbreviation for Microsoft disk operating system. The command line operating system that was used in the first PCs.

multimedia /mAlti'mi:diə/ noun U – the combination of text graphics animation sound and video.

multimodal input /.mAlti.məudəl 'input/ noun U – the process of operating a user interface using a combination of types of input, e.g. keyboard and speech recognition.

MVS /em vi: 'es/ noun U – abbreviation for multiple virtual storage. It is the name given to a family of operating systems used on IBM mainframe computers.

mW /'miliwot/ noun C – abbreviation for milliwatt. A unit of power equal to one thousandth of a watt.

My Briefcase /mai 'bri:fkeis/ noun U – a Microsoft Windows feature that simplifies the process of copying and synchronising files between a desktop and a portable computer.

N

natural-language programming /ˌnæCrəl ˌlæNgwiG 'prəuGræmiN/ noun U – the process of writing programs using a computer language that is very similar to natural human language.

near-line storage /niə lain 'stO:riG/ noun U – the part of a hierarchical storage management system that stores infrequently-used files in a way that will allow them to be easily retrieved.

Net (the) /net/ noun U – the common name for the Internet.

NetPC /net pi: 'si:/ noun U – an industry specification for a low-cost basic Windows PC with an Intel processor designed for use on a multiuser network system. It is managed centrally and has no floppy disk drive CD-ROM drive or hardware expansion slots, i.e. it is a type of thin client.

Netscape Communicator /ˌnetskeip kə'mju:nikeitə(r)/ noun U – a widely used web browser package.

NetWare /'netweə(r)/ noun U – a widely-used LAN operating system produced by Novell Incorporated.

network /'netwE:k/ verb – to connect a number of computers and peripheral devices together.

network /'netwE:k/ noun C – a combination of a number of computers and peripheral devices connected together.

network computer /'netwE:k kəmˌpju:tə(r)/ noun C – a computer designed using the industry specification from Oracle and Sun Microsystems for a low-cost basic personal computer that can have an Intel processor or another type of processor and can use a Java-based operating system. It is designed for use on a multi-user network system and is managed centrally. It has no floppy disk drive, CD-ROM drive or hardware expansion slots, i.e. it is a type of thin client.

network guru /'netwE:k ˌguru:/ noun C – a person who is an expert in networking and gives talks and advice on the future development of networking.

network layer /'netwE:k leiə(r)/ noun C – the part of a network communications system that forms the data into packets and selects a route for the message.

network operating system /'netwE:k 'opəreitiN .sistəm/ noun C – an operating system that is used to administer and control a network allowing computers to share hardware and software while providing file security and backup facilities.

neural net(work) /'njuərəl net(wE:k)/ noun C – an artificial intelligence system that is capable of developing rules from given input so that it learns how to deal with more complex input.

newsgroup /nju:zɡru:p/ noun C – an Internet discussion group that uses a restricted area on a server computer to display messages about a common interest.

node /nəud/ noun C – a network terminal or point where a computer is connected to a network.

notebook (computer) /nəutbuk/ noun C – a portable computer that is about the same size as a piece of writing paper.

Novell /nəu'vel/ noun U – the common name for Novell Incorporated. The American company that designs and produces the Netware network operating system.

numeric keyboard /nju:ˌmerik 'ki:bo:d/ noun C – the section of a computer keyboard that includes keys for entering numerical digits (0-9) and mathematical operators (+-,/).

O

object /'obGekt/ noun C – an object-oriented programming module that has its own properties created by bundling data and program instructions together.

object-oriented programming /ˌobGekt ˌo:rientid 'prəuɡræmiN/ noun U – a type of programming where programs are made from combinations of predefined modules that can be used over and over again.

OCR /əu si: 'a:(r)/ noun U – abbreviation for optical character recognition.

(Microsoft) Office /'ofis/ noun U – a widely-used application package developed by the Microsoft Corporation that includes programs used in a typical office, e.g. a wordprocessor and spreadsheet.

office application / suite /'ofis æpli.keiSn, ˌswi:t/ noun C – a computer program or set of programs that are used in a typical office, e.g. a wordprocessor spreadsheet and database.

offline /of'lain/ adj – disconnected from a computer system or the Internet.

online /on'lain/ adj – connected to a computer system or the Internet.

OOP /əu əu 'pi:/ noun U – acronym for object-oriented programming.

Open Source /ˌəupen so:s/ adj – part of a system of software development where anyone is free to take a copy of the source code and extend develop or fix bugs in it.

operating system /'opəreitiN .sistəm/ noun C – the set of programs that control the basic functions of a computer and provides communication between the application programs and the hardware.

optical character recognition /ˌoptikl .kæriktə rekəɡ'niSn/ noun U – a process that enables a computer to scan and recognise printed characters using the reflection of light.

optical fibre /ˌoptikl faibə(r)/ noun C – a common name for glass fibre cable used in high speed networks. It enables data signals to be transmitted using laser light.

optical media /.optikl 'mi:diə/ noun U – data storage material that is written to or read from using laser light.

ORACLE /'orəkl/ noun U – a widely used database management system.

OS /əu 'es/ noun C – abbreviation for operating system.

OS X /əu es 'ten/ noun U – version 10 of the Apple Macintosh operating.

system. It is a modular OS and has a desktop with a 3-D appearance. It includes support for UNIX-based applications as well as older Mac applications.

OS/2 /əu es 'tu:/ noun U – a multitasking desktop operating system for PCs that was marketed by IBM.

Outlook Express /ˌautluk ik'spres/ noun U – a free graphical interface email program integrated into the Internet Explorer browser developed by the Microsoft Corporation.

output / autput/ noun U – the processed data or signals that come out of a computer system.

P

pA /'pi:kəuæmp/ noun C – abbreviation for picoamp. A unit of current equal to a millionth of a millionth of an amp.

(software) package /'pækiɢ/ noun C – an application program or collection of programs that can be used in different ways.

packet /'pækit/ noun C – a fixed size unit of data prepared for transmission across a network. Messages are normally divided into packets before transmission.

packet-switching /'pækit ˌswiɕiN/ noun U – a method of transferring data across a network by dividing it into packets and transferring the packets individually from node to node then putting the packets together again when they arrive at the destination.

page-description language /.peiɢ dis'kripSn .læNɡwiɢ/ noun C – a type of programming language that uses tags to define the layout of a document, e.g. HTML is a page-description language used to design webpages.

pager /'peiɢə(r)/ noun C – a small radio receiver which beeps to alert the wearer of messages or telephone calls. It displays the telephone number of the caller so the wearer can call back. Some pagers can display very short messages.

Palm Pilot /'pa:m ˌpailət/ noun U – a popular handheld personal organiser produced by 3Com.

palm-size PC /pa:m saiz pi: 'si:/ noun C – another name for a handheld IBM compatible computer.

palmtop (computer) /pa:mtop/ noun C – a portable computer that is small enough to be held in the palm of one hand. See handheld computer.

pane /pein/ noun C – a subsection of a graphical user interface window.

parity data /'pærəti .deitə/ noun U – extra data bits added to the end of units of data before transmission and then checked and added after transmission to see if the data has arrived accurately.

Pascal /pæs'kæl/ noun U – a high-level structured computer language named after the mathematician Blaise Pascal. It is often used in college computing courses to teach programming.

password /'pa:swE:d/ noun C – a secret code used to control access to a network system.

paste /peist/ verb – to insert a copy of data held in a computer's memory at a chosen position.

patch /pæɕ/ verb – to insert programming code into a computer program to fix or modify it in some way.

payload /'peiləud/ noun C – the part of a virus that carries out the threat such as displaying a slogan on the screen.

payroll package /'peirəul .pækiɢ/ noun C – a set of computer programs used for calculating pay cheques.

PC /pi: 'si:/ noun C – abbreviation for an IBM type of personal computer.

PC-DOS /pi: si: 'dos/ noun U – an operating system for desktop PC computers that is similar to MS-DOS.

PCMCIA /pi: si: em si: ai 'ei/ noun U – a type of interface for connecting credit-sized electronic upgrade cards to portable computers. Devised by the Personal Computer Memory Card International Association.

PDA /pi: di: 'ei/ noun C – abbreviation for personal digital assistant. A small handheld computer providing a variety of tools for organising work, e.g. a calendar, to do list, diary, address list, calculator, etc.

pen-based computer /pen beist kəm'pju:tə(r)/ noun C – a small computer that has a pen input device instead of a keyboard.

Pentium /'pentiəm/ noun C – a family of processors produced by the Intel Corporation.

peripheral /pə'rifərəl/ noun C – a piece of equipment that is connected to the central processing unit of a computer system.

personal computer /ˌpɜ:sənl kəm'pju:tə(r)/ noun C – a computer designed to be used by one person at a time.

personal organiser /ˌpɛ:sənl 'ɔ:gənaizə(r)/ noun C – see PDA.

P-frame /'pi: freim/ noun C – the common name for a predicted frame in an MPEG compressed file.

Photoshop /'fəutəuʃop/ noun U – an image-editing computer program produced by Adobe Systems Inc.

physical layer /'fizikl ˌleiə(r)/ noun C – the part of a network communications system that encodes the packets into the medium that will carry them and sends the packets along that medium.

piconet /pi:kəunet/ noun C – a set of very small low power wireless links consuming only picoamps of electricity that are set up between Bluetooth devices when they are within 10 metres of each other.

piggybacking /'pigibækiŋ/ noun U – a computer crime that involves using another person's identification code or using that person's files before he or she has logged off.

PIM /pim/ noun C – acronym for personal information manager. A computer program that provides a variety of tools for organising work, e.g. a calendar, to do list, diary, address list, calculator, etc.

PIN /pin/ noun C – an acronym for personal identification number. A unique number used by electronic systems to indicate who a person is.

platform /'plætfɔ:m/ noun C – a distinctive type of computer system that needs software to be written specifically for it, e.g. PC, Apple Mac, etc.

PlayStation /'pleisteiʃn/ noun U – a games console developed by the Sony Corporation.

pointer /'pointə(r)/ noun C – an arrow-shaped cursor.

polymorphism /.poli'mɔ:fizm/ noun U – a key feature of OOP programming by which different objects can receive the same instructions but deal with them in different ways.

POP /pop/ noun U – acronym for post office protocol.

port /po:t/ verb – to convert for use in another operating system or computer platform.

port replicator /'po:t ˌreplikeitə(r)/ noun C – a device that connects to a portable computer to make it easier to connect peripheral devices.

portable (computer) /pɒ:təbl/ noun C – a computer that is small and light enough to be carried from place to place. It can usually be powered by batteries.

post /pəust/ verb – to display a message in a computer newsgroup or bulletin board.

post office protocol /pəust ˌofis 'prəutəkol/ noun U – a message-retrieval protocol used by many mail clients to get messages from a server. It only allows you to download all messages in your mailbox at once and works in 'pull' mode, i.e. the receiving PC initiating the connection.

predicted frame /pri'diktid freim/ noun C – a type of image frame used in MPEG compression. A predicted frame only stores the differences in the image compared to the previous I frame or P frame.

presentation layer /.prezən'teiSn ˌleiə(r)/ noun C – the part of a network communications system that ensures the message is transmitted in a language that the receiving computer can interpret.

primary disk drive /'praiməri disk draiv/ noun C – the main disk drive in a computer. In a PC this is usually a hard disk known as the C drive.

Print Screen (key) /print skri:n/ noun C – the computer keyboard key that copies the current display screen image to memory or to the printer.

printed circuit board /ˌprintid 'sE:kit bo:d/ noun C – an electronic board that holds and connects the components of an electronic circuit.

printer /'printə(r)/ noun C – a common output device used for printing the output of a computer on paper.

private key /.praivət 'ki:/ noun C – secret code known only to the owner that is used for encrypting and decrypting messages.

procedural language /prə'si:Gərəl .læNgwiG/ noun C – a computer programming language that enables programs to be written using sections of code known as procedures. Each procedure performs a specific task.

processor /'prəusesə(r)/ noun C – the part of a computer that processes the data.

program /'prəugræm/ noun C – a set of instructions written in a computer language that control the behaviour of a computer.

program /'prəugræm/ verb – to write a set of instructions for controlling a computer using a computer language.

programmer /'prəugræmə(r)/ noun C – a person who writes computer programs.

programming /'prəugræmiN/ noun U – the processes of writing a computer program using a computer language.

programming language /'prəugræmiN ˌlæNgwiG/ noun C – a computer language used for writing computer programs.

protocol /'prəutəkol/ noun C – a set of agreed standards.

pseudocode /'sju:dəukəud/ noun C – a way of writing a description of a computer program using a mixture of natural language and computer language code.

public domain /ˌpʌblik dəˈmein/ noun U – a condition in which there is no copyright on a work such as a computer program allowing it to be freely copied and used.

public key /ˌpʌblik ˈki:/noun C – a secret code the owner makes available to others so that they can encrypt messages they are sending to the owner.

public-key cryptography /ˌpʌblik ki: kripˈtoɡrəfi/ noun U – a method of coding messages using public and private keys to prevent others from reading them.

pull mode /ˈpul məud/ noun U – a type of communication where the receiving computer initiates the connection.

pull-down menu /ˌpul daun ˈmenju:/ noun C – a list of choices that appear below a menu title on a display screen when the user clicks on the menu title using a mouse.

push operation /ˈpuʃ opə.reiʃn/ noun U – a communication where the sending computer initiates the connection.

R

radar /ˈreida:(r)/ noun U – a system of using the reflection of radio waves to detect an object and determine its location.

radio button /ˈreidiəu ˌbʌtən/ noun C – one of a set of mutually exclusive options in a dialog box, i.e. the user can only select one, causing the others to be deselected.

RAID /reid/ noun U – acronym for redundant array of inexpensive disks.

RAID level /ˈreid ˌlevl/ noun C – a particular arrangement of RAID array disks. Each RAID level is given a number with higher numbers indicating more elaborate methods for ensuring a computer can recover from hardware errors. The best known are RAID 0 to RAID 5.

RAM /ræm/ noun U – acronym for random access memory.

Rambus memory /ræmbʌs ˌmeməri/ noun U – a fast memory architecture commonly known as DRDRAM (or RDRAM) that is a possible future successor to SDRAM. It was originally developed by Rambus Inc.

random access memory /ˌrændəm ˈækses ˌmeməri/ noun U – a type of memory that can be accessed in any order. RAM is the main electronic memory of a personal computer and is used for storing the programs and data being used.

raw data /rɔ: ˈdeitə/ noun U – data that has not been processed.

RDBMS /a: di: bi: em ˈes/ noun C – abbreviation for relational database management system. A database system that links files together as required.

RDRAM /a: di: ˈræm/ noun U – abbreviation for Rambus dynamic random access memory. A new RAM technology capable of very high-speed transfer of data. See Rambus memory.

real-time /ˈri:l taim/ noun U – the immediate processing of computer data enabling interactive applications.

reboot /ri:ˈbu:t/ verb – to restart a computer operating system.

record /ˈrekɔ:d/ noun C – a section of a database made up of related database fields.

recorder (program) /ri'kɔ:də(r)/ noun C – a computer program that allows the user to create their own audio CDs with a writeable CD-ROM drive.

Recycle Bin /ri:'saikl bin/ noun U – the folder in Microsoft Windows operating systems where deleted files are stored.

redundant array of inexpensive disks /ri.dʌndənt əˌrei əv ˌinik.spensiv disks/ noun U – a storage system consisting of a set of hard disks that can be combined in different arrangements to store data in such a way that the data can be recovered if one or more of the disks fail.

reliable stream service /ri.laiəbl stri:m sɛ:vis/ noun U – a data management system provided by the TCP protocol to ensure that data is transferred across a network correctly. It structures and buffers the data flow, looks for responses, and takes action to replace missing data blocks.

resident /'rezidənt/ adj – is kept in the computer's memory.

resistor /ri'zistə(r)/ noun C – an electronic component that reduces the flow of current in a circuit.

resolution /.rezə'lu:ʃn/ noun C – a measure of the quality of a display screen in terms of the amount of graphical information that can be shown on the screen. This partly depends on the number of dots that make up the image.

resolution protocol /rezəˌlu:ʃn 'prəutəkol/ noun U – a set of standards for software used with internal look-up tables in a TCP/IP network for routing data through a gateway between networks.

restore /ri'stɔ:(r)/ verb – to put data back into its original location.

reverse engineering /riˌvɛ:s enʤi'niəriɲ/ noun U – to take an object apart to discover how it was originally designed and put together.

RF /a:r 'ef/ noun U – abbreviation for radio frequency.

right click /rait 'klik/ verb – to press and release the right-hand button on a mouse.

ring main /'riɲ mein/ noun C – the main electrical supply circuit in a building.

rip /rip/ verb – to extract songs from a CD and turn them into WAV files.

ripper /'ripə(r)/ noun C – a program that extracts songs from a CD and turns them into WAV files.

rm /a:r 'em/ noun U – a Unix command for deleting a file.

rmdir /a:r em 'diə(r)/ noun U – a Unix and MS-DOS command for deleting a directory.

robot /'rəubot/ noun C – a mechanical device controlled by a computer.

robotics /rəu'botiks/ noun U – the study of robot systems.

rocket science /'rokit .saiəns/ noun U – something requiring great intelligence or technical ability.

ROM /rom/ noun U – acronym for read only memory.

route /ru:t/ noun C – the path that is used to transfer data in a network.

route /ru:t/ verb – to move data from node to node on a network.

router /'ru:tə(r)/ noun C – an electronic device that links different networks or parts of a network. It determines the path that a signal should take to reach its destination.

rpm /a: pi: 'em/ noun C – abbreviation for revolutions per minute.

rule /ruːl/ noun C – the name given to patterns found in data when using neural networks.

run /rʌn/ verb – to execute a program, i.e. to get a program to process the data.

rwho /aː huː/ noun U – a Unix command for displaying a report of who is currently logged in to the local network.

S

s/w /ˈsoftweə(r)/ noun U – abbreviation for software.

salami shaving /səˈlaːmi ˌʃeiviŋ/ noun U – a computer crime that involves manipulating programs or data so that small amounts of money are deducted from a large number of transactions or accounts and accumulated elsewhere.

SAP /sæp/ noun U – a widely used enterprise resource planning tool program.

save /seiv/ verb – to copy a program or data to a storage device.

scan /skæn/ verb – to copy text or graphics using a scanner.

scanner /ˈskænə(r)/ noun C – an optical input device that uses the reflection of light to copy text or graphics into a computer.

(monitor)(display) screen /skriːn/ noun C – a computer output device used for displaying text and graphic images.

scroll /skrəul/ verb – to move through displayed information smoothly on the screen either horizontally or vertically.

scrollbar /ˈskrəulbaː(r)/ noun C – the part of a graphical user interface window that allows the user to move through a document by clicking or dragging with the mouse.

SCSI /es siː es ˈai/ noun U – acronym for small computer systems interface. A standard way of connecting peripheral devices to a personal computer system. It is often used to connect hard disks and CD-ROM drives in server computers.

SDRAM /es diː ˈræm/ noun U – abbreviation for synchronous dynamic random access memory. A type of fast memory that uses a separate clock signal in addition to the normal control signals.

search engine /ˈsəːʃ ˌendʒin/ noun C – a program designed to find information on the World Wide Web according to data entered by the user. Search engines are usually accessed from special websites.

sector /ˈsektə(r)/ noun C – a formatted section of a circular magnetic track used for storing data on a disk.

seek time /ˈsiːk taim/ noun C – the amount of time taken by a disk drive to find a particular track on a disk.

segment /ˈsegmənt/ noun C – a subdivision of data created by a network communications transport layer for which a checksum is generated.

serial /ˈsiəriəl/ adj – designed to transfer data sequentially, i.e. one data bit after another.

serial number /ˈsiəriəl ˌnʌmbə(r)/ noun C – a number that uniquely identifies a product.

serial port /ˈsiəriəl pɔːt/ noun C – the small connector at the back of the system unit of a personal computer that is used to connect a serial device such as a serial

mouse or a modem. Two serial ports labelled COMI and COM2 are usually provided on a PC.

server /'sE:və(r)/ noun C – a main computer that provides a service on a network.

service tag number /'sE:vis tæɡ ˌnAmbə(r)/ noun C – a number used to identify a computer for maintenance agreements.

session layer /'seSn 1eiə(r)/ noun C – the part of a network communications system that opens communications and has the job of keeping straight the communications among all nodes on the network. It sets boundaries for the beginning and end of a message and establishes whether the messages will be sent half-duplex or full duplex.

SGML /es Ɡi: em 'el/ noun U – abbreviation for Standard Generalised Markup Language.

shareware /'Seəweə(r)/ noun U – software that is distributed freely and only paid for if the user decides to keep it.

shell /Sel/ noun C – a graphical user interface for an operating system.

shell script /Sel skript/ noun C – a text file that contains a sequence of commands for a UNIX-based operating system. In DOS operating systems a shell script is called a batch file.

shift key /'Sift ki:/ noun C – the computer keyboard key that is held down to produce uppercase letters.

signup /sain Ap/ verb – to register with a service.

SimCity /sim'siti/ noun U – a well-known computer simulation game in which the users control various aspects of running a virtual city.

simple mail transfer protocol /simpl meil 'trænsfE: .prəutəkol/ noun U – a set of standards for sending email from an email client and transferring email between server computers on the Internet.

simulation /.simju'leiSn/ noun C – a programmed virtual environment that imitates a real or planned system.

site /sait/ noun C – a common name for a website.

site map /'sait mæp/ noun C – a webpage that is used to show the overall layout of a website.

skin /skin/ noun C – a computer program that is used to change the interface of another program, e.g. to change the screen display on an MP3 player program.

SM band /es 'em bænd/ noun U – common name for the Industrial Scientific and Medical frequency band.

smart card /'sma:t ka:d/ noun C – a plastic card containing a processor and memory chip. It can be used to store large amounts of confidential data.

smart card reader /'sma:t ka:d ˌri:də(r)/ noun C – a device used for reading smart cards.

smart device /'sma:t di.vais/ noun C – a device that contains an embedded processor and memory.

smart phone /'sma:t fəun/ noun C – a telephone that contains an embedded processor and memory and can process data, e.g. translate English into German, Japanese and French in real time.

SMS /es em 'es/ noun U – abbreviation for Short Message Service. A method of sending text messages that are 160 characters in length or shorter over a mobile phone.

SMTP /es em ti: 'pi:/ noun U – abbreviation for simple message transfer protocol.

software /softweə(r)/ noun U – the programs and data used in a computer.

software engineering /'softweər enGiˌniəriN/ noun U – the discipline of designing high quality software solutions.

software house /'softweə haus/ noun C – a company that designs and produces software.

software piracy /'softweə .pairəsi/ noun U – a computer crime that involves unauthorised copying of a program for sale or distributing to other users.

soundcard /'saundka:d/ noun C – the electronic circuit expansion board in a computer that is used to process audio signals and connect to and control a microphone loudspeaker or headphone.

source code /'so:s kəud/ noun C – programming code that has to be processed by a compiler or translator to make object code for use in a computer.

spam /spæm/ noun U – unsolicited email sent to large numbers of people indiscriminately usually advertising or trying to sell a product.

speaker /'spi:kə(r)/ noun C – common term for a loudspeaker. An output device for providing sound output.

spectrum analyser /'spektrəm .ænəlaizə(r)/ noun C – an instrument that plots a graph of frequency parameters for a complete frequency band.

splitter-based service /'splitə beist ˌsE:vis/ noun C – a DSL system that separates the data signal from the phone line as it enters a building and sends it to a DSL modem.

spoofing /'spu:fiN/ noun U – a computer crime that involves tricking a user into revealing confidential information such as an access code or a credit card number.

spread spectrum /'spred .spektrəm/ noun U – a radiowave system that switches rapidly between different frequencies in a frequency band allowing a number of devices to share the same frequency band without interfering with each other.

spreadsheet (program) /'spredSi:t/ noun C – a type of application program with an array of cells that is used for calculating formulas.

SQL /es kju: 'el/ noun U – abbreviation for structured query language. A language used for searching databases.

standalone /'stændələun/ adj – not connected to a network.

standard generalised markup language /.stændəd .Genrəlaizd 'ma:kAp .læNgwiG/ noun U – the complex metalanguage from which both HTML and XML were created.

Start (button) /sta:t/ noun C – an icon on the bottom left corner of Microsoft Windows operating system desktops that allows the user to access programs and data and to close down the system.

start bit /'sta:t bit/ noun C – a data bit that marks the beginning of a data block in a network transmission.

Start menu /'sta:t ˌmenju:/ noun C – the list of choices that opens upon the -display screen when the user clicks the Start button in a Microsoft Windows desktop.

start-stop transmission /sta:t .stop trænz'miSn/ noun C – another name for asynchronous transmission where data is sent one byte (or character) at a time.

static earthing band /.stætik 'ɜ:TiN bænd/ noun C – a strip of material that is wound round the wrist of a repair technician and connected to earth to prevent the build up of static electricity which could destroy electronic components.

status bar /'steitəs ba:(r)/ noun C – a narrow band displayed across the bottom of a window in a Microsoft Windows application to display useful information for the user, e.g. number of pages in a document.

stealth virus /'stelT .vairəs/ noun C – a type of virus that hides itself making it hard to detect.

stop bit /'stop bit/ noun C – a data bit that marks the end of a data block in a network transmission.

storage device /'sto:riG di.vais/ noun C – a piece of equipment used for reading from and writing to a storage medium.

storage medium /'sto:rid3 .mi:diəm/ noun C – a material used for storing programs and data.

streaming /'stri:miN/ noun U – a process of downloading and storing the next part of a data signal while the first part is being used. In this way the data signal, e.g. an audio or video is fed to the slower destination device at a steady rate.

string /striN/ noun C – a series of data characters which can be a mixture of letters or numbers.

striping /'straipiN/ noun U – a process where data is spread across all drives in a RAID array rather than filling up one disk with data before writing to the next disk in the array.

structured language /ˌstrAkCəd 'læNgwiG/ noun C – a computer programming language that requires the programmer to write programs made up of self-contained units or procedures.

structured programming /.strAkCəd 'prəuGræmiN/ noun U – the process of writing a program using a structured programming language.

subfolder /'sAbˌfəuldə(r)/ noun C – a storage area that provides a subdivision of a folder so that stored files can be organised into smaller groups.

submenu /'sAb.menju:/ noun C – a list of choices that is displayed when the user clicks on an item in a menu.

sub-network /'sAb ˌnetwE:k/ noun C – a self-contained part of a larger network.

subpage /'sAbpeiG/ noun C – a webpage that gives further detailed information about part of the information on a main webpage.

sub-program /'sʌb ˌprəuɡræm/ noun C – a small program that performs a specific function and is part of a larger program.

subset /'sʌbset/ noun C – a small group of related data that is part of a larger set of data.

supercomputer /'su:pəkəmˌpju:tə(r)/ noun C – the most powerful type of mainframe computer.

superset /'su:pəset/ noun C – a larger group of objects that include a smaller set of objects.

supervisor (program) /'su:pəvaizə(r)/ noun C – the most important program in the operating system. It is resident and controls the entire operating system. It loads other operating system programs into memory when they are needed.

support analyst /sə'po:t ˌænəlist/ noun C – a person who provides help to computer users by studying their requirements and designing systems to provide for their needs.

support engineer /sə'po:t enɡiˌniə(r)/ noun C – a professional who provides help for computer users by designing, building, and maintaining computer systems.

support line /sə'po:t lain/ noun C – a telephone line that can be used to get help with hardware or software problems. See helpdesk/helpline.

support technician /sə'pɒt tekˌniʃn/ noun C – a person who maintains and troubleshoots problems with computers.

surf /sɛ:f/ verb – to browse webpages on the Internet in an unplanned way.

surge protector /'sɛ:ɡ prəˌtektə(r)/ noun C – an electronic device that protects equipment from damage due to sudden high voltage or current in the power supply.

SVGA /es vi: ɡi: 'ei/ noun U – abbreviation for super video graphics array. A video screen display standard that provides 1024X768 or 1280X1024 pixel resolution with up to 16.7 million colours.

swipe card /'swaip ka:d/ noun C – a plastic card with a magnetic strip running across it containing confidential data.

SXGA /es eks ɡi: 'ei/ noun U – abbreviation for super extended graphics array. An IBM video screen display standard similar to SVGA that provides 1024X768 or 1280X1024 pixel resolution with up to 16.7 million colours.

synch byte /'siŋk bait/ noun C – a start or stop bit pattern that marks the beginning or end of a transmitted data block.

synchronise /'siŋkrənaiz/ verb – to cause different processes to occur at the same time.

synchronous /siŋkrənəs/ adj – occurring at regular intervals and in step with other systems usually controlled by an electronic clock circuit.

synthesiser /'sinθəˌsaizə(r)/ noun C – a device that uses electronic circuits to generate sounds.

system bus /'sistəm bʌs/ noun C – the sets of connectors that carry signals between system components such as the processor and memory in a computer.

system tray /'sistəm trei/ noun C – a section at the far right of a Microsoft Windows task bar that holds icons for the clock and other programs that run constantly in the background.

systems administrator /sistəmz ədˌminəstreitə(r)/ noun C – a person who maintains a multi-user computer system.

systems analysis /'sistəmz ə.næləsis/ noun U – the study of a system to determine how it can be computerized.

systems analyst /'sistəmz .ænəlist/ noun C – a person who designs or modifies information systems to meet users' requirements. This includes investigating feasibility and cost-producing documentation and testing prototypes of the system.

systems manager /'sistəmz ˌmæniGə(r)/ noun C – a person who manages a computer system.

systems program / software /'sistəmz .prəuGræm, ˌsoftweə(r)/ noun C/U – a program or set of programs that is used to control the basic functions of a computer system, e.g. operating system programs.

systems programmer /'sistəmz ˌprəuGræmə(r)/ noun C – a person who specialises in writing systems software such as operating system programs.

systems programming /'sistəmz .prəuGræmiN/ noun U – the writing of systems programs.

T

TA /ti: 'ei/ noun C – abbreviation for terminal adapter.

tab /tæb/ noun C – a dialog box component that is used to switch between different sets of data.

tab (key) /tæb/ noun C – the computer keyboard key that is used to move the cursor to the next tabulation point in a wordprocessor program so that data can be spaced evenly on the screen.

tag /tæg/ noun C – a label used in a markup language such as HTML It is attached to a piece of text to mark the start or the end of a particular function.

tape /teip/ noun U – a magnetic storage medium commonly used for storing backup files.

tape changer /'teip ˌCeinGə(r)/ noun C – a backup device that allows different magnetic tapes to be used when required during a backup operation.

taskbar /'ta:skba:(r)/ noun C – a Microsoft Windows desktop component that indicates what programs are currently being used and allows the user to switch between them.

TCP /ti: si: 'pi:/ noun U – abbreviation for transfer control protocol. A part of the TCP/IP protocol used on the Internet.

TCP/IP /ti: si: pi: 'ai pi:/ noun U – abbreviation for transmission control protocol/Internet protocol. The official set of standards for determining the form of the signals used for transmitting data on the Internet.

technophobic /teknə'fəubik/ adj – having a fear or strong dislike of technology and technological devices.

telecomms /'telikomz/ noun U – common term for telecommunications.

telecommunications /ˌtelikəmju:ni'keiSnz/ noun U – branch of technology concerned with communications over long distances.

telecommunications engineer /ˌtelikəmju:ni' keiSnz enGiniə(r)/ noun C – a person who works with systems concerned with communications over long distances.

telecommute /telikə'mju:t/ verb – to communicate with your office by computer, telephone and fax while working a distance from your office, e.g. at home.

telephony /tə'lefəni/ noun U – the science of audio communication through electric devices. It commonly refers to software that will make a computer act like a telephone.

teleworking /'teliwE:kiN/ noun U – the process of working at home while communicating with your office by computer, telephone and fax. See telecommute.

teller machine /'telə mə͵Si:n/ noun C – a machine used for taking payments in large shops and supermarkets.

telnet /'telnet/ noun U – acronym for teletype network. An Internet service that allows a user to connect to a multi-user server using a computer as a terminal.

terabit /'terəbit/ noun C – a unit of storage capacity equal to 1 009 511 627 776 bits.

terminal /'tɜ:minəl/ noun C – a network device used to input and output data (usually a basic computer).

terminal adapter /'tɜ:minəl ə͵dæptə(r)/ noun C – a device for connecting an ISDN system to an existing telephone line.

text editor /'tekst ͵editə(r)/ noun C – a computer program for editing basic data or program text, i.e. like a basic word processor.

TFT display /ti: ef 'ti: di.splei/ noun C – abbreviation for thin film transistor display. A type of LCD screen display commonly used in portable computers. It uses a separate transistor to control each pixel on the display.

thin client /'Tin .klaiənt/ noun C – a low-cost centrally-managed basic computer with a keyboard and display screen processor and memory but no CD-ROM drive, floppy disk drive or expansion slots, e.g. a NetPC or a network computer (NC).

third-generation GSM /TE:d Genə.reiSn Gi: es 'em/ noun U – the third generation of the Global System for Mobile communication standard. It is the standard for mobile users around the world.

throughput /'Tru:put/ noun U – the amount of data that passes through a system in a given period of time.

toggle-box /'toglboks/ noun C – a screen icon in Windows Explorer that opens or closes a folder to show or hide its subfolders when the user clicks on it using a mouse.

tooltip /'tu:ltip/ noun C – a label that appear on the screen when the user holds the mouse pointer over an icon in a Microsoft Windows system.

topology /tə'poləGi/ noun C – the physical layout of a network.

tower chassis /'tauə ͵Sæsi/ noun C – a personal computer case that stands on end and can be placed on the floor unlike the normal desktop case that sits flat on a desk under the monitor.

track /træk/ noun C – a formatted circular magnetic storage area on a computer disk.

traffic /'træfik/ noun U – the volume of signals or data that passes through a network system.

transaction processing /trænz'ækSn .prəusesiN/ noun U – the processing of computer transactions by updating the computer file as each transaction takes place rather than storing them until later to be processed as a batch.

transistor /træn'zistə(r)/ noun C – a solid state electronic switch or amplifier.

transmission control protocol /trænz.miSn kən.trəul 'prəutəkol/ noun U – a set of standards for the delivery of error-free data in communications between computers. It comes into operation once a data packet is delivered to the correct Internet address and application port. It manages the communication exchanges and provides reliable stream service by structuring and buffering the data flow looking for responses and taking action to replace missing data blocks.

transponder /træns'pondə(r)/ noun C – a device that responds to received coded radio signals by automatically transmitting a different coded signal.

transport layer /'tra:nspo:t 1eiə(r)/ noun C – the part of a network communications system that protects the data being sent. It subdivides the data into segments and creates checksum tests. It can also make backup copies of the data.

trapdoor /ˌtræp'do:(r)/ noun C – a technique used in a computer crime that involves leaving within a completed program an illicit program that allows unauthorised - and unknown –entry.

Trojan (horse) /'trəuGən/ noun C – a technique used in a computer crime that involves adding concealed instructions to a computer program so that it will still work but will also perform prohibited duties. In other words it appears to do something useful but actually does something destructive in the background.

troubleshoot /'trAblSu:t/ verb – to find and fix faults in a system.

troubleshooter /'trAblˌSu:tə(r)/ noun C – a person who finds and fixes faults in a system.

TTS /ti: ti: 'es/ noun U – abbreviation for text to speech. A system where a computer reads text to the user using a speech synthesiser.

tuned /tju:nd/ adj – set to operate on the same frequency.

TV (set) /ti: vi:/ noun C – abbreviation for television. A television set is the actual television device used for displaying the video signals.

twisted-pair (cabling) /ˌtwistid peə(ɾ)/ noun U – a common type of network cable that uses two wires twisted together to reduce interference from external signals.

typesetting /'taipsetiN/ noun U – preparation for printing.

U
UDP /ju: di: 'pi:/ noun U – abbreviation for user datagram protocol.

undo /An'du:/ verb – to restore a file to the condition it was in before the last change was made.

unencrypt /Anen'kript/ verb – to remove the encryption from a file.

uniform resource locator /ˌju:nifO:m ri'zo:s ləuˌkeitə(r)/ noun C – the unique address of a webpage.

uninterruptible power supply /.Anintə.rAptəbl 'pauə sə.plai/ noun C – a battery backup system that automatically provides power to a computer when the normal electricity source fails.

universal mobile telecommunications system /ˌjuːnivEːsl .məubail telikəˌmjuːniˈkeiSnz ˌsistəm/ noun U – a third-generation, broadband, packet-based communications system based on the Global System for Mobile (GSM) communication standard. It provides the same services including the transmission of text-digitised voice video and multimedia to mobile computer and phone users throughout the world.

Unix /ˈjuːniks/ noun U – a popular multi-user multitasking operating system originally designed for mainframe computers, A wide variety of versions exist.

update /ˈApdeit/ noun C – a change that provides the latest version.

update /Apˈdeit/ verb – to bring up to date, i.e. to change into the latest version.

upgrade /ˈApgreid/ noun C – a change that improves the features or performance of a system.

upgrade /Apˈgreid/ verb – to add components to improve the features or performance of a system.

upload /Apˈləud/ verb – to copy a file from a client computer to a server in a network.

UPS /juː piː ˈes/ noun C – abbreviation for uninterruptible power supply.

upstream /ˈApstriːm/ noun U – the signal path for receiving communications from a client computer to a server in a network.

URL /juː aːr ˈel/ noun C – abbreviation for uniform (or universal) resource locator.

Usenet /ˈjuːznet/ noun U – an Internet service that allows users to communicate by means of newsgroups.

user /ˈjuːzə(r)/ noun C – the person using a computer.

user datagram protocol / juːzə .deitəgræm ˈprəutəkol/ noun U – a set of standards for creating a data address in a TCP/IP message. It is used to indicate what application the message is supposed to contact and provides the final routing for the data within the receiving system.

user-authentication system /juːzər oːˌTentiˈkeiSn ˌsistəm/ noun C – a system that identifies users. This can be done using digital certificates.

username /ˈjuːzəneim/ noun C – the network account name assigned to a particular user.

utility (program) /juːˈtiləti/ noun C – a program included with an operating system that can perform useful common routine tasks or housekeeping operations, e.g. formatting disks or copying files.

UTMS /juː tiː em ˈes/ noun U – abbreviation for Universal Mobile Telecommunications System.

V

V /volt/ noun C – abbreviation for volt, the international unit of voltage.

VB /viː biː/ noun U – abbreviation for Visual Basic.

VCR /viː si ˈaː(r)/ noun C – abbreviation for video cassette recorder.

VDU /viː di ˈjuː/ noun C – abbreviation for visual display unit. Another name for a computer monitor.

verify /'veri͵fai/ verb – to check for accuracy.

video /'vidiəu/ noun U – signals containing picture information.

video (cassette) recorder /'vidiəu ri͵ko:də(r)/ noun C – a device for recording video signals onto magnetic tape cassettes.

video memory /'vidiəu ͵memori/ noun U – the memory used to store graphics data on a graphics card.

videoconferencing /͵vidiəu'konfərənsiN/ noun U – a form of communication over a network that uses video cameras so that the people taking part can see and hear each other.

virtual /'vE:Cuəl/ adj – computer-simulated enabling the user to experience something without needing its physical presence.

virtual reality /͵vE:Cuəl ri'æləti/ noun U – a simulated three-dimensional environment that surrounds the user and is generated by a computer.

virus /'vairəs/ noun C – a program written with the purpose of causing damage or causing a computer to behave in an unusual way.

virus-check /'vairəs Cek/ verb – to check for viruses.

VIS /viz/ noun U – abbreviation for viewable image size. The actual size of the image that can be seen by the user on a computer display screen.

Visual Basic /.viZuəl 'beisik/ noun U – a general-purpose programming language with a graphical interface. It is particularly suitable for use by beginners learning how to program.

visualisation technology /͵viZuəlai͵zeiSn tek'noləGi/ noun U – systems and devices used to create a virtual reality environment.

VMS /vi: em es/ noun U – an operating system used by DEC VAX minicomputers.

voice /vois/ noun C – a stored musical instrument sound sample used to produce realistic music output in a wavetable sound card.

voice clip /'vois klip/ noun C – a short sound recording of the human voice.

voice recognition /'vois rekəg͵niSn/ noun U – a system that can respond to words spoken by a human being.

voice synthesis /'vois .sinTəsis/ noun U – the generation of a human-sounding voice using electronic circuits.

voice synthesiser /'vois ͵sinTəsaizə(r)/ noun C – an electronic device that generates sounds that represent the human voice.

VR /vi: 'a:(r)/ noun U – abbreviation for virtual reality.

W

wallpaper /'wO:lpeipə(r)/ noun C – the background graphics on a Microsoft Windows desktop.

Wap /wæp/ noun U – acronym for wireless application protocol. A set of standards for allowing users to send emails and access information including video transmissions from the Internet on a mobile phone.

WAV /wæv/ noun U – an audio file format.

wavetable system /'weivteibl .sistəm/ noun C – a system used in some soundcards for more accurately creating the sound of real musical instruments by reproducing a wide frequency range from a small number of original samples.

Web address /'web ə‚dres/ noun C – the Internet address of a webpage.

Web developer /'web di‚veləpə(r)/ noun C – a person who is employed to create websites.

Web mail /'web meil/ noun U – a type of email that is accessed from webpages.

Webserver /web‚sE:və(r)/ noun C – a server computer that stores and provides access to websites.

Web space /'web speis/ noun U – disk storage space on a web server used for storing webpages.

Web (the) /web/ noun U – common name for the World Wide Web.

Webmaster /'webma:stə(r)/ noun C – a person who administers a Web server.

webpage /'webpeiG/ noun C – a hyperlinked document in a web network system.

web-ready appliances protocol /web ‚redi ə.plaiənsiz 'prəutəkol/ noun U – a set of standards for enabling domestic appliances to be connected to the Web and to communicate with each other.

website /'websait/ noun C – a set of related pages on the World Wide Web.

wildcard /'waildka:d/ noun C – a symbol used in computer commands and for searching databases. It represents any character or combination of characters, e.g. using an asterisk searching for *ed would find all words ending in ed.

window /'windəu/ noun C – a rectangular screen area containing a program folder or file in a WIMP system.

(Microsoft) Windows /'windəuz/ noun U – a graphical user interface operating system front-end to MS-DOS developed by the Microsoft Corporation. It has been gradually developed into a full operating system.

Windows Explorer /‚windəuz ik'splO:rə(r)/ noun U – a Microsoft Windows program that allows the user to see the files and folders on all the disks attached to the computer. It can be used for general housekeeping such as moving or deleting files.

Windows Media Player /‚windəuz 'mi:diə ‚p1eiə(r)/ noun U – a Microsoft Windows program for playing multimedia files including audio and video.

wipe (a disk) /waip/ verb – to delete all the files stored on a disk.

wirelessly /'waiələsli/ adj – using radio signals without the need for connecting wires or cables.

WML /‚dAbl ju: em 'el/ noun U – abbreviation for wireless markup language. A language similar to HTML used for designing webpages suitable for mobile phones.

(Microsoft) Word /wE:d/ noun U – a widely-used wordprocessing program developed by the Microsoft Corporation. It is a component of the Microsoft Office package.

wordprocessing /‚wE:d'prəusesiN/ noun U – the process of typing and editing text using a wordprocessor.

wordprocessor /‚wE:d'prəusesə(r)/ noun C – a type of computer application program used for typing and editing text documents.

workstation /'wE:ksteiSn/ noun C – a powerful desktop computer used by power users for work that requires a lot of processing, e.g. graphic design.

World Wide Web (the) /wE:ld ˌwaid 'web/ noun U – an information service on the Internet that allows document pages to be accessed using hyperlinks.

WORM /wE:m/ noun U – acronym for write once read many. A standard for optical storage devices that only allows data to be recorded on to a particular optical disk once but allows the data to be read from the disk over and over again. It is commonly used for archiving data.

WRAP /ræp/ noun U – acronym for Web-ready appliances protocol. A set of communications system standards that enable web-connected appliances to communicate.

writeable CD-ROM drive /.raitəbl si: di: 'rom draiv/ noun C – a compact disk drive that allows the user to write data onto a CD as well as read data stored on the CD.

write-back cache /'rait bæk kæS/ noun C – a buffer storage system where the processor writes changes only to the cache and not to main memory. Cache entries that have changed are flagged as 'dirty' telling the cache controller to write their contents back to main memory before using the space to cache new data.

write-through cache /rait Tru: kæS/ noun C – a buffer storage system where the processor writes directly to both the cache and main memory at the same time.

WWW /.dAblju: .dAblju: 'dAblju:/ noun U – abbreviation for the World Wide Web. The Internet service used for connecting to multimedia webpages.

X

X (windowing) (system) /eks/ noun U – a windowing system used with different versions of Unix.

X.25 /eks .twenti 'faiv/ noun U – the International Telegraphic Union packet-switching data communications standard for connecting computers and a public network.

XGA /eks Gi: 'ei/ noun U – abbreviation for extended graphics array. An IBM display screen standard with a resolution of 1024X768 pixels and up to 65,536 colours.

XML /eks em 'el/ noun U – abbreviation for extensible markup language.

Y

Yahoo /jæ'hu:/ noun U – the name of a popular Internet search engine website.

RESOURCES

1. Dinos Demetriades. Information Technology. Workshop. Oxford University Press. 2003. 40 p.

2. Eric H. Glendinning, John McEwan. Oxford English for Information Technology. Oxford University Press. 2002. 224 p.

3. Materials from http://www.bbc.co.uk/

4. Materials from http://www.bbcworldwide.com/

5. Materials from http://ru.wikipedia.org/wiki/BBC

<div align="center">

EDUCATIONAL PUBLICATION

Zavalevskaya Elena Vasilevna, Minich Natalia Philipovna

INFORMATION TECHNOLOGY

TEXTBOOK

</div>