Міністерство транспорту та зв'язку України
Міністерство освіти і науки України
Державний університет інформаційно-комунікаційних технологій

В.М. Богуш, В.А. Мухачов

Криптографічні застосування елементарної теорії чисел

Навчальний посібник

Київ – 2006

УДК 003.26
ББК 81-8
Б73

Рекомендовано до видання Вченою радою Державного університету інформаційно-комунікаційних технологій (протокол № 4 від 01.12.2005 р.)

Рецензенти:

доктор технічних наук, професор Кузнецов Г.В.
доктор технічних наук, професор Шелест М.Є.

Богуш В.М., Мухачов В.А.

Криптографічні застосування елементарної теорії чисел. Навчальний посібник — К.: ДУІКТ, 2006. — 126 с.

Приведена структурована сукупність відомостей щодо застосування методів елементарної теорії чисел для побудови та тестування параметрів криптосистем.

Для студентів, що навчаються за освітнім напрямом "Інформаційна безпека", а також спеціалістів, що займаються забезпеченням криптографічного захисту інформації.

ISBN 966–2970-06–1

ПЕРЕДМОВА

Сучасні методи обчислювальної теорії чисел, що застосовуються у криптографії, розвинуті завдяки дослідженням стійкості асиметричних криптосистем, перші з яких появилися у 70-ті роки XX сторіччя. На теперішній час ці методи набувають все більшої актуальності внаслідок масового застосування засобів криптографічного захисту інформації та впровадження нових криптоалгоритмів у комп'ютерних системах та мережах.

Мета начального посібника — показати роль та методику застосування теоретико-числових методів для оцінки якості параметрів криптоалгоритмів.

Матеріал викладено відповідно до певної компактної логічної структури виходячи з мінімальних вимог до початкової підготовки читача. Для розуміння матеріалу читачу потрібно володіти курсом вищої математики для технічних вищих навчальних закладів.

У першому розділі посібника висвітлені основні принципи та проблеми криптології. Особлива увага приділена викладенню у структурно-логічному взаємозв'язку термінів і понять, що дозволяють усвідомити основну сутність алгоритмічних проблем криптографії.

Другий і третій розділи присвячені використанню властивостей модульних операцій та арифметичних алгоритмів для вибору параметрів криптоперетворень відповідно в симетричній та асиметричній криптографії.

До кожного з розділів посібника наведено значний перелік контрольних тестів, що дозволяють здійснити ретельну перевірку засвоєних знань.

ОСНОВНІ ПОЗНАЧЕННЯ

n	—	натуральне число
(e, d, n)	—	криптосистема RSA з параметрами e, d, n
p	—	просте число
q	—	степінь простого числа
$\oplus$	—	операція порозрядного додавання за модулем 2
$\varphi(n)$	—	функція Ейлера
$a \mid b$	—	a ділить b
$a \nmid b$	—	a не ділить b
$p \parallel n$	—	p власний дільник n, тобто p ділить n і $p \neq 1, n$
(a, b),НСД(a, b)	—	найбільший спільний дільник чисел a і b
$[a, b]$,НСК(a, b)	—	найменше спільне кратне чисел a і b
$GF(q)$	—	поле з q елементів
$ord_p a$	—	порядок числа a за модулем p
$a \equiv b (\mathrm{mod} m)$	—	a порівнянне з b за модулем m
$a \not\equiv b (\mathrm{mod} m)$	—	a не порівнянне з b за модулем m
$\left(\frac{a}{p}\right)$	—	символ Лежандра
$\left(\frac{a}{m}\right)$	—	символ Якобі
$\forall$	—	квантор загальності (для усіх)
$\exists$	—	квантор існування (існує)
$\|$	—	конкатенація елементів та блоків даних
$\lfloor x \rfloor$	—	максимальне ціле число, що не перевищує x

Розділ 1

ЗАГАЛЬНІ ПРИНЦИПИ І МЕТОДИ СУЧАСНОЇ КРИПТОЛОГІЇ

1.1 Актуальність проблеми надійності діючих криптосистем. Причини та висновки

Впровадження та активне використання сучасних інформаційних технологій суттєво підвищили уразливість інформації, що циркулює в інформаційно-телекомунікаційних системах.

Несанкціоноване спотворення, копіювання, знищення інформації на теперішній час торкається не тільки процесів, що відносяться до сфери державного управління, але й процесів, що зачіпають інтереси фізичних осіб. Виникла низка нових задач, що мають практичне значення, наприклад, задача нотаріальних рішень в автоматичному режимі. Виявилось, що методи, необхідні для розв'язання вказаних задач, розроблені й використовуються у криптології.

Криптологія — наука, що вивчає методи побудови та аналізу систем захисту інформації, основаних на математичних перетвореннях інформації з використанням секретних параметрів. Такі системи називаються криптографічними.

За якої причини є актуальною проблема надійності діючих (тільки що впроваджених) **криптосистем**?

Глобальні причини полягають у наступному:

1. Відсутність повних формальних критеріїв якості криптосистем, а також неможливість виконання на практиці (у повному обсязі) вимог, виходячи з яких розробники могли би обґрунтувати висновок про достатній рівень захисту інформації.

2. При масовому застосуванні криптосистем, проявляються малоймовірні ситуації, в яких криптографічна стійкість знижується.

Додаткове джерело потенційної ненадійності криптосистем — можливість створювати криптосистеми зі свідомо внесеними слаб-

костями (лазівками).

З приведених положень можна зробити наступні висновки.

Необхідно зберігати в таємниці виявлені недоробки в діючих криптосистемах або методи несанкціонованого доступу до відкритої інформації до усунення недоліків. Для користувача це призводить до економічних проблем, для розробника, крім того, виникає питання професійної некомпетентності. Проте, найважливішим є те, щоб недоліки системи не були виявлені зловмисниками.

Невідворотними є приховані змагання між **криптографами** і **криптоаналітиками**, а також боротьба за кращі параметри обчислювальних потужностей у глобальному масштабі.

Нереально розраховувати на допомогу із-зовні для розвитку криптографічного потенціалу — необхідно розраховувати тільки на свої сили.

Необхідна уніфікація криптосистем відповідно до стандартів, прийнятих в розвинених країнах (політичний та економічний фактор).

Крім того, діючі криптосистеми необхідно модернізовувати або замінювати відповідно до світової практики зміни їх поколінь (як правило, зміна поколінь зв'язана з досягненням нового рівня обчислювальних потужностей в криптографічно розвинених країнах).

Якщо діючі криптосистеми розглядати як потенційно ненадійні, то виникає проблема їх супроводження протягом усього терміну їх експлуатації.

Таким чином необхідне випереджальне оволодіння технологіями, які забезпечували би захист інформації на сучасному науково-технічному рівні, інакше можна назавжди залишитися поза межами прогресу в даній галузі.

1.2 Загальна симетрична система секретного зв'язку (за К. Шенноном). Загальні визначення і терміни криптографії

Криптографія — це дисципліна, що вивчає принципи, засоби та математичні методи перетворення інформації з метою прихо-

вування смислової структури даних, а також для захисту від їх несанкціонованого використання або підробки. Основним методом є шифрування. При шифруванні можуть використовуватися секретні параметри — ключі.

Шифрування — це взаємно однозначне перетворення повідомлення з метою приховування його смислу від сторонніх осіб. **Вхідний текст повідомлення** — це **відкритий текст**, а результат шифрування — **шифрований текст** (**шифротекст**).

Криптограма — шифротекст, підготовлений для передавання каналами зв'язку.

Розшифрування криптограми — операція, зворотна до шифрування відкритого тексту. Здійснюється при наявності секретного параметра (ключа).

Криптосистема в широкому розумінні — документи, пристрої, обладнання та відповідні методи, використання яких (у сукупності), забезпечує засоби зашифрування і розшифрування.

Криптосистема у вузькому розумінні — система шифрування, тобто методи, що забезпечують зашифрування і розшифрування при обміні інформацією.

Ключі — секретні параметри, що використовуються при розшифруванні. При зашифруванні секретні параметри використовуються не завжди.

Дешифрування — одержання відкритого тексту без попереднього знання ключів.

Модель системи секретного зв'язку була запропонована К. Шенноном в роботі "Теорія зв'язку в секретних системах", що опублікована в 1949 році.

За Шенноном **криптографічна система** (рис. 1.1) представляє собою параметричне сімейство оборотних відображень множини можливих повідомлень у множину криптограм. Кожне відображення є шифруванням. Вибір відображення здійснюється за допомогою випадкового секретного параметра — ключа.

Ключ також дозволяє вибрати **зворотне перетворення** (розшифрування). Ключ повинен бути доступним відправнику і одержувачу в необхідний момент.

Передбачається, що ключі розсилаються безпечним каналом —

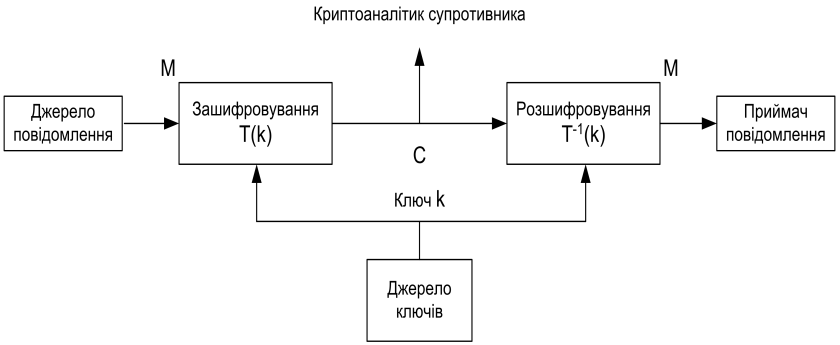

Рис. 1.1. Модель системи секретного зв'язку

методом, який не обговорюється у даній моделі.

Така система секретного зв'язку носит назву **симетричної криптосистеми** (симетрія користувачів відносно знання секрету).

Модель супротивника. Доступний для перехоплення шифротекст, відомий алгоритм шифрування та його параметри, за виключенням ключа (принцип відкритості, загальнодоступності системи).

Практична стійкість шифроперетворення полягає у трудомісткості одержання відкритого тексту аналітичним способом, без знання ключа, за допомогою найкращих з існуючих на сьогоднішній день алгоритмів.

Вважається, що в моделі Шеннона за допомогою шифрування вирішується задача забезпечення тільки **конфіденційності інформації** (даних).

1.3 Загальна ідея односпрямованої функції з лазівкою. Асиметричні криптосистеми

Для практичної реалізації моделі Шеннона, необхідність побудови захищеного каналу для ключового обміну породжує так звану **проблему безпечного розповсюдження ключів**.

При використанні засобів шифрування в автоматизованих сис-

темах оброблення інформації, крім того, виникає **проблема нотаріального підтвердження істинності даних**, що призводить до проблеми так званого **підпису електронних повідомлень**.

Обидві ці задачі, без використання захищеного каналу зв'язку, вдалося вирішити в так званій **моделі криптосистеми з "відкритим" ключем**, яка була запропонована В. Діффі та М. Хеллманом в 1976 році (рис. 1.2).

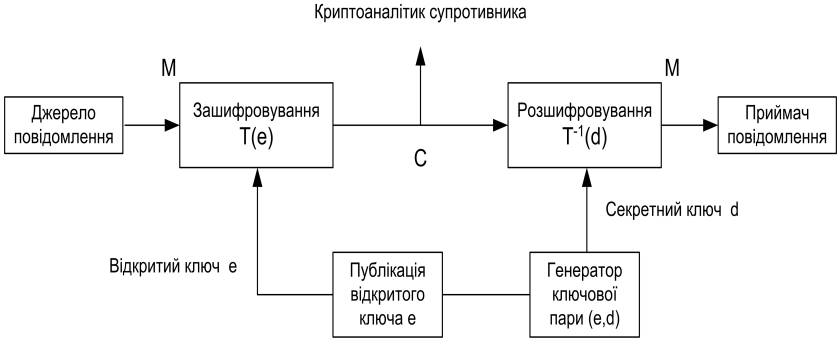

Рис. 1.2. Модель криптосистеми з відкритим ключем

Відмінність моделі системи секретного зв'язку В. Діффі та М. Хеллмана від моделі К. Шеннона у тому, що вона є асиметричною в тому сенсі, що користувачі по відношенню до секретного параметра нерівноправні.

Ключ відомий тільки одержувачу повідомлення і представляє собою пару (e, d), де **підключ** e (так званий **відкритий ключ**) служить ключем зашифрування, а підключ d призначений для розшифрування. При цьому тільки d є секретним параметром (так званий **секретний**, **особистий**, або **приватний ключ**).

Ключ d відомий тільки одержувачу повідомлень, які відправники повинні шифрувати, використовуючи ключ e. Стійкість системи забезпечується за рахунок особливих властивостей шифроперетворення, яке представляє собою так звану **однобічну** (**односпрямовану, важкооборотну**) **функцію** з "**лазівкою**". Обчислення значення такої функції (від відкритого тексту і параметра e) повинно бути нескладним, у той же час обернену до неї

функцію знайти обчислювальним способом неможливо без знання секретної інформації "лазівки", пов'язаної з секретним ключем d.

Такі криптосистеми називаються **асиметричними** або **системами з відкритими ключами**.

Строго кажучи, існування важкооборотних функцій не доведено. Проте, можна відзначити, що деякі перетворення мають властивості, що наближаються до властивостей односпрямованих функцій.

Яким чином проблема безпечного розповсюдження ключів вирішується за допомогою асиметричних криптосистем? Для цього кожний, хто бажає передати ключ для асиметричної криптосистеми своєму абоненту, перешифровує його ключем e цього абонента (припускається, що асиметрична криптосистема створена заздалегідь і відкритий ключ є опублікованим) та надсилає результат шифрування відкритим каналом. Такий ключ хоча і відомий супротивнику, але виключається можливість його модифікації або підміни.

Односпрямована функція з "лазівкою" гарантує безпеку, оскільки розшифрувати повідомлення можна тільки знаючи ключ d, а його знає тільки потрібний абонент. На практиці запропонований механізм не є безпечним. Для забезпечення захисту відкритого ключа від модифікації і підміни необхідно вводити систему так званих **центрів сертифікації відкритих ключів** (у глобальному масштабі).

Ідея використання односпрямованих функцій з "лазівкою" у криптографії дозволила вирішити цілий ряд задач, пов'язаних із захистом інформації. Найбільш часто зустрічаються наступні задачі.

Забезпечення цілісності даних. **Цілісність даних** — це властивість даних, яка дозволяє одержати їх у вихідному вигляді після передачі, не зважаючи на зміни, передбачені протоколом системи зв'язку.

Автентифікація абонента — перевірка того, що абонент дійсно є тією особою, за яку себе видає.

Автентифікація повідомлення — перевірка того, що повідомлення надіслано без змін від заявленого відправника до призначеного кореспондента.

1.4 Елементарні шифри. Поняття ключового потоку. Основні типи шифрів

Шифр заміни (шифр підстановки) — метод шифрування, при якому кожний знак відкритого тексту взаємно однозначно замінюється одним або декількома знаками деякого алфавіту. **Шифр простої заміни** замінює кожний знак вхідного алфавіту на деякий знак з того ж алфавіту, причому на один і той самий знак, незалежно від місця у відкритому тексті. Ключами для шифрів заміни є **таблиці заміни**.

Шифри перестановки відрізняються від шифрів заміни тим, що при зашифруванні буква відкритого тексту переходит не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, в результаті чого букви розташовуються на нових місцях, тобто переставляются.

Ключі шифрів перестановки представляються у вигляді підстановок розміром до довжини тексту включно. Шифри перестановки мають багато різновидів, які відрізняються в основному тим, яким способом породжуються ключі. Наприклад, для цього використовуються різноманітні варіанти розташування відкритих текстів на площині у фігурах різної конфігурації та виписування їх за законом, який тримається у секреті.

Шифри гамування. Розповсюджені приклади шифру даного типу основані на операції додавання чисел за деяким модулем. Символи алфавіту відкритого тексту, попередньо замінені на числа, "додаються" до елементів деякої числової послідовності, яка є ключем і називається **гамою**. Процедура зашифрування називається **гамуванням**, а кількість m знаків в алфавіті — **модулем гамування**. Звичайно, операція гамування пов'язана тільки з так званим модульним додаванням, але це не обов'язково: часто використовують оборотні табличні функції.

Поняття ключового потоку

Розглянемо пронумерований список Δ усіх дозволених перетворень, які могли би виникнути у процесі шифрування повідомлень довільної довжини за допомогою даної криптосистеми. Назвемо Δ

списком шифроперетворень.

Процес зашифрування можна записати як послідовність номерів шифроперетворень, вибраних на кожному такті шифрування. Позначимо цю послідовність через Г та назвемо **ключовим потоком**. Послідовність Г є аналогічною функції вибору стану деякого автомата. Вона визначається ключом і номером такту.

Властивості цієї послідовності відображають якість шифру і визначають його класифікацію. Наприклад, якщо список Δ містить тільки перетворення додавання за модулем n, кожне з фіксованим числом c_i, $(i = 0, 1, ...n-1)$, то шифр є **шифром гамування за модулем** n. У цьому випадку ключовий потік можна представити гамою безпосередньо.

Основні типи шифрів

Потоковим шифром називається система шифрування, в якій на кожному такті використовується змінний алгоритм шифрування, що вибирається за допомогою елементів ключового потоку зі списку шифроперетворень.

Ключовий потік визначається вихідними ключовими даними та номерами тактів шифрування, аж до того, що розглядається.

Необхідність застосування **криптографічного захисту інформації** в мережах ЕОМ, в базах даних, в системах електронних платежів, призвела до широкого застосування програмних засобів шифрування. При цьому стало очевидним, що програмна реалізація багатьох потокових шифрів поступається у швидкодії шифрам іншого типу, так званим блоковим шифрам.

Блоковим шифром називається система шифрування, яка використовує на кожному такті постійний, вибраний до початку шифрування, залежно від ключів, алгоритм. Оскільки зашифрування повинно бути оборотним перетворенням, то блочні шифри є шифрами заміни з дуже великим алфавітом. Наприклад, алгоритм стандарту шифрування ГОСТ 28147-89 у режимі простої заміни, взаємно однозначно відображає множину потужності 2^{64} на себе.

1.5 Загальні алгоритмічні проблеми, пов'язані зі стійкістю сучасних криптоалгоритмів

Для блокових шифрів стійкість пов'язана з оцінкою якості **віртуальних таблиць заміни**, тобто таблиць заміни, які неможливо надати на носії повністю із-за великого обсягу даних. Блоковий шифр являє собою сукупність віртуальних таблиць заміни. Ключ використовується для вибору таблиці, яка є незмінною у процесі шифрування окремого повідомлення.

Одним із загальних підходів до аналізу потокових шифрів є **декомпозиція** автомата на відповідні вузли і аналіз вихідних послідовностей вузлів та шифратора у цілому.

Для нерівноймовірного відкритого тексту корисно розглядати гамування як спотворення гами знаками відкритого тексту. У даному випадку, ігноруючи викривлення, можна записати співвідношення, що властиві істинній гамі, для складання відповідних систем рівнянь для знаків шифротексту, а потім розглядати їх як системи рівнянь зі спотвореними правими частинами для гами. Відносно спотворень відомий лише розподіл ймовірностей.

Даний підхід приводить до загальної **проблеми розв'язку систем рівнянь зі спотвореними параметрами**. Загальна проблема відновлення спотвореної рекуренти є **алгоритмічною проблемою**, на якій ґрунтується стійкість значної частини потокових шифрів.

Для деяких шифрів алгоритмічні проблеми, що забезпечують складність їх дешифрування, можна сформулювати конкретно. Нехай h і m додатні цілі числа. Позначимо залишок від ділення h на m через $h \bmod m$.

Якщо p — велике просте число, то за відповідних умов функція $f(x) = a^x \bmod p$ поводить себе як односпрямована. Таким чином, обернена функція (дискретний логарифм) не може бути обчислена за прийнятний час і задача дискретного логарифмування є алгоритмічною проблемою.

Аналогічні властивості має і степенева функція виду

$$g(x) = x^e \bmod n,$$

де $n = pq$.

Для обернення цієї функції достатньо вирішити задачу розкладання числа n на співмножники, проте ця задача також є алгоритмічною проблемою теорії чисел.

До вказаних **теоретико-числових проблем** зводиться стійкість переважної більшості сучасних асиметричних криптоалгоритмів.

1.6 Основна теорема арифметики. Вираз найбільшого спільного дільника двох чисел за допомогою діофантового рівняння. Розширений алгоритм Евкліда

Числа $1, 2, 3, ...$ називаються **натуральними**. Число 0, а також числа виду $\pm a$, де a — натуральне число, називаються цілими числами. Відношення двох цілих чисел називається **раціональним дробом** і є результатом ділення одного числа на інше. Ділення на ноль не визначене.

Простим число називається натуральне число, для якого існують тільки два нерівні натуральні дільники, а саме: 1 та дане натуральне число.

Основна теорема арифметики: кожне натуральне число єдиним чином, з точністю до порядку співмножників, представляється у вигляді добутку степенів простих чисел.

Найбільшим спільним дільником двох цілих чисел a и b називається найбільше ціле число, яке ділить як a, так і b. Позначення: (a, b) або НСД(a, b).

Найменшим спільним кратним цілих чисел a і b називається найменше натуральне число НСК(a, b), яке ділиться як на a, так і на b.

Виразимо НСД(a, b) за допомогою **діофантового рівняння**. Нехай $d = (a, b)$. Тоді існують цілі числа x, y, що є розв'язком рівняння $xa+yb = d$. Якщо $d = 1$, числа a і b називаються **взаємно простими**.

Розв'язок x, y, d рівняння $xa + yb = d$, $a > b$, можна знайти за допомогою **розширеного алгоритму Евкліда**. Очевидно, достатньо розв'язати рівняння при позитивних a і b.

Розглянемо схему розширеного алгоритму Евкліда на прикладі чисел 15 і 25. Ми будемо знаходити залишки і (неповні) частки від ділення двох чисел, тобто користуватися рівностями виду $A = kB + r$, де всі числа цілі і $0 \le r < B$. Оскільки повинна виконуватися нерівність $a > b$, то замінимо позначення: $r_0 = 25$, $r_1 = 15$.

Випишемо послідовність рядків.

$r_0 = 25$, $x_0 = 1$, $y_0 = 0$,

$r_1 = 15$, $x_1 = 0$, $y_1 = 1$ $(d_2 = 1, r_2 = 10)$.

Пояснення. Ділимо r_0 на r_1 із залишком. Одержуємо: $r_0 = d_2 r_1 + r_2$, тобто $25 = 1 \cdot 15 + 10$, звідки $d_2 = 1, r_2 = 10$. Перевіряємо $r_2 = 0$? Ні — працюємо далі. Обчислюємо x_2, y_2: $x_2 = x_0 - x_1 d_2 = 1$, $y_2 = y_0 - y_1 d_2 = -1$. Формуємо наступний рядок: r_2, x_2, y_2.

Вихідними даними для кроку 2 будуть рядки r_1, x_1, y_1 (з попереднього кроку) і r_2, x_2, y_2. З цими рядками діємо аналогічно. Якщо наступний залишок від ділення дорівнює нулю — виписуємо рішення (див. нижче).

$r_2 = 10$, $x_2 = 1$, $y_2 = -1$ $(d_3 = 1, r_3 = 5)$,

$r_3 = 5$, $x_3 = -1$, $y_3 = 2$ $(d_4 = 2, r_4 = 0)$.

При формуванні наступного рядка залишок $r_4 = 0$ — виписуємо розв'язок з даних попереднього кроку:

НСД$(25, 15) = r_3 = 5$, $x = x_3 = -1$, $y = y_3 = 2$, $xr_0 + yr_1 = -25 + 30 = 5$.

1.7 Лишки за модулем. Визначення відношення порівняння. Обчислення зворотного елемента. Китайська теорема про залишки

Кожне натуральне число можна розділити із **залишком**: $a = km + r$, де $0 \le r < m$.

Залишок називається **лишком** (у даному випадку — числа a) за модулем m.

Визначення. Два цілих числа a і b порівняні за модулем m, якщо їх різниця ділиться на m. Аналогія — тіло, що рухається по колу періодично попадає в одну й ту ж точку кола, хоча проходить різний шлях. Довжини шляхів "порівняні за модулем довжини ко-

ла". Відношення порівняння чисел a і b за модулем m записується у вигляді $a \equiv b(\mathrm{mod} m)$, $a \equiv b(m)$, $a \equiv b \bmod m$, або $a = b(m)$ і т.ін. З алгоритму Евкліда випливає, що для взаємно простих чисел a і m завжди існує число b, таке що $ab = 1 \bmod m$. Це число називається **оберненим** до a **за модулем** m и позначається a^{-1}. Якщо числа a і m не взаємно прості, то a^{-1} не існує.

Для простого модуля кожний ненульовий лишок має обернений. Поняття оберненого елемента використовується, зокрема, при розв'язувані порівнянь виду

$$ax \equiv b \bmod m,$$

якщо $(a, m) = 1$.

Наступне твердження називається **китайською теоремою про залишки**.

Нехай числа $m_1, m_2 ... m_k$ попарно взаємно прості і $M = m_1, m_2 ... m_k$. Тоді існує єдиний за модулем M мінімальний невід'ємний розв'язок системи порівнянь

$$x \equiv c_i \pmod{m_i}.$$

При цьому

$$x \equiv \sum_{i=1}^{k} c_i M_i N_i \pmod{M},$$

де $M_i = m_1 \cdot m_2 \cdot ... \cdot m_{i-1} \cdot m_{i+1} \cdot m_k$, $N_i \equiv M_i^{-1} \bmod m_i$.

Дійсно, у виразі для x за модулем m_i тільки один додаток не порівняний з нулем і дорівнює c_i.

Зазначимо, що коефіцієнти M_i, N_i, $\mathrm{mod} M$ можна обчислити заздалегідь і розв'язувати системи, підставляючи праві частини в лінійну форму.

1.8 Порядок числа за модулем. Функція Ейлера. Теореми Ейлера і Ферма. Первісний корінь за простим модулем

Розглянемо степені числа a за модулем m, де a і m взаємно прості.

Нехай $m = 11$. Лишки степенів числа 2 для показників $0, 1, 2, ..., 10$ такі: $1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1$. Аналогічно, ті ж степені числа 3 порівнянні відповідно з числами $1, 3, 9, 5, 4, 1, 3, 9, 5, 4, 1$.

У кожному випадку наявна періодичність. Найменша довжина періоду числа a за модулем m називається **порядком** (показником) **числа a за модулем m**.

Порядок числа a за модулем m позначається $ord_m a$.

Порядки чисел за модулем m різні. Існують числа, що є порядком одночасно для всіх чисел, взаємно простих з m. Одне з них дорівнює значенню так званої **функції Ейлера** $\varphi(m)$, що визначається як кількість чисел в послідовності $1, .., m$, взаємно простих з m.

Функція Ейлера є мультиплікативною: якщо $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$ і $\varphi(1) = 1$.

Нехай $m = p_1^a p_2^b ... p_s^t$, тоді

$$\varphi(m) = p_1^{a-1} p_2^{b-1} ... p_s^{t-1}(p_1 - 1)...(p_s - 1).$$

Теорема Ейлера. Якщо $(a, m) = 1$, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

З теореми Ейлера випливає **мала теорема Ферма**:

$$a^{p-1} \equiv 1 \pmod{p},$$

де p — просте число, $(a, p) = 1$.

Ці теореми дуже корисні для скорочення обчислень.

Визначення. Елемент називається **первісним коренем** (первісним, або примітивним елементом) за модулем m, якщо його порядок за модулем m дорівнює $\varphi(m)$. При $m = p$ первісні корені існують завжди.

Множина лишків з модульними операціями за простим модулем p становить так зване просте поле Галуа з p елементів. Позначення: $GF(p)$. На відміну від поля раціональних чисел поле $GF(p)$ є скінченним.

Відомо, що в кожному скінченному полі існує первісний елемент (генератор поля). Степені первісного елемента g представляють усі ненульові елементи поля. Отже, порівняння $g^x \equiv a \bmod p$ розв'язне для ненульових лишків a за модулем p.

Показник x в цьому порівнянні називається **дискретним логарифмом числа a за основою g**. Дискретні алгоритми часто називають індексами і позначають $inda$ або $ind_g a$.

Елемент g є первісним коренем за модулем p тоді і тільки тоді, коли виконуються співвідношення:

$$\forall_i g^{\frac{p-1}{p_i}} \neq 1(p),$$

де

$$(p-1) = \prod_{i=1}^{k} p_i^{a_i}.$$

1.9 Порівняння першого степеня з одним невідомим

Вірним є твердження про те, що якщо обидві частини істинного порівняння і модуль помножити або розділити націло на одне й те ж число, то в результаті отримаємо істинне порівняння.

Виходячи з нього можна досліджувати порівняння виду

$$ax \equiv b \pmod{m}.$$

Виявляється, ці порівняння можуть мати декілька розв'язків, мати єдиний розв'язок або не мати розв'язків зовсім. Якщо $(a, m) = 1$, то розв'язок єдиний: $x \equiv a^{-1}b$. Розв'язки існують тоді і тільки тоді, коли $d = (a, m)$ ділить b. В останньому випадку розглядається порівняння виду

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

з єдиним розв'язком x_0. Усі інші розв'язки є числами виду

$$x_0 + j\frac{m}{d} \bmod m,$$

де $j = 0, 1, ..., d-1$ (очевидно, вони не перевищують m).

Важлива теорема. Кількість коренів многочлена від однієї змінної з коефіцієнтами $GF(p)$, що лежать в $GF(p)$, не перевищує степеня многочлена.

Порівняння першого степеня дозволяють дослідити властивості степеневих порівнянь виду

$$x^n \equiv a(p).$$

Розв'язність порівняння

$$x^n \equiv a(p)$$

є еквівалентною виконанню умови

$$a^{(p-1)/d} \equiv 1 \pmod{p}, \quad d = (n, p-1).$$

Дійсно, переходячи до індексів, одержимо $n(indx) = inda \bmod (p-1)$. Необхідна та достатня умова розв'язності останнього порівняння полягає в тому, щоб $inda$ ділився на $d = (n, p-1)$, тобто $inda \equiv 0 \bmod d$.

Помноживши модуль і обидві частини останнього порівняння на

$$\frac{p-1}{d},$$

одержимо

$$\frac{p-1}{d} inda \equiv 0 \pmod{p-1},$$

звідки випливає, що співвідношення

$$inda \equiv 0 \pmod{d}$$

є еквівалентним умові

$$a^{(p-1)/d} \equiv 1 \pmod{p}.$$

Відомий наступний результат: нехай p — просте число, $(a, p) = 1$, $h = ord_p a$, тоді порівняння

$$x^h \equiv 1 \pmod{p}$$

має $\varphi(h)$ рішень.

Наслідок. При $h = \varphi(p)$ число первісних коренів дорівнює

$$\varphi(p-1).$$

1.10 Загальні відомості про побудову криптосистеми RSA

Криптографічна система RSA є асиметричною криптосистемою, основаною на **односпрямованій функції з лазівкою**, за яку вибрана **степенева функція в кільці лишків цілих чисел** за складеним (біпростим) модулем $n = pq$. Стійкість системи приводиться до складності **задачі факторизації** великих біпростих чисел.

Криптосистеми RSA на кожному такті шифрування перетворює двійковий блок відкритого тексту m довжини $size(n)$, що розглядається як ціле число $< n$, за допомогою піднесення до степеня за модулем n: $c = m^e(n)$. Показник степеня і модуль є елементами **відкритого ключа**. Лазівка забезпечується за рахунок секретного ключа d, побудованого таким чином, що для всіх m виконується співвідношення $m^{ed} = m(n)$.

Побудову системи забезпечує одержувач повідомлень. Спочатку випадковим чином вибираються два різні великі **прості числа** p і q. На практиці вибрані прості числа повинні задовольняти деяким додатковим умовам.

Потім обчислюється модуль $n = pq$, функція Ейлера від модуля $\varphi(n) = (p-1)(q-1)$, а також вибирається **випадкове число** e, взаємно просте з $\varphi(n)$.

Секретний ключ створюється за допомогою розширеного алгоритму Евкліда, як число d, що задовольняє порівнянню $de \equiv 1(\varphi(n))$. Потім усі дані, крім e, d, n, а також дані проміжних обчислень знищуються. Пара e, n об'являється відкритим ключем.

Розшифрування забезпечується двома фактами: для $(m, n) = 1$ з теореми Ейлера випливає, що

$$c^d = m^{1+k\varphi} \equiv m(n),$$

крім того, для інших значень m можна показати, що для модуля виду $n = pq$ співвідношення

$$m^{ed} \equiv m(n)$$

також має місце. При побудові ключів можна використовувати функцію $\lambda(n) = \text{НСК}[(p-1), (q-1)]$ замість $\varphi(n)$.

Приклад. Побудувати криптосистему RSA: $p = 3$, $q = 11(e = 7)$. Зашифрувати повідомлення $m = 3, 1, 2$.

1. $p = 3, q = 11$.
2. $n = 33$.
3. $\varphi(n) = 20$.
4. $e = 7, (e, \varphi(n)) = 1$.
5. $d = 3, ed = 1(\varphi)$.

Відкритий ключ — (7,33).

Зашифруємо повідомлення з трьох блоків: 3,1,2.

$$RSA(3) = 3^7 = 2187 = 9(33),$$
$$RSA(1) = 1^7 = 1(33),$$
$$RSA(2) = 2^7 = 128 = 29(33).$$

Для розшифрування підносимо кожний блок до степеня $d = 3$ за модулем 33: $9^3 = 729 = 3(33)$, $1^3 = 1(33)$, $29^3 = 24389 = 2(33)$.

Секретний ключ для навчальної системи легко знайти перебором. На практиці це нездійсненно, тому що реальний розмір модуля (довжина бітового представлення) $size(n)$ знаходиться у діапазоні від 512 до 4096 бітів.

1.11 Загальний підхід до побудови цифрового підпису на основі криптосистеми RSA. Визначення геш-функції

Цифровим підписом (ЦП) називається результат спеціального криптографічного перетворення, що здійснюється над електронним документом його власником. Мета перетворення — довести неспростовність тексту документа та факту перетворення даних конкретною особою. Основний метод — перевірка факту використання секретного параметра (ключа) підпису (без знання власне ключа).

Підпис на основі RSA являє собою блок даних. Підписане повідомлення — це повідомлення, що передається разом з ЦП.

Власник секретного ключа криптосистеми RSA як підписане повідомлення подає пару $(m, m^d) = (m, c)$. Дійсно, перетворення

m^d може здійснити тільки він. Оскільки m знаходиться у повідомлення у вихідному вигляді, будь-який абонент може перевірити співвідношення $m = c^e$, яке буде виконуватися лише у тому випадку, коли дійсно $c = m^d$.

Проте подібний підхід не забезпечує стійкості підпису при передачі випадкових даних. Дійсно, виберемо число a и побудуємо повідомлення $m = a^e(n)$. Тоді, очевидно, $(m, m^d) = (m, a)$, тобто підпис дійсний. За цієї причини краще замість (m, m^d) використати пару $(m, (h(m))^d)$, $h(m)$ — так звана **геш-функція** повідомлення m — несекретне, наперед обумовлене перетворення. Перевірка підпису (m, c) починається з обчислення $h(m)$, потім результат порівнюється з c^e.

Реальні геш-функції представляють собою складні алгоритми, які рекомендуються у відповідних стандартах.

Визначення геш-функції. Геш-функція $z = h(m)$ — перетворення бітового рядка довільної довжини у бітовий рядок (блок) фіксованої довжини (звичайно, 160–512 бітів), який має має наступні властивості.

1. Відновлення m по z, виходячи із співвідношення $z = h(m)$, обчислювально неможливо.

2. Більш того, виходячи з m і z, обчислювально неможливо знаходження іншого прообразу для z, тобто такого повідомлення $m_1 \neq m$, що $z = h(m) = h(m_1)$.

На практиці, як правило, використовуються геш-функції, що задовольняють більш жорсткій, ніж остання, умові: знаходження довільної колізії, тобто пари повідомлень x, y, таких, що $z = h(m) = h(m_1)$ обчислювально неможливе.

Приклад. Підписати повідомлення $m = 9$, використовуючи систему RSA з параметрами: $p = 3$, $q = 11$, $e = 7$, $d = 3$ і геш-функцією $h(m) = m$.

Відкритий ключ — (7,33).

$9^3 = 729 = 3(33)$. Підписане повідомлення: $(9, 3)$. Перевірка: $3^7 = 2187 = 9(33)$.

1.12 Змішані криптосистеми. Протокол обміну ключами Діффі-Хеллмана

На теперішній час в системах зв'язку загального призначення широко використовуються **змішані криптосистеми**. В таких системах шифрування повідомлень забезпечується за рахунок симетричних криптосистем, а розповсюдження ключів — за допомогою асиметричних криптоалгоритмів. Тут виникає новий тип задач, пов'язаний з так званою недовірою кореспондентів один до одного. Існує велика кількість стандартизованих протоколів безпечного ключового обміну, що застосовуються в різноманітних ситуаціях. При виконанні таких протоколів забезпечується автентифікація абонентів і створення загального секретного набору даних для подальшої генерації ключів.

Найбільш ранній **протокол обміну ключами** при взаємній недовірі учасників обміну запропонований Діффі і Хеллманом. В цьому протоколі використовується показникова функція у простому **полі Галуа** $GF(p)$, оберненою до якої є **дискретний логарифм**.

Абонент А є ініціатором обміну. Він має намір створити загальний секретний ключ для симетричної криптосистеми з абонентом В. При цьому обом відомий первісний елемент (на практиці — елемент великого порядку) g поля $GF(p)$ і, звичайно, просте число p.

Протокол розв'язує задачу побудови загального секретного блоку даних виду

$$g^{xy}(p),$$

x, y — випадкові лишки за модулем $p-1$.

Абонент А випадково вибирає x, обчислює значення $g^x(p)$ та відправляє це значення абоненту В. Абонент В діє аналогічно: вибирає y, обчислює значення $g^y(p)$ та відправляє це значення абоненту А. Кожний з абонентів має змогу тепер обчислити значення загального секретного блоку $g^{xy}(p)$. Обчислити це значення за даними перехоплення неможливо внаслідок властивостей дискретного логарифма.

Приклад системи експоненціального ключового обміну Діффі-Хеллмана.

1. $p = 13$, $g = 7$, оскільки $g^{(p-1)/2} = 117649 \equiv -1(p) \neq 1(p)$ і $g^{(p-1)/3} = 9 \neq 1(p)$ (див. п. 1.8).

2. Абонент А генерує псевдовипадкове число, наприклад, $x = 8$ і передає В значення $g^x = 7^8 = 3(13)$.

3. Абонент А, аналогічно, генерує $y = 5$ та відправляє А значення $g^y = 7^5 = 11(13)$.

4. А обчислює загальний секретний параметр $k = (g^y)^x = 11^8 = 9(13)$.

5. В обчислює загальний секретний параметр $k = (g^x)^y = 3^5 = 9(13)$.

1.13 Загальні принципи побудови систем управління ключами

Криптосистеми основані на використанні ключів. Несанкціонований доступ до ключів повинен бути неможливим. У цей же час велика кількість ключів повинна формуватися і розподілятися між абонентами.

Під **ключовою інформацією** розуміють сукупність усіх діючих у системі ключів.

Система управління ключами — система обробки і передачі інформації, що включає генерацію, зберігання і розподіл ключів.

Генерування ключів в реальних системах здійснюється на основі використання спеціальних апаратних та програмних методів, для яких необхідна наявність так знаного випадкового фактора. Наприклад, генератори на основі білого радіошуму, або програмні генератори псевдовипадкових послідовностей.

Зберігання ключів — це організація їх охорони, обліку та знищення. Звичайно зберігання відбувається в базах даних. Секретні ключі ніколи не зберігаються у явному вигляді на носії, який може бути прочитаний або скопійований.

Інформація про ключі повинна зберігатися в перешифрованому вигляді. Ключі для зашифрування ключової інформації називаються **майстер-ключами**.

Важливою умовою є періодичне **оновлення** як звичайних, так

і майстер-**ключів**. Оновлення ключів пов'язане з третьою складовою управління ключами — **розподілом ключів**, який забезпечує призначення ключів абонентам та доставку ключів.

Розподіл ключів повинен здійснюватися потай, а також оперативно і вчасно.

Існує два основних методи доставки ключів з використанням незахищених каналів зв'язку: пересилка (транспортування) та узгодження.

Транспортування ключів зводиться до передавання їх у зашифрованому вигляді. **Узгодження ключів** полягає у синхронному виготовленні ключів із секретних даних, сформованих перед початком сеансу шифрування відповідно до призначеного протоколу.

Розділ 2

МОДУЛЬНІ ОПЕРАЦІЇ В СИМЕТРИЧНІЙ КРИПТОГРАФІЇ

2.1 Криптоеквівалентна схема алгоритму ГОСТ 28147-89 для режиму простої заміни. Принципова можливість послаблення шифру за рахунок структури сеансового ключа

Алгоритм криптографічного перетворення, встановлений **стандартом шифрування ГОСТ 28147-89** (надалі — GA) використовується для зашифрування відкритого тексту у двох режимах, а також для створення **імітовставки**.

Для зашифрування даних ГОСТ приводится до **шифру блокового гамування** з довжиною блока в 64 біта. Гама накладається порозрядно за модулем два.

Основна задача кожного з режимів **гамування** — формування 64-х бітових блоків для входу в блочний шифр — основний режим роботи ГОСТ, який називається режимом простої заміни.

Для шифрування кожної криптограми створюється 64-х бітовий несекретний псевдовипадковий блок S, що називається **синхропосилкою**. Цей блок служить параметром у ході деяких ітеративних перетворень.

Вихід з блочного шифру і є власне блоком гами. Ключі безпосередньо необхідні для роботи ГОСТ саме у цьому режимі.

Існує два типи ключів: довгостроковий K і сеансовий X розміром 512 і 256 бітів відповідно. Ключ K реалізує потетрадну заміну 32-розрядних підблоків в 32-х розрядні та складається з 8 вузлів: $K = (K_1, ..., K_8)$. В стандарті довгостроковий ключ називається блоком підстановки K.

Вузол K_i є таблицею заміни для i-ї (справа) тетради, тобто складається з 16 тетрад.

Ключ X складається з **конкатенації** восьми 32-х розрядних підключів $X = X_0, ..., X_7$, кожний з яких у підповідний момент підсумовується до деякого підблоку за модулем 2^{32} (операція $+$).

Зашифрування блоку в режимі простої заміни $T = GA(S)$ представляє собою реалізацію так званого блочного **шифру Фейстела** і складається з 32-х циклів. На кожному циклі здійснюється перетворення 64-х бітового блоку в 64-х бітовий.

Результатом зашифрування є результат роботи (вихід) тридцять другого циклу, який піддається додатковому перетворенню (перестановка підблоків, тобто половинок блоків, місцями).

Криптоеквівалентним чином процес простої заміни блока S на блок T можна представити у вигляді послідовності 34 підблоків розміром 32 біта кожний:

$$u = (U_{-2}, U_{-1}, U_0, U_1, U_{i-1}, U_i, ..., U_{30}, U_{31}),$$

$$U_{-2} \parallel U_{-1} = S, U_{31} \parallel U_{30} = T.$$

Тут $U_{i-1} \parallel U_i$ — результат роботи циклу номер i. Додаткове перетворення змінює порядок підблоків у вихідному блоці циклу номер 31.

Елементи послідовності u пов'язані ланцюговою залежністю виду

$$U_{i-2} \oplus \widetilde{U}_{i-1} = U_i \quad (i = 0, 1, ..., 31),$$

де $\oplus$ — порозрядне додавання підблоків за модулем два.

Запис $\tilde{\mathrm{U}}_{i-1}$ означає, що підблок U_{i-1} модифікується за допомогою перетворення, що залежить від i. Іншими словами,

$$\widetilde{U}_{i-1} = F_i(U_{i-1}),$$

де F_i залежить від параметрів, що використовуються у циклі з номером i.

Кожна з функцій F_i використовує ключ K і деякий підключ сеансового ключа $X_{t(i)}$, де $t(i)$ — послідовність вибору підключів:

$$t(i) = (0, 1...7, 0, 1...7, 0, 1...7, 7, 6...1, 0).$$

Перетворення $\tilde{\mathrm{U}}_{i-1} = F_i(U_{i-1})$ полягає в обчисленні підблоку

$$U^*_{i-1} = U_{i-1} + X_{t(i)} \bmod 2^{32},$$

заміні кожної тетради підблоку U_{i-1}^{*} за допомогою відповідного вузла K_j та циклічного зсуву одержаного підблоку на 11 розрядів вліво.

Звернемо увагу, що, таким чином, $\widetilde{U}_{i-1}$ є циклічно зсунутим виходом з блоку підстановки K.

Розшифрування відбувається відповідно до алгоритму зашифрування, проте вибір підключів здійснюється у зворотному порядку по відношенню до $t(i)$. Підкреслимо, що ця властивість не залежить від кількості циклів та послідовності $t(i)$, що використовується у перетворенні $GA(S)$.

У свою чергу, це дозволяє зробити висновок, що для кожного K існує блок відкритого тексту B та сеансовий ключ X, такий, що $GA(B) = B$.

Розглянемо чотирицикловий алгоритм $G\widetilde{A}$ з послідовністю $t(i) = (0, 1, 2, 3)$ та нехай $G\widetilde{A}^{-1}(T) = B$, де $T = U \parallel U$. Тоді вихід після четвертого циклу $G\widetilde{A}(B)$ має вигляд $U \parallel U$, тобто додаткове перетворення його не змінює. Відзначимо, що для $G\widetilde{A}^{-1}$ $t(i) = (3, 2, 1, 0)$. Тому для восьмициклового $G\widetilde{A}$ з послідовністю $t(i) = (0, 1, 2, 3, 3, 2, 1, 0)$ одержуємо $GA(B) = B$.

Це ж буде вірним для тридцять двох циклів, при

$$t(i) = (0, 1, 2, 3, 3, 2, 1, 0, ..., 0, 1, 2, 3, 3, 2, 1, 0),$$

що при стандартному значенні $t(i)$ є еквівалентним використанню сеансового ключа виду

$$X = X_0, X_1, X_2, X_3, X_3, X_2, X_1, X_0.$$

Таким чином, для алгоритму ГОСТ в режимі простої заміни віртуальні таблиці заміни можуть відрізнятися за якістю, залежно від сеансових ключів.

2.2 Вплив блоку підстановки на послідовність виходів ітерацій алгоритму ГОСТ 28147-89. Наявність слабких ключів

Вплив **довгострокового ключа** K на виходи циклів (послідовність u) можна простежити, виходячи з того, що блок $U_{30} \parallel U_{31}$

порозрядно відрізняється від вхідного блока $U_{-2} \parallel U_{-1}$ на доданок $L \parallel R$, де підблоки L і R є лінійними комбінаціями виду $\widetilde{V}_1 \oplus \widetilde{V}_2 \oplus ... \oplus \widetilde{V}_h$, де $\widetilde{V}_i$ — результат перетворення $F_i(V)$.

Дійсно, за визначенням,

$$U_{i-2} \oplus \widetilde{U}_{i-1} = U_i \quad (i = 0, 1, ..., 31).$$

Таким чином, із $U_{-1} \oplus \widetilde{U}_0 = U_1$ і $U_1 \oplus \widetilde{U}_2 = U_3$ випливає

$$U_{-1} \oplus \widetilde{U}_0 \oplus \widetilde{U}_2 = U_3.$$

За індукцією:

$$U_{2k+1} = U_{-1} \oplus \widetilde{U}_0 \oplus \widetilde{U}_2 ... \oplus \widetilde{U}_{2k}, \quad (k = 0, 1, ..., 15).$$

Аналогічно:

$$U_{2k} = U_{-2} \oplus \widetilde{U}_{-1} \oplus \widetilde{U}_1 ... \oplus \widetilde{U}_{2k-1}, \quad (k = 0, 1, ..., 15).$$

Таким чином, лівий і правий підблоки відкритого тексту фактично шістнадцять разів гамуються порозрядним додаванням виходами з блоку підстановки в непарних і парних циклах відповідно. Отже, певну інформацію про властивості "сумарної псевдогами" L і R можна одержати виходячи з властивостей K без урахування решти параметрів.

Розглянемо довгостроковий ключ K як таблицю, колонки якої є правими частинами двійкових функцій від чотирьох змінних (в криптографії подібні функції називаються булевими).

З попереднього випливає, що при перевазі, скажімо, нулів у колонці і при випадковому рівноймовірному та незалежномі виборі аргументів, на відповідному місці вихідного блоку ймовірність нуля також буде завищеною. У даному випадку поява нуля або одиниці є подіями, що відповідають схемі Бернуллі з постійними ймовірностями.

При рівній кількості нулів та одиниць перевага нулів у колонці є рівною нулю. Найменша можлива перевага нулів у колонці (на два біти) відповідає розподілу ймовірностей одиниці (p) і нуля (q) при якому $q - p = 1/8$.

Дійсно, сума нулів і одиниць дорівнює $z + e = 16$, а їх різниця дорівнює перевазі: $z - e = h$. Тому h — мінімальне парне число що є більшим за нуль, тобто $h = 2$, звідки

$$q - p = (z - e)/16 = 1/8.$$

Легко одержати формулу для обчислення ймовірності нуля в сумі з k бітів при заданій перевазі $q - p = \delta$:

$$P(0) = 1/2 + 1/2(\delta)^k.$$

Таким чином, для $h = 2$, при підсумовуванні шістнадцяти підблоків "псевдогами" біт на виході GA співпадає з бітом на вході з ймовірністю

$$1/2 + 1/2(1/8)^{16} = 1/2 + (1/2)^{49}.$$

Отже, можлива генерація ослабленої гами.

Зокрема, якщо кожний вузол заміни K_i містить лише однакові тетради, скажімо m_i, то підблоки L, R дорівнюють нулю, як порозрядні суми шістнадцяти однакових підблоків $m_1 \parallel ... \parallel m_8$.

У цьому випадку U_{-2} і U_{-1} лише міняються місцями і довгостроковий ключ є **слабким**. Усі сеансові ключі є **криптоеквівалентними**.

Таким чином, для алгоритму ГОСТ віртуальні таблиці заміни можуть відрізнятися за якістю, залежно від структури ключів.

2.3 Поняття області сильних ключів. Тестування блоку підстановки алгоритму ГОСТ 28147-89

При некоректному виборі **блоку підстановки** K сеансові ключі можуть не забезпечувати належний рівень безпеки інформації. В таких випадках відповідні ключі (X, K) називають **слабкими**.

На противагу слабким ключам, ключі, що забезпечують обумовлений рівень безпеки інформації називаються **сильними ключами**. Хоча знання структури **ключового простору** є бажаним, проте проаналізувати шифр до такої міри, щоб став можливим опис множини слабких ключів, не вдається.

Аналогічно, не вдається повністю описати в множину сильних ключів, але часто виникає можливість визначити частину множини сильних ключів, достатню для практичних застосувань.

Підмножина множини сильних ключів достатньо велика, щоб протистояти методу повного перебору, називаються областю сильних ключів.

Одним із підходів, що дозволяють визначити область сильних довгострокових ключів для алгоритму ГОСТ, є підхід, при якому таблиця заміни K розглядається як шифр, подібний до гамування за модулем два:

$$K(h) = h \oplus R(h),$$

де h — 32-розрядний підблок.

Тут відображення $R(h)$ залежить від відкритого тексту і визначається як

$$K(h) \oplus h = R(h).$$

Назвемо $R(h)$ **псевдогамою**, оскільки гама, що використовується у **шифрі гамування**, від відкритого тексту не залежить.

З іншого боку, виходячи з розглянутого раніше впливу блоку підстановки на вихідні послідовності ітерацій, приходимо до висновку, що чим більше псевдогама має властивості рівноймовірної послідовності, тим більше її властивості підсилюються у процесі ітерацій циклів, що приводить до створення якісної гами в режимах шифрування алгоритму ГОСТ.

Таким чином, максимальна відповідність властивостей псевдогами до властивостей рійвноймовірної двійкової послідовності з незалежними, рівноймовірно розподіленими елементами, характеризує сильний довгостроковий ключ.

Для побудови області сильних ключів на цій основі, необхідно сформулювати, чим характеризується відповідність властивостей псевдогами до властивостей рівноймовірної двійкової послідовності, а також показати, що кількість ключів, що задовольнять висунутим вимогам, достатньо велика.

В криптографії розроблено ряд критеріїв, що дозволяють виділити класи **булевих функцій**, які перетворюють послідовності аргументів у послідовності, що є близькими до рівноймовірних. Такі булеві функції називаються **криптографічно сильними**.

Сильні довгострокові ключі для алгоритму ГОСТ можна створювати, використовуючи подібні критерії для булевих функцій від чотирьох змінних.

Дійсно, відображення $K(h)$ можна розглядати як (0,1)–матрицю розміром 16×32, а тетраду $x = (x_1, x_2, x_3, x_4)$, що замінюється за допомогою вузла заміни K_i, як $(0,1)$–вектор $x = (x_1, x_2, x_3, x_4)$ розмірності чотири. Отже,

$$K_i(x) = y = (y_1, y_2, y_3, y_4).$$

Проте набір (y_1, y_2, y_3, y_4) можна одержати, якщо вибирати біти не одночасно, а послідовно, що є еквівалентним вибору значень чотирьох функцій (для кожного вузла заміни своїх) $y_1 = g_{i1}(x)$, $y_2 = g_{i2}(x)$, $y_3 = g_{i3}(x)$, $y_4 = g_{i4}(x)$.

Таким чином можна розглядати кожну колонку з номером j вузла заміни K_i як праву частину булевої функції $y_j = g_{ij}(x)$ від чотирьох змінних.

Відповідна **тетрада псевдогами** дорівнює $x \oplus y$, тому кожний біт псевдогами можна записати у вигляді

$$\gamma_j = x_j \oplus g_{ij}(x),$$

де x_j входить до складу тетради x. Отже для всього блока K можна перепозначити: $\gamma_j = \gamma_j(x)$, $y_j = f_j(x)$, $j = 1, 2, ..., 32$.

Сильний довгостроковий ключ K будується на основі вибору сукупності функцій

$$f_j(x), \quad j = 1, 2, ..., 32,$$

що задовольняють деяким специфічним вимогам. Ці вимоги одночасно забезпечують необхідні властивості функцій $\gamma_j(x)$. Наприклад, однією з таких вимог є умова, за якою кожний вузол заміни K_i має бути підстановкою.

Для алгоритму ГОСТ небезпечним може бути використання слабких ключів. У принципі, існує підхід щодо їх виявлення за допомогою багатократного тестування шифрувального засобу методом "**чорного ящика**" (порядку 2^{32} випробувань).

Суть тестування полягає у виборі фіксованого блоку відкритого тексту виду $A = U \parallel U$ і перевірки при спеціально вибраних

сеансових ключах умови

$$A = GA(A),$$

де $GA(A)$ — результат шифрування алгоритмом ГОСТ блоку A (вихід "чорного ящика").

При кожному випробуванні висувається припущення про значення восьми тетрад, розташованих на фіксованих місцях у блоці підстановки K. Для визначення перших восьми тетрад необхідно 2^{32} випробувань.

Залежно від припущення і конкретного виду U визначається сеансовий ключ

$$X = X(K, U),$$

такий, що $A = GA(A)$ лише при істинному припущенні.

Після визначення істинного значення перших восьми тетрад, усі решта тетрад тестуються поодинці. Кожне нове місце у блоці K разом з місцями деяких семи тетрад, що визначилися, дозволяє визначити значення чергової невідомої тетради з шістнадцяти її варіантів.

Припустимо, що **конкатенація** передбачуваних значень восьми тетрад, розташованих у блоці підстановки K на фіксованих місцях $i_1, ..., i_8$, утворюють двійковий підблок h. Позначимо через h^1 циклічний зсув підблоку h на 11 бітів вліво. Нехай також конкатенація номерів місць шуканих тетрад у шістнадцятеричній системі числення дає двійкових підблок

$$I = (i_1, ..., i_8).$$

Виберемо підключ X_1 із умови

$$U + X_1 \pmod{2^{32}} = I$$

і підключ X_2 із умови

$$(U \oplus h^1) + X_2 \pmod{2^{32}} = I,$$

де $h^1 = \tilde{U}$ — за припущенням, вихід циклової функції на першій ітерації $GA(A)$ при **підключі** X_1.

Можна показати, що коли всі K_i — підстановки, то

$$X(K, U) = X_1 \parallel X_2 \parallel X_2 \parallel X_1 \parallel X_1 \parallel X_2 \parallel X_2 \parallel X_1.$$

2.4 Компрометація шифрів. Двійковий регістр зсуву з лінійним зворотним зв'язком як генератор гами

Однією з особливостей потокових шифрів є те, що число параметрів, що впливають на їх стійкість, суттєво більше, ніж для блокових шифрів.

Криптосхеми потокових шифрів звичайно створюються на основі комбінування криптовузлів зі специфічними характеристиками. За цієї причини для їх синтезу необхідно враховувати не тільки загрозу дешифрування для відомих типів криптоатак, але й можливість так званої **компрометації шифру**.

Необхідність введення цього поняття пов'язана з тим, що в ряді ситуацій можливість дешифрування повідомлень зловмисником не виключається, але й не є неминучою.

Неформально шифр називається скомпрометованим, якщо з достатньо малою ймовірністю помилки **криптоаналітик** визначає, чи одержана задана послідовність символів у результаті зашифрування конкретним шифром, чи ні.

Хоча суть поняття компрометації полягає в тому, що невдалий вибір деяких параметрів часто дозволяє ідентифікувати шифр за шифротекстом, на практиці компрометація шифру оцінюється як передумова до існування невідомих розробнику криптографічних атак, що є специфічними для даної шифрсистеми.

Шифр може бути скомпрометованим у тій чи іншій мірі. Подібна оцінка є якісною і розглядається у межах від визначення типу шифру до розкриття окремих параметрів вузлів та елементі ключової системи. Задача звичайно зводиться до виявлення у шифротексті наявності особливостей, властивих спотворенній вихідній послідовності деякого криптовузла. Для розв'язання подібних задач звичайно використовується статистичний підхід, що комбінується з методами оптимізації.

В криптосистемах потокових шифрів широко застосовуються криптовузли, засновані на так званих двійкових регістрах зсуву із зворотним зв'язком.

Двійковий регістр зсуву — це послідовність бітових комірок. Їх кількість називається довжиною регістра. Під час роботи вміст

комірок змінюється. Початковий стан регістра називається його початковим заповненням. Вміст комірки називається розрядом (з відповідним номером).

Регістр зсуву із зворотним зв'язком складається з двох частин: регістра зсуву та **функції зворотного зв'язку**.

У результаті одного такту роботи регістра генерується один біт. Новий біт обчислюється як функція від бітів, що вибираються з комірок регістра з фіксованими номерами. Вказані комірки називаються комірками зворотного зв'язку, а функція — функцією зворотного зв'язку. Номери комірок зворотного зв'язку називаються точками знімання зворотного зв'язку.

У такті роботи обчислюється значення функції зворотного зв'язку, потім регістр зсувається, скажемо вліво, втрачаючи лівий крайній розряд та звільнюючи крайню праву комірку. У цю комірку поміщається значення функції зворотного зв'язку. Виходом регістра є біт, знятий з фіксованої (звичайно, з крайньої правої) комірки.

У потокових шифрах генератори гами у більшості випадків складаються з типових вузлів, що основані на комбінаціях регістрів зсуву та функціях ускладнення.

Найбільш простим вузлом є так званий **регістр зсуву з лінійними зворотними зв'язками** (РЗЛЗЗ), що генерує **рекурентну послідовність** виду

$$x_{i+0} \oplus x_{i+k} \oplus ... \oplus x_{i+t} = x_{i+n}.$$

Приклад розгортки РЗЛЗЗ для $n = 5, k = 2$:
11000110111010100001001011001111000110111010100001001 0.

Тут n — довжина вихідного блока бітів (початкового заповнення регістра), $0, k$ — параметри рекурентного закону (точки знімання зворотного зв'язку регістра).

Сам закон має вигляд:

$$x_{i+0} \oplus x_{i+2} = x_{i+5}.$$

Рекурентні послідовності періодичні. При відповідному виборі параметрів РЗЛЗЗ можна досягнути максимально можливих значень періоду рівних $2^n - 1$.

Безпосередньо для генерації гами РЗЛЗЗ не підходить. На практиці застосовують комбінації залежних РЗЛЗЗ, що взаємно впливають на формування своїх послідовних заповнень.

Проілюструємо тепер суть поняття **компрометації шифру** на елементарному прикладі.

Припустимо, що криптосистема потокового шифру гамування за модулем два генерує гаму як вихід з РЗЛЗЗ, а ключем є початкове заповнення. У цьому випадку шифротекст є спотвореною рекурентною послідовністю і задача дешифрування зводиться до відновлення початкового заповнення регістра.

Що стосується компрометації шифру, то відповідним тестом може бути розв'язання іншої задачі, а саме, задачі відновлення точок знімання зворотного зв'язку.

У цьому випадку, при позитивному результаті тестування не можна стверджувати, що вузол є РЗЛЗЗ.

Дійсно, тестування показує лише наявність лінійної складової у шифртексті або вихідній послідовності вузла.

Наприклад, у послідовності

$$\widetilde{a}_{n+i} = a_i \oplus a_{k_1+i} \oplus ... \oplus a_{k_r+i} \oplus a_{i+1} \cdot a_{i+2} \cdot a_{i+3} \cdot a_{i+4}$$

останній доданок дорівнює нулю з ймовірністю 15/16 і може бути непомітним на фоні спотворень, що вносяться в рекуренту бітами відкритого тексту.

З точки зору визначення наявності лінійної складової, лінійна та нелінійна рекуренти нерозрізнені, але в обох випадках можна стверджувати про наявність у криптосхемі типового вузла.

2.5 Комбінування лінійних регістрів зсуву. Нелінійний зворотний зв'язок

При побудові криптосхем застосовуються різноманітні комбінації регістрів зсуву з лінійними зворотними зв'язками. Найбільш часто зустрічаються вузли, які називаються комбінуючими генераторами і (нелінійними) **фільтр-генераторами** (рис. 2.1).

У **комбінуючих генераторів** у кожному такті роботи чергові елементи вихідних послідовностей декількох регістрів зсуву

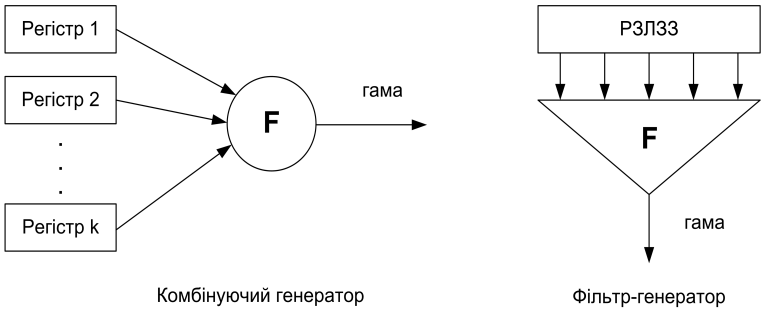

Рис. 2.1. Комбінування регістрів зсуву

поступають на вхід деякої функції. Значення цієї функції є виходом генератора (елементом гами).

Нелінійні фільтр-генератори генерують вихідну послідовність як нелінійну функцію від станів одного й того ж регістру.

У свою чергу, при об'єднанні в криптосхему, цілі вузли, або їх частини можуть впливати одне на одного, змінюючи заповнення деяких регістрів, а також управляючи їх рухом. Звичайно регістри зсуву змінюють свій стан регулярно, рухаючись орбітою на один крок протягом такту роботи генератора. Якщо ж рух регістра протягом такту роботи генератора залежить від стану схеми, то такий рух називається керованим. Нерівномірний рух регістрів, як правило, суттєво ускладнює вихідну послідовність.

Крім регістрів зсуву з лінійними зворотними зв'язками в криптографії використовуються регістри зсуву з нелінійними функціями зворотного зв'язку, у тому числі необов'язково з двійковими елементами. У найбільш загальному випадку функція зворотного зв'язку задається у вигляді таблиці.

Необхідно враховувати, що теорія регістрів зсуву з нелінійними функціями зворотного зв'язку розроблена недостатньо. При обґрунтуванні вибору конкретного типу нелінійного зв'язку можуть виникнути суттєві труднощі.

2.6 Зведення до діофантового рівняння задачі відновлення початкового заповнення і конфігурації РЗЛЗЗ за шифротекстом

Нехай в результаті роботи РЗЛЗЗ довжини n з номером точок знімання $(0, k_1, k_2, ...k_r)$ і початковим заповненням $\mathbf{s_0} = (a_0, a_1, ...a_{n-1})$ виникла рекурентна послідовність $R(\mathbf{s_0}) = a_0, a_1, ...a_i..., $, для якої виконується лінійне рекурентне співвідношення $a_i \oplus a_{k_1+i} \oplus ... \oplus a_{k_r+i} = a_{n+i}$ $(i = 0, 1, 2, ...)$.

Очевидно, рекуренту можна записати через усі елементи початкового заповнення у вигляді

$$a_{n+i} + \sum_{j=0}^{n-1} b_{j+i} a_{j+i} = 0 \pmod 2,$$

де $b_j = 1$, якщо $j \in \{0, k_1, k_2, ..., k_r\}$, або $b_j = 0$, у іншому випадку.

Послідовність $R(\mathbf{s})$ зручно розглядати як послідовність $\mathbf{s_0}, \mathbf{s_1}, ...$ станів регістра, тобто у вигляді послідовності векторів.

Введемо матрицю

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & ... & 0 & b_0 \\ 1 & 0 & ... & 0 & b_1 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 1 & ... & b_{n-2} \\ 0 & 0 & ... & 1 & b_{n-1} \end{pmatrix}, \quad b_i \in \{0, 1\}, \quad b_0 = 1.$$

Очевидно,

$$\mathbf{s_0 A} = (a_0, ..., a_{n-1}) \cdot \mathbf{A} = (a_1, ..., a_{n-1}, \oplus_{j=0}^{n-1} a_j b_j).$$

Таким чином, для послідовних станів регістра виконується співвідношення

$$\mathbf{s_k A} = \mathbf{s_{k+1}},$$

тому

$$\mathbf{s_0 A^k} = \mathbf{s_k}, \quad (k = 0, 1, 2, ...).$$

Звідси виходить, якщо

$$\mathbf{s_0} = \mathbf{s_0}^{(1)} \oplus \mathbf{s_0}^{(2)},$$

то $R(\mathbf{s_0}) = R(\mathbf{s_0}^{(1)}) \oplus R(\mathbf{s_0}^{(2)})$ (послідовності підсумовуються поелементно).

Нехай $\mathbf{e_i}$ $(i = 0, 1, ..., n-1)$ — рядки одиничної матриці порядку n. З попереднього випливає, що

$$R(\mathbf{s_0}) = a_0 R(\mathbf{e_0}) \oplus a_1 R(\mathbf{e_1}) \oplus ... \oplus a_{n-1} R(\mathbf{e_{n-1}}).$$

Якщо підписати послідовність $R(\mathbf{e_i})$ одна під одною, утвориться матриця

$$\mathbf{M} = (\mathbf{h_0}, \mathbf{h_1}, ...),$$

що складається із n рядків та нескінченного числа стовпців $\mathbf{h_k}$. Легко бачити, що послідовність $\mathbf{h_0}, \mathbf{h_1}, ...$ є рекурентною, яка задовольняє тому ж співвідношенню, що і $R(\mathbf{s_0})$.

Початковим заповненням є послідовність стовпців

$$\mathbf{h_0}, \mathbf{h_1}, ..., \mathbf{h_{n-1}}.$$

За побудовою, ці стовпці утворюють одиничну матрицю, тобто відомі. Оскільки степінь матриці обчислити легко, то можна швидко обчислити будь-який з векторів $\mathbf{h_k}$.

В термінах стовпців матриці $\mathbf{M}$ елемент a_k послідовності $R(\mathbf{s_0})$ дорівнює

$$a_k = \oplus_{j=0}^{n-1} a_j h_j^{(k)},$$

де $h_j^{(k)}$ — координати вектора $\mathbf{h_k}$.

Якщо розглядати цей вираз як функцію від $a_0, a_1, ..., a_{n-1}$ з коефіцієнтами $h_j^{(k)}$ та позначити її $\langle \mathbf{s}, \mathbf{h_k} \rangle$ (вона є аналогічною скалярному добутку, приведеному за модулем два), то

$$a_k = \langle \mathbf{s_0}, \mathbf{h_k} \rangle, \quad k = (0, 1, 2, ...).$$

Номери координат вектора $\mathbf{h_k}$, які дорівнюють одиниці, указують, які компоненти вектора $\mathbf{s_0}$ брали участь в сумі $a_k = \langle \mathbf{s_0}, \mathbf{h_k} \rangle$. Таким чином, завжди можна сказати, сумою яких елементів початкового стану є будь-який елемент a_k рекурентної послідовності.

Отже, кожний елемент рекурентної послідовності легко записати у вигляді лінійної комбінації змінних, що входять до складу початкового заповнення.

Припустимо, що наша рекурента використовується як двійкова гама. Якщо прирівняти лінійну комбінацію, що відповідає біту гами a_k, до біта шифртексту з номером k, то одержимо рівняння зі спотвореною правою частиною.

Якісну характеристику задачі відновлення параметрів двійкової спотвореної рекуренти можна одержати, якщо використати наступний підхід.

Нехай відрізкові $c_0, c_1, ..., c_{N-1}$ спотвореної рекуренти довжиною N при істинних значеннях точки знімання та істинному початковому заповненні відповідає послідовність спотворень (тобто відкритого тексту), що містить N_- одиниць і $N_+ = N - N_-$ нулів.

Нехай $\mathbf{z} = (z_0, z_1, ..., z_{n-1})$ — шукане початкове заповнення і $N_+ \geq N_-$. Розглянемо передбачуваний варіант набору точок знімання.

Позначимо відрізок рекуренти $R(\mathbf{z})$, який відповідає послідовності $c_0, c_1, ..., c_{N-1}$ через $t_0, t_1, ..., t_{N-1}$. Спотворення мають вигляд $u_k = c_k \oplus t_k$.

Перетворимо тепер значення бітів за допомогою перетворення (гомоморфізму) T: $T(0) = 1$, $T(1) = -1$.

Легко перевірити, що сума бітів за модулем два перейде у звичайне множення:

$$T(x \oplus y) = T(x)T(y).$$

Позначимо $T(x)$ через $\hat{x}$.

Нам невідоме початкове заповнення, проте є відомим вектор $\mathbf{h_k}$. Оскільки $t_k = \langle \mathbf{z}, \mathbf{h_k} \rangle$, то можна виразити t_k через $z_0, z_1, ..., z_{n-1}$ у вигляді суми за модулем два, скажемо $g_k(\mathbf{z})$. Замінимо цю суму на добуток, користуючись перетворенням T.

Із властивостей перетворення T випливає, що

$$\hat{u}_k = \hat{c}_k \hat{g}_k(\mathbf{z}),$$

де $\hat{c}_k = \pm 1$, а $\hat{g}_k(\mathbf{z})$ — добутки змінних із множини $z_0, z_1, ..., z_{n-1}$, номери яких відомі.

Таким чином можна утворити поліном

$$P(z_0, z_1, ..., z_{n-1}) = \sum_{k=0}^{N-1} \hat{c}_k \hat{g}_k(z_0, z_1, ..., z_{n-1}).$$

Розглянемо рівняння

$$P(\mathbf{z}) = B,$$

де B — ціле число від нуля до N, а змінні задовольняють обмеженням $z_i = \pm 1$.

Припустимо, що можна при будь-якому B відповісти на питання чи існує розв'язок цього рівняння, а також знайти його, якщо він існує. Тоді, розв'язуючи рівняння при кожному значенні від нуля до N, можна знайти максимальне значення B, при якому розв'язок існує та вказати цей розв'язок.

Проте

$$P(\mathbf{z}) = \sum_{k=0}^{N-1} \hat{u}_k(\mathbf{z}),$$

тобто

$$B = P(\mathbf{z}) = N_+ - N_-,$$

звідки одержуємо мінімальне для даного набору точок знімання значення N_-, оскільки $N_+ + N_-$ є відомим і дорівнює N.

Очевидно, що для визначення істинного набору точок знімання необхідно лише відповісти на питання, чи існує розв'язок при даному значенні B. Максимальне B, при якому рівняння розв'язне, відповідає істинному набору точок знімання.

Для визначення початкового заповнення регістра необхідно, крім того, знайти розв'язок рівняння $P(\mathbf{z}) = B$, при обмеженнях $z_i = \pm 1$.

Задачі відновлення точок знімання зворотного зв'язку та початкового заповнення РЗЛЗЗ за шифртекстом є реальними задачами практичної криптології. Хоча вони вивчалися багатьма авторами, для великих довжин регістрів методу, прийнятного для практики, знайдено не було.

Розділ 3

АРИФМЕТИЧНІ АЛГОРИТМИ В АСИМЕТРИЧНІЙ КРИПТОГРАФІЇ

3.1 Квадратичні порівняння і квадратичний закон взаємності Гауса. Символи Лежандра і Якобі

Двочленним квадратичним порівнянням називається порівняння виду

$$x^2 \equiv a(n),$$

де x — невідомий лишок.

Ціле число a називається **квадратичним лишком** за модулем n, якщо порівняння

$$x^2 \equiv a(n)$$

є розв'язним. Якщо порівняння розв'язне, то для випадкового складеного модуля кількість рішень, як правило, є більшою двох.

Задача знаходженя розв'язків квадратичного порівняння має важливе значення в криптографії.

Виявляється, що у загальному випадку, не тільки ця задача, але навіть питання про розв'язність квадратичного порівняння за складеним модулем, **факторизація** якого невідома, є невирішеною проблемою. Для модулів, які є простими числами, проблема досить легко піддається аналізу. Очевидно, якщо

$$x^2 \equiv a(n),$$

є розв'язним то a є квадратичним лишком за модулем будь-якого дільника числа n.

Нехай p — непарне **просте число**. Нехай a квадратичний лишок за модулем p.

Очевидно, при $a = 0(p)$ існує єдиний розв'язок:

$$x = 0(p).$$

Усі **ненульові лишки** за модулем p знаходяться серед чисел

$$\pm 1, \pm 2, .., \pm \frac{p-1}{2},$$

отже, їх квадрати складають список

$$1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$$

і порівняння

$$x^2 \equiv a(n)$$

є розв'язним, якщо a належить до цього списку.

Далі, якщо

$$x^2 \equiv k^2(p),$$

то існує два очевидних розв'язки: $\pm k$. Крім того, кількість розв'язків не може перевищувати степінь многочлена у лівій частині, тобто двох. Щоб переконатися, що розв'язків точно два, достатньо показати, що $k \neq -k(p)$. Проте, якщо це не так, то $2k = 0(p)$, що є вірним тільки для $k = 0(p)$.

Відзначимо тепер, що у нашому списку **квадратичних лишків** усі лишки попарно непорівнянні. Дійсно, якщо, наприклад

$$a \equiv k^2 \equiv l^2(p)$$

і

$$1 \leq k < l \leq \frac{p-1}{2},$$

то порівняння

$$x^2 \equiv a(n)$$

мало би чотири рішення: $\pm k, \pm l$, що є неможливим. Таким чином, кількість ненульових квадратичних лишків дорівнює

$$\frac{p-1}{2}.$$

Отже, кількість **квадратичних нелишків** також дорівнює

$$\frac{p-1}{2}.$$

Нехай g — примітивний елемент поля $GF(p)$. Тоді a — квадратичний лишок у тому і тільки у тому випадку, коли у представленні $a = g^j(p)$ число j парне.

Дійсно, якщо

$$x^2 \equiv a(p),$$

то дискретне логарифмування дає

$$2y \equiv j(p-1),$$

де модуль парний.

Існують алгоритми для визначення, чи є дане число квадратичним лишком за простим модулем, чи ні. Один з алгоритмів оснований на обчисленні так званого **символу Лежандра**, який для непарного простого p визначається так:

$$\left(\frac{a}{p}\right) = \left| \begin{array}{l} 0, a \equiv 0 \pmod p, \\ 1, \exists x : x^2 \equiv a \pmod p,\ a \bmod p \neq 0, \\ -1, \neg\exists x : x^2 \equiv a \pmod p,\ a \bmod p \neq 0. \end{array} \right.$$

Значення символу Лежандра називається квадратичним характером числа a за модулем p.

Основні властивості символу Лежандра.

$$a_1 = a(p) \Rightarrow \left(\frac{a_1}{p}\right) = \left(\frac{a}{p}\right);$$

Критерій Ейлера:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p;$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right);$$

$$(a,b) = 1 \Rightarrow \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right);$$

$$\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2};$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Крім того, має місце **квадратичний закон взаємності Гауса**: для будь-яких простих непарних чисел p і q виконується рівність

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Обчислення символу Лежандра полягає у використанні його властивостей для зниження абсолютних величин чисел, що беруть участь в обчисленні і є достатньо зручним при роботі вручну. При використанні ЕОМ, звичайно застосовується критерій Ейлера.

Приклад. $\left(\frac{126}{53}\right) = \left(\frac{20}{53}\right) = \left(\frac{2^2}{53}\right)\left(\frac{5}{53}\right) = (-1)^{26\cdot 2}\left(\frac{53}{5}\right) = \left(\frac{-2}{5}\right) = (-1)^2(-1)^3 = -1$.

Для визначення квадратичного характеру числа за складеним модулем n за допомогою символу Лежандра необхідно знати прості дільники n. Для великих чисел це нереально.

Існує алгоритм, що обчислює так званий **символ Якобі**, який дозволяє, принаймні, вирішити питання, чи є число x **квадратичним нелишком** за заданим непарним модулем.

Нехай n непарне та має наступний канонічний розклад

$$n = \prod_{i=1}^{k} p_i^{a_i}.$$

Символ Якобі числа x за модулем n визначається як добуток символів Лежандра

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)^{a_1} \cdots \left(\frac{x}{p_k}\right)^{a_k}.$$

Він має майже ті самі властивості, що і символ Лежандра.

Проте, за значенням символу Якобі, що дорівнює одиниці, не можна стверджувати, що відповідний лишок — квадратичний.

Тим не менше, для квадратичного лишку символ Якобі дорівнює одиниці, а це означає, що якщо $\left(\frac{x}{n}\right) = -1$, то x — квадратичний нелишок за модулем n.

Властивості символу Якобі.

Нехай x, x_1, x_2 — цілі, n_1, n_2, n — непарні числа, що більші за одиницю.

$$x_1 = x_2 (n) \Rightarrow \left(\frac{x_1}{n}\right) = \left(\frac{x_2}{n}\right);$$

$$\left(\frac{x_1 x_2}{n}\right) = \left(\frac{x_1}{n}\right)\left(\frac{x_2}{n}\right);$$

$$(x_2, n) = 1 \Rightarrow \left(\frac{x_2^2 x_1}{n}\right) = \left(\frac{x_1}{n}\right);$$

$$\left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2};$$

$$\left(\frac{x}{n_1 n_2}\right) = \left(\frac{x}{n_1}\right)\left(\frac{x}{n_2}\right);$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Крім того, має місце квадратичний закон взаємності Гауса: для будь-яких взаємно простих, більших за одиницю, непарних чисел m і n виконується рівність

$$\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right).$$

Обчислення символу Якобі полягає у використанні його властивостей для зменшення абсолютних величин чисел, що виникають у ході обчислень.

Приклад. Обчислити символ Якобі $\left(\frac{12}{35}\right)$.

$$\left(\frac{12}{35}\right) = \left(\frac{2^2 \cdot 3}{35}\right) = \left(\frac{35}{3}\right)(-1)^{\frac{(35-1)(3-1)}{4}} =$$

$$-\left(\frac{2}{3}\right) = -(-1)^{\frac{(3\cdot 3-1)}{8}} = 1.$$

3.2 Алгоритм знаходження квадратного кореня у простому полі

Даний алгоритм призначений для розв'язання відносно y порівняння виду

$$x \equiv y^2 (p)$$

за простим модулем $p > 2$.

Перед тим як приступити до обчислень, необхідно переконатися у розв'язності порівняння, тобто у тому, що $\left(\frac{x}{p}\right) = 1$.

Алгоритм розбивається на три випадки залежно від представлення p у вигляді $p = 4k + 3$, $p = 8k + 5$, $p = 8k + 1$ (можна переконатися, що будь яке непарне просте число представляється одним із вказаних способів).

В алгоритмі суттєво використовується **критерій Ейлера**, який для розв'язного порівняння дає:

$$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \equiv 1 \pmod{p}.$$

Випадок $p = 4k + 3$. Маємо

$$1 = \left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \equiv x^{2k+1} \pmod{p}.$$

Помножимо на x ліву і праву частину порівняння, одержимо

$$x \equiv x^{2k+2} \pmod{p},$$

звідки:

$$y \equiv \pm x^{k+1} \pmod{p}.$$

Випадок $p = 8k + 5$. Оскільки

$$1 = \left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \equiv x^{4k+2} \pmod{p},$$

то

$$x^{2k+1} \equiv \pm 1 \pmod{p}.$$

Отже, вірне одне з двох співвідношень

$$x^{2k+2} \equiv \pm x \pmod{p}.$$

Оскільки x і k відомі, то за допомогою обчислень можна перевірити, яке із співвідношень виконується. Якщо вірне

$$x^{2k+2} \equiv x \pmod{p},$$

то очевидно,

$$y \equiv \pm x^{k+1} \pmod{p}.$$

Інакше,

$$x^{2k+2} \equiv -x \pmod{p}.$$

Обидві частини останнього порівняння помножимо на число у відомому парному степені. При цьому підберемо вказаний множник так, щоб помінявся знак у правій частині порівняння.

Таким множником може бути число

$$2^{4k+2} = 2^{(p-1)/2} = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1(p),$$

оскільки

$$p^2 - 1 = (8k)^2 + 80k + 24.$$

Отже,

$$y \equiv \pm 2^{2k+1} \cdot x^{k+1} \pmod{p}.$$

Останній випадок $p = 8k + 1$ найбільш складний. Насамперед, для роботи алгоритму необхідна наявність (будь-якого) квадратичного нелишку за модулем p.

Щоб його знайти, приходиться вибирати навмання число, скажімо a, і перевіряти співвідношення

$$\left(\frac{a}{p}\right) \equiv x^{(p-1)/2} \equiv -1 \pmod{p}.$$

Припустимо, що деякий квадратичний нелишок a є відомим.

Уточнимо вигляд числа p:

$$p = 8k + 1 = 2^l h + 1,$$

де h — непарне число і, очевидно, $l \geq 3$.

Основна ідея алгоритму — побудувати співвідношення виду

$$x^h \cdot a^{2m} = 1 \bmod p.$$

У випадку успіху достатньо помножити обидві частини порівняння на x та добути корінь із обох частин (ураховуючи, що число $h+1$ парне).

У співвідношенні $x^{p-1} = 1(p)$ ми будемо послідовно ділити на двійки показник $p-1 = 2^l h$, доки не одержимо у показнику h. Ділення на двійки — це послідовне добування квадратних коренів, у нашому випадку — квадратних коренів з одиниці. Будемо знижувати показник таким чином, щоб права частина деякого порівняння весь час була рівною одиниці.

На кожному кроці може бути одержаним лише один з коренів: 1 або (-1). При цьому буде достатньо даних, щоб з'ясувати, який випадок реально має місце. Змінювати знак у (-1) будемо за допомогою множення порівняння на степені числа a, причому так, щоб показник степеня у добутку таких додаткових множників завжди залишався парним.

У результаті, одержимо порівняння виду

$$x^h \cdot a^{2m} \equiv 1 \pmod{p},$$

звідки, помноживши обидві частини на x, одержимо:

$$y = \pm x^{(h+1)/2} a^m \bmod p.$$

Приклад. Розв'язати порівняння $y^2 = 8(41)$.

З'ясуємо, насамперед, чи є порівняння розв'язним. Це дійсно так, оскільки

$$\left(\frac{8}{41}\right) = \left(\frac{2}{41}\right)^3 = \left(\frac{2}{41}\right) = (-1)^{\frac{41\cdot 41-1}{8}} = (-1)^{5.42} = 1.$$

Далі з'ясуємо, який з трьох випадків алгоритму p має місце. Очевидно, має має місце випадок $p = 8k+1$. Записавши $p = 2^3 \cdot 5 + 1$, одержимо $h = 5$, $l = 3$.

Знайдемо квадратичний нелишок за модулем 41.

Можна вибрати $a = 3$, оскільки

$$\left(\frac{3}{41}\right) = 3^{\frac{41-1}{2}} = 3^4 = -1(41).$$

Приступимо до добування кореня, враховуючи при обчисленнях, що $3^{20} = -1(41)$.

За **теоремою Ейлера** маємо $8^{p-1} = 8^{8\cdot 5} = 1(41)$. Можна здобути квадратний корінь, розділивши показник на два. При цьому значення кореня дорівнює 1, оскільки 8 — квадратичний лишок і

$$8^{4\cdot 5} = 8^{\frac{p-1}{2}} = 1(41).$$

Показник можна знову розділити на два, проте необхідно з'ясувати до якого числа (1 або -1) прирівняти значення квадратного кореня. Отже, $8^{2\cdot 5} = \pm 1(41)$. Оскільки $8^5 = 9(41)$, то $8^{2\cdot 5} = 81 = -1(41)$.

Необхідно домагатися значення 1 у правій частині порівняння. Помножимо обидві частини на 3^{20}, одержимо $8^{2\cdot 5}3^{20} = 1(41)$. Як і належало очікувати, показник при трійці парний.

Залишився тільки один крок, щоб знизити показник при вісімці до $h = 5$. Ділимо показники на два та обчислюємо значення лівої частини:

$$8^5 3^{10} = \pm 1(41),$$

$$8^5 3^8 3^2 = 9(3^4)^2 3^2 = 9(-1)^2 9 = -1(41),$$

тобто $8^5 3^{10} = -1(41)$.

Знову необхідно помножити обидві частини порівняння на 3^{20}, що дає результат $8^5 3^{10} 3^{20} = 1(41)$.

Показник при вісімці $h = 5$. Можна перейти до виписування результату. Помноживши обидві частини порівняння на 8, одержимо $8^6 3^{30} = 8(41)$, що дозволяє записати квадратний корінь із 8 у вигляді $y = \pm 8^3 3^{15} = \pm 7(41)$. Перевірка: $(\pm 7)^2 = 49 = 8(41)$.

3.3 Криптосистема і цифровий підпис Ель-Гамаля

Криптосистема Ель-Гамаля є асиметричною. Стійкість системи основана на **проблемі дискретного логарифмування у скінченному полі**.

Для побудови пари ключів вибирається велике просте число p і два псевдовипадкових числа, що менші за p.

Одне з них, g, повинно бути елементом великого порядку за модулем p, скажімо **первісним коренем**. Друге число, x, вибирається як **секретний ключ**. Вважається, що повідомлення — **лишки за модулем** p.

Відкритим ключем є три числа $p, g, y = g^x(p)$.

Для кожного повідомлення формуються додаткові дані, які відіграють роль **лазівки** для конкретного сеансу шифрування.

Для **зашифрування** повідомлення m вибирається псевдовипадкове число k (**рандомізатор**, **разовий ключ**) з умовою НСД$(k, p-1) = 1$. Рандомізатори не повинні повторюватися і повинні триматися у секреті.

Потім обчислюються числа $a = g^k(p)$ — лазівка та $b = y^k m(p)$ — шифротекст. Криптограмою ж є пара блоків даних a, b.

Для **розшифрування** достатньо одержати співмножник y^k, що можна зробити за допомогою секретного ключа на основі обчислення значення $a^x = g^{kx}(p)$.

Дійсно, $y^k = g^{kx}(p)$, тому $m = a^{-x}b(p)$.

У механізмі **цифрового підпису Ель-Гамаля** використовуються ті ж самі параметри, що і в системі Ель-Гамаля. Перетворення, звичайно, здійснюється особою, що має секретний ключ. Крім того, використовується геш-функція повідомлення $h(m)$.

Цифровий підпис Ель-Гамаля складається з пари блоків r, s.

Особа, що підписує документ, повинна для кожного повідомлення m, що підписується, вибрати рандомізатор k та обчислити "передпідпис" $r = g^k(p)$. Рандомізатор має бути взаємно простим із $(p-1)$.

Потім необхідно використати секретний ключ як один із коефіцієнтів порівняння, з якого визначається блок підпису s.

Порівняння має вид

$$h = h(m) = xr + ks \bmod (p-1).$$

Тут модулем порівняння вибране число $q = p-1$, оскільки обидві частини порівняння у перевірочному співвідношенні будуть брати участь у показниках.

Зауважимо, що число r може дорівнювати $p-1$, оскільки воно визначається із порівняння за модулем p.

Підпис r, s вважається дійсним, якщо

$$g^h = g^{xr+ks}(p).$$

Оскільки $y = g^x(p)$ і $r = g^k(p)$, то остаточний вигляд перевi-

рочного співвідношення наступний:

$$g^h = y^r r^s (p).$$

Таким чином, знання відкритого ключа є достатнім для перевірки підпису.

Приклад цифрового підпису Ель-Гамаля.

Виберемо $p = 17$. Оскільки

$$3^{p-1/2} = 6561 = -1(p),$$

то $g = 3$ — первісний елемент.

Приймемо $x = 5$. Тоді відкритий ключ

$$y = g^x(p) = 3^5 = 5(17).$$

Нехай $h(m) = 9$.

Виберемо рандомізатор $k = 7$. Обчислимо першу частину підпису

$$r = g^k(p) = 3^7 = 11(17).$$

Потім — другу частину підпису за формулою

$$s = k^{-1}(h - xr) \bmod q.$$

Одержуємо: $k^{-1} = 7(16)$ і $s = 14(16)$. Підпис дорівнює 11,14.

Перевірка підпису. Обчислюємо геш-код повідомлення h (припустимо, він дорівнює 9) и перевіряємо співвідношення

$$g^h = y^r r^s (p).$$

Одержуємо. $g^h = 3^9 = 14(17)$, $y^r = 5^{11} = 11(17)$, $r^s = 11^{14} = 9(17)$, $14 = 11 \cdot 9(17)$, тобто в даному випадку підпис є вірним.

3.4 Розкриття ключа або підробка підпису Ель-Гамаля, при невиконанні обмежень на довжину та порядок використання параметрів

Схеми цифрового підпису типу Ель-Гамаля стандартизовані та широко застосовуються на практиці. Відхилення від рекомендацій стандартів може привести до послаблення підпису.

Приклад 1. Нехай k відоме, тоді зі співвідношення

$$h = xr + ks \bmod (p-1)$$

знаходимо секретний ключ x і можемо підписувати повідомлення замість власника підпису.

Приклад 2. При повторення рандомізатора одержимо систему порівнянь відносно x і k виду,

$$h_1 = xr_1 + ks_1 \bmod (p-1),$$

$$h_2 = xr_2 + ks_2 \bmod (p-1),$$

що також призводить до визначення секретного ключа навіть при змінній геш-функції.

Приклад 3. Недотримання обмежень на розмір параметра: $r < p$.

Дійсно, нехай сторона, що перевіряє, не враховує можливість ситуації, коли $r > p$. Спостерігаючи за мережею зв'язку, можна одержати підписане повідомлення m та виділити блоки деякого істинного підпису r, s, пов'язаного із значенням геш-коду $h = h(m)$.

Нехай необхідно підробити підпис для повідомлення m_1. Насамперед обчислимо *геш-код*

$$h_1 = h(m_1).$$

Припустимо, геш-коди відрізняються деяким множником u, який можна знайти із порівняння

$$h_1 = uh \bmod (p-1).$$

Якщо це порівняння не має розв'язку, то перехоплюємо з мережі наступне підписане повідомлення і т.ін.

Для істинного підпису виконується перевірочне співвідношення

$$g^h = y^r r^s (p).$$

Спробуємо підібрати такий підпис r_1, s_1, щоб аналогічне співвідношення виконувалось для r_1, s_1, h_1.

Розглянемо

$$g^{h_1} = g^{uh} = [y^r r^s]^u(p),$$

тобто

$$g^{h_1} = y^{ru} r^{su}(p).$$

Очевидно, можна прийняти

$$s_1 = su \bmod (p-1).$$

Проте, якщо прийняти

$$r_1 = ru \bmod (p-1),$$

то перевірочне співвідношення виконуватися не буде, оскільки r_1 повинно брати участь в основі і показнику степеня одночасно, що не має місця. Вихід з положення існує, якщо допускається можливість значень $r_1 > p$.

Дійсно, r_1 у показнику і основі степеня приводяться за різними модулями, тобто повинні одночасно виконуватися порівняння

$$r_1 = ru \bmod (p-1)$$

і

$$r_1 = r \bmod p.$$

Модулі порівнянь взаємно прості, отже за китайською теоремою про залишки, існує розв'язок:

$$r_1 = r \bmod (p(p-1)),$$

проте $r_1 > p$.

Таким чином, для r_1, s_1 перевірочне співвідношення виконується, тобто підпис може бути підробленим, якщо обмеження на довжину параметрів не контролюються.

3.5 Алгоритм дискретного логарифмування Сільвера-Полліга-Хеллмана

Задача дискретного логарифмування є алгоритмічною проблемою, на якій основана стійкість багатьох криптоалгоритмів, що

використовуються на практиці. Тому методи дискретного логарифмування, що застосовуються в часткових випадках, є важливими, наприклад, з точки зору вибору параметрів криптосистеми.

Алгоритм Сільвера-Полліга-Хеллмана розв'язує задачу дискретного логарифмування в скінченному полі F_q, що складається з $q = P^\alpha$ елементів, за умови, що число $q-1$ — "гладке", тобто всі прості дільники числа $(q-1)$ є невеликими.

Останнє означає, що наявні ресурси пам'яті та обчислювальної потужності дозволяють виконати необхідні обчислення за прийнятний час.

Позначимо множину ненульових елементів поля F_q через F_q^*.

Нехай задане поле F_q та первісний елемент поля b. При заданому $y \in F_q^*$, потрібно знайти ціле x:

$$0 \le x < q-1,$$

таке, що виконується рівність

$$y = b^x.$$

Нехай канонічний розклад $q-1$ має вигляд:

$$q-1 = \prod_p p^a.$$

Позначимо кількість різних простих чисел у цьому розкладі через n. Нехай також m — максимальне просте число у розкладі $q-1$. Для зручності запису введемо додаткове позначення $u = q-1$.

Будемо користуватися тим фактом, що будь-який ненульовий елемент поля $g \in F_q^*$ задовольняє умові $g^{q-1} = 1$, тобто $g^u = 1$.

Алгоритм полягає у визначенні лишків числа x за усіма модулями виду p^a та відновлення x за допомогою китайської теореми про залишки.

Насамперед, побудуємо таблицю R розміром $n \times m$, рядкам якої надамо як мітки прості числа p із розкладу $q-1$. Заповнимо спочатку її нулями.

У рядок з міткою p помістимо числа

$$r_{p,j} = b^{ju/p}, \quad (j = 0, \ldots, p-1).$$

Очевидно $b^u = 1$, тому $r_{p,j}^p = b^{ju} = 1$, тобто числа $r_{p,j}$ — корені степеня p з одиниці у полі.

Подальша робота зводиться до обчислень, у результаті яких з'являються числа, які є коренями степеня p з одиниці у полі.

Для кожного такого числа необхідно буде визначити його позицію j (номер колонки) у рядку таблиці R з міткою p.

Оскільки у кожному рядку елементи різні, то для даного числа відповідна йому позиція визначається однозначно.

У ході обчислень систематично використовується факт, що коли число d ділить u і деяке число w, то

$$g^{uw/d} = 1.$$

Припустимо, що x представлено у p-ічній системі числення. Тоді його лишок за модулем p^a має вигляд

$$x = x_0 + x_1 p + \ldots + x_{a-1} p^{a-1} \mod p^a, \quad 0 \le x_i < p - 1.$$

Позначимо $y_0 = y$. Обчислимо $y_0^{u/p}$. Очевидно, $y_0^{u/p}$ — корінь степені p з одиниці, причому,

$$y_0^{u/p} = y^{u/p} = b^{xu/p} = b^{x_0 u/p + (x - x_0)u/p},$$

де $x - x_0 = x_1 p + \ldots + x_{a-1} p^{a-1}$.

Нагадаємо, що p ділить u, тому число $x_0 u/p$ є цілим.

У виразі $(x - x_0)u/p$ обидва співмножники діляться на p. Розділивши на p перший співмножник, одержуємо, що

$$(x - x_0)u/p = ku,$$

тому

$$y_0^{u/p} = b^{x_0 u/p}.$$

Порівнявши з позначеннями

$$r_{p,j} = b^{ju/p},$$

одержимо, що

$$y_0^{u/p} = r_{p,j}$$

при $j = x_0$.

Це дозволяє визначити x_0, як позицію $y_0^{u/p}$ у рядку таблиці R з міткою p.

При подальшій роботі для визначення x_i будемо попередньо ліквідовувати в показнику x усі члени x_j з індексами $j < i$.

Ліквідуємо x_0 в показнику степеня b^x, розділивши y_0 на b^{x_0}. Позначимо результат через y_1:

$$y_1 = \frac{y_0}{b^{x_0 p^0}}$$

та обчислимо

$$y_1^{u/p^2} = b^{u(x-x_0)/p^2}.$$

У виразі $x - x_0$ усі члени, крім $x_1 p$, діляться на p^2. Тому в показнику $u(x - x_0)/p^2$ усі члени, крім $ux_1 p/p^2$, кратні u і на значення $b^{u(x-x_0)/p^2}$ не впливають.

Оскільки u ділиться на p, то число $ux_1 p/p^2$ — ціле, звідки $y_1^{u/p^2} = b^{x_1 u/p} = r_{p,j}$ при $j = x_1$, таким чином, x_1 дорівнює позиції y_1^{u/p^2} у рядку з міткою p таблиці R.

Для визначення x_2 ліквідуємо x_1 у показнику степеня b^{x-x_0}, розділивши y_1 на $b^{x_1 p^1}$. Одержимо

$$y_2 = \frac{y_0}{b^{x_0 p^0 + x_1 p^1}},$$

тобто $y_2 = b^h$, де

$$h = x_2 p^2 + \ldots + x_{a-1} p^{a-1}.$$

Обчислюємо далі $y_2^{u/p^3} = b^{x_2 u/p} = r_{p,j}$ при $j = x_2$, що дозволяє визначити x_2 за таблицею R, і так далі, поки не визначимо x_{a-1}.

Повторивши процедуру для кожного p, що ділить $q - 1$, одержуємо значення $x \mod p^a$ для всіх p і всіх a.

За допомогою китайської теореми про залишки, відновлюємо x.

Приклад. У полі F_{37} при $b = 2$ знайти дискретний логарифм елемента 28.

Розв'язок. Задача зводиться до розв'язування в полі F_{37} рівняння $28 = 2^x$.

Число $q = 37$ є першим степенем простого числа, тому операції у полі збігаються з операціями у полі лишків за модулем 37, зокрема, ділення є множенням на зворотний елемент.

Оскільки $u = q-1 = 36 = 2^2 \cdot 3^2$, то маємо два простих дільники: 2 і 3.

Складемо таблицю R. Почнемо з рядка з міткою $p = 2$. Обчислимо $r_{2,j} = b^{j(q-1)/2}$ для $j = 0, 1$: $r_{2,0} = 1$, $r_{2,1} = 2^{(q-1)/2} \equiv -1(37)$.

Елементами рядка з міткою 3 є числа: $r_{3,j} = b^{j(q-1)/3}$, $j = 0, 1, 2$, тобто: $r_{3,0} = 1$, $r_{3,1} = 2^{36/3} \equiv 26(37)$, $r_{3,2} = 2^{2 \cdot 36/3} \equiv 2^{24} \equiv 10(37)$. Таблиця R має наступний вигляд.

$R =$

	0	1	2
2	1	-1	0
3	1	26	10

Знайдемо лишок

$$x = x_0 + x_1 p + \ldots + x_{a-1} p^{a-1} \mod p^a, \quad (p = 2, a = 2).$$

Число кроків дорівнює $a = 2$. Отже необхідно визначити x_0, x_1. Знайдемо x_0. Обчислимо

$$y_0^{u/p} = 28^{18} \equiv 1(37).$$

Позиція одиниці у другому рядку таблиці R дорівнює нулю, отже, $x_0 = 0$.

Далі будемо обчислювати значення y_k та віднести їх до степеня u/p^{k+1}.

Обчислимо y_1, ліквідувавши член x_0 у показнику числа b^x:

$$y_1 = \frac{y_0}{b^{x_0 p^0}}.$$

Оскільки $x_0 = 0$, то $y_1 = y_0$. Підносимо y_1 до степеня u/p^2, де $p^2 = 4$:

$$y_1^{u/4} = 28^{36/4} = -1(37).$$

Позиція числа -1 у рядку 2 таблиці R дорівнює 1, звідки, $x_1 = 1$. Отже

$$x = x_0 + x_1 p = 2 \mod 4.$$

Знайдемо лишок $x \bmod p^a$, при $p = 3, a = 2$. Число кроків дорівнює $a = 2$.

$y_0^{u/p} = 28^{12} \equiv 26(37)$. Позиція числа 26 у рядку 3 таблиці R дорівнює 1, отже, $x_0 = 1$, тому $y_1 = y_0/p^{x_0 p^0} = 14$. Підносимо y_1 до степеня u/p^2: $y_1^{u/9} = 14^{36/9} = 10(37)$, звідки, $x_1 = 2$. Отже, $x = 7 \bmod 9$.

Розв'язуємо систему порівнянь $x = 2 \bmod 4$, $x = 7 \bmod 9$: $4^{-1}(9) = 7$, $9^{-1}(4) = 1$, $x \equiv 2 \cdot 9 \cdot (9^{-1} \pmod 4) + 7 \cdot 4 \cdot (4^{-1} \pmod 9) = 214$, тобто $x \equiv 34 \pmod{36}$.

3.6 Ро-метод факторизації Поларда

Назва пов'язана з тим, що метод здійснює пошук дільників числа n виходячи з властивостей циклічності деяких послідовностей.

Ці послідовності не є чисто періодичними, а мають так звані підходи до циклів, що графічно виглядає як грецька буква ρ (ро).

Даний метод є суттєво ефективнішим, ніж метод повного перебору дільників n.

Крім того, ідея методу може застосовуватися і в інших ситуаціях, наприклад, для логарифмування у групах точок еліптичних кривих.

В ро-методі, насамперед, вибирається деяке відображення $f: Z_n \to Z_n$ кільця лишків за модулем n в себе. Необхідно, щоб значення цього відображення можна було б обчислити достатньо швидко. Наприклад, це може бути поліном із цілими коефіцієнтами, скажемо $f(x) = x^2 + x + 1 \mod n$.

Потім псевдовипадковим чином вибирається число x_0 (початкове значення) та розглядаються елементи послідовних ітерацій:

$$x_{j+1} = f(x_j) \bmod n, \quad j = 0, 1, 2, ...,$$

тобто $x_1 = f(x_0)$, $x_2 = f(x_1)$, $x_3 = f(f(f(x_1)))$ і так далі.

Очевидно, дана послідовність циклічна не тільки як послідовність лишків за модулем n, але і як послідовність лишків за деяким простим дільником $p < \sqrt{n}$ числа n.

Розглянемо пари елементів послідовності.

Серед цих пар знайдуться такі, скажемо x_j, x_k, що $x_j \neq x_k(n)$, але $x_j = x_k(p)$.

Якщо така пара, назвемо її критичною, знайдеться серед множини пар, що розглядається, то можна знайти власний дільник r числа n виду

$$r = (x_j - x_k, n) = \lambda p.$$

Приклад. Знайти нетривіальний дільник числа $n = 2431$.

Виберемо

$$f(x) = x^2 + x + 1, \quad x_0 = \lfloor \sqrt{2431} \rfloor = 50.$$

Обчислимо рекуренту та перевіримо пари: $x_0 = 50(2431)$, $x_1 = 50^2 + 50 + 1 = 120(2431)$, $x_2 = 2366(2431)$, $x_3 = 1730(2431)$, $x_4 = 2070(2431)$ і так далі. При цьому величина $x_4 - x_1 = 1950(2431)$ має з n, нетривіальний спільний дільник $2431, 1950) = 13$.

Бажано максимально скоротити кількість пар, що підлягають перевірці. З цієї точки зору вибір поліномів в якості відображення f є зручним, оскільки з $x = y \pmod p$ випливає $f(x) = f(y) \pmod p$. Очевидно, розташування критичних пар визначається властивостями рекуренти, приведеної за (невідомим) модулем r. До її складу входять r різноманітних елементів.

Виявляється, що при пошуку критичної пари можна виграти у часі, якщо працювати з більш довгою послідовністю $x_0, x_1, ..., x_{i-1}$, але для кожного елемента x_k, що формується заново, обчислювати $(x_j - x_k, n)$ тільки один раз, використовуючи елементи x_j, що мають деякі фіксовані номери.

Суть у тому, що якщо пара (x_j, x_k) є критичною, то

$$f(f(f(x_j))) = f(f(f(x_k))) \bmod p$$

для будь-якого числа ітерацій. Іншими словами, пари виду (x_{j+s}, x_{k+s}) слід перевіряти не більше одного разу.

До того ж нам не обов'язково шукати критичні пари з мінімальними номерами, щоб розв'язати задачу.

Запропонований спосіб спирається на пошук критичної пари, яка не обов'язково є першою, тому необхідна довжина рекуренти l збільшується. Виявляється, вона збільшується не більше, ніж у чотири рази.

Нехай (j_0, k_0) — мінімальні індекси критичної пари, що існує у нашій рекуренті. Знайдемо індекси іншої критичної пари (j, k), де

$$k - j = k_0 - j_0.$$

Будемо орієнтуватися на довжину представлення k_0 у двійковій системі числення. Нехай представлення k_0 у двійковій системі займає $h + 1$ біт. Це означає, що $2^h \le k_0 < 2^{h+1}$.

Виберемо за j максимальне $(h + 1)$–бітове число, тобто

$$j = 2^{h+1} - 1.$$

Тоді

$$k = j + (k_0 - j_0).$$

Оскільки $k_0 > j_0$, то

$$2^{h+1} \le k < 2^{h+2}.$$

Отже,

$$k < 4 \cdot 2^h \le 4k_0 \le 4l.$$

Таким чином, ми можемо шукати критичні пари, на основі випробування усіх значень $k > j$ в кожному діапазоні виду

$$2^m \le k < 2^{m+1}$$

при фіксованому, визначеному діапазоном, значенні

$$j = j(m) = 2^m - 1.$$

Ці пари мають індекси виду

$$(2^m - 1, 2^m \le k < 2^{m+1}).$$

Приклад. Розкладемо число $n = 4087$, використовуючи

$$f(x) = x^2 + x + 1, \quad x_0 = 2.$$

$x_1 = f(2) = 7(n)$, $(x_1 - x_0, n) = (7 - 2, n) = 1$;
діапазон двобітових значень k: $m = 1$, $j = 1$:
$x_2 = f(7) = 57(n)$, $(x_2 - x_1, n) = (57 - 7, n) = 1$;

$x_3 = f(57) = 3307(n)$, $(x_3 - x_1, n) = (3307 - 7, n) = 1$;
діапазон $m = 2$, $j = 3$:
$x_4 = f(3307) = 2745(n)$, $(x_4 - x_3, n) = (2745 - 3307, n) = 1$;
$x_5 = f(2745) = 1343(n)$, $(x_5 - x_3, n) = (1343 - 3307, n) = 1$;
$x_6 = f(1343) = 2626(n)$, $(x_6 - x_3, n) = (2626 - 3307, n) = 1$;
$x_7 = f(2626) = 3734(n)$, $(x_7 - x_3, n) = (3734 - 3307, n) = 61$;
$4087 = 61 \cdot 67$.

3.7 (p-1) алгоритм факторизації Полларда

На основі аналізу **криптосистеми RSA** легко виявити, що складність **задачі факторизації** модуля $N = pq$, на якій основана стійкість системи, залежить від співвідношення між співмножниками, наприклад, від величини різниці $p - q$.

Виявляється, на складність факторизації впливають, крім того, індивідуальні особливості кожного із співмножників, які виражені як теоретико-числові властивості деяких функцій від p і q.

Нехай дано непарне натуральне число $n = pq$, де p — його найменший простий дільник. Розглянемо задачу факторизації n, за умови, що число $p - 1$ є гладким, тобто

$$p - 1 = \prod_i p_i^{m_i}, \quad \forall_i \cdot p_i < B,$$

де B — границя, що визначається обчислювальними можливостями при реалізації алгоритму.

Припустимо, для деякого a, $(a, n) = 1$, вдалося локалізувати значення $ord_p a$, яке, очевидно ділить $p - 1$.

Наприклад, вдалося знайти число ν, що задовольняє наступним умовам:

1) ν ділиться на $ord_p a$;

2) $a^\nu = 1 \bmod p$, але $a^\nu \neq 1 \bmod n$.

У цьому випадку, оскільки $a^\nu - 1$ не ділиться на n, можна визначити $p = (a^\nu - 1, n)$. Залежно від обчислювальних можливостей вибираємо параметр k і будуємо число $\nu = \nu(k)$, так, щоб $\nu(k)$ ділилося на $p-1$. Наприклад, $\nu(k) = k!$, або $\nu(k) =$НСК$(1, 2, ..., k)$, де $k = \lfloor \sqrt{n} \rfloor$, оскільки $p < \sqrt{n}$. Даний етап є неформальним і найбільш складним.

Не виключено, наприклад, що слід вибирати $\nu(k) = m(k)^h$ як степінь добутку усіх, або частини простих чисел, що є меншими за B, оскільки $p-1$ може ділитися на високі степені малих простих чисел. При цьому h слід вибирати починаючи з мінімального значення.

Якщо $p-1$ ділить $\nu(k)$, то порядки $ord_p a$ усіх чисел, що є взаємно прості з p, також ділять $\nu(k)$. Отже $a^\nu = 1 \bmod p$.

Тим не менше, не можна стверджувати, що $a^\nu \neq 1 \bmod n$, оскільки можливий випадок, коли $ord_n a$ ділить $\nu(k)$. Тому при $(a^\nu - 1, n) = n$ необхідно псевдовипадковим чином вибрати нове значення a та повторити обчислення $(a^\nu - 1, n)$.

Приклад. Знайти нетривіальний дільник d числа $n = 2431 = p_1 p_2 p_3 = 11 \cdot 13 \cdot 17$.

Виберемо відносно невелике $k = 7 \leq \lfloor \sqrt[4]{n} \rfloor$.

Зауважимо, що при виборі $\nu(k) = (2 \cdot 3 \cdot 5 \cdot 7)^4$ ми не зможемо розв'язати задачу, оскільки усі $\varphi(p_i)$, $i = 1, 2, 3$ ділять $\nu(k)$ і $(a^\nu - 1, n) = n$ для усіх a, що є взаємно простими з n.

Нехай $\nu(k) = (2 \cdot 3 \cdot 5 \cdot 7)^2 = 210^2$. У даному випадку $\varphi(17)$ не ділить $\nu(k)$. Звичайно, заздалегідь це не може бути відомо.

Виберемо a: $(a, n) = 1$, наприклад, $a = 3$. Обчислимо $(a^\nu - 1, n) = 3^{210 \cdot 210} - 1 \bmod n$.

Одержимо:

$$a^\nu - 1 = 3^{180} - 1 = 1287 \mod 2431,$$

d =НСД(1287,2431)=143.

3.8 Алгоритм факторизації Діксона

В багатьох алгоритмах факторизації непарного числа n використовується ідея Лежандра, яка полягає у пошуку пар чисел x, y, що задовольняють співвідношенню $x^2 = y^2(n)$.

Скажемо, що для чисел x, y виконується нетривіальне співвідношення $x^2 = y^2(n)$, якщо $x \neq \pm y(n)$. Для таких чисел вираз $(x - y)(x + y)$ ділиться на n, при цьому кожний з указаний співмножників, наприклад, $(x - y)$, має з n нетривіальний спільний дільник.

В **алгоритмі Діксона** застосовується побудова нетривіальних співвідношень для чисел x, y виходячи з множини відносно невеликих простих чисел, що формується заздалегідь.

Ця множина називається **факторною базою**: $B = \{p_1, \ldots, p_k\}, \max p_i \leq M$. Границя M вибирається, виходячи з наявності обчислювальних ресурсів.

Звичайно з метою зменшення абсолютних величин чисел, що беруть участь в обчисленнях, у факторальну базу вводять число -1.

Скажемо, що натуральне число b є B-числом, якщо після приведення за модулем n число b^2 розкладається на добуток степенів простих чисел з факторної бази, іншими словами, якщо

$$b^2 \bmod n = \prod_{p \in B} p^{u_p(b)}.$$

Відзначимо, що при $b^2 < n$ усі показники у правій частині останньої рівності парні, тобто відміни від випадку розкладу квадрата натурального числа нема.

Якщо ж $b^2 > n$, то після приведення за модулем n, розклад його лишку може містити як парні, так і непарні степені простих чисел.

Таким чином, з однієї сторони, $b^2 \bmod n$ є добутком квадратів, а з іншої сторони — його можна записати інакше: у вигляді добутку як парних, так і непарних степенів простих чисел.

Це можливо тому, що розклад лишків на степені співмножників, що є простими натуральними числами, неоднозначний, внаслідок операції приведення за модулем.

Якщо ми знайдемо декілька B-чисел, то перемножуючи відповідні частини порівнянь виду

$$b^2 \bmod n = \prod_{p \in B} p^{u_p(b)},$$

одержуємо у лівій частині квадратичний лишок, корінь із якого нам є відомим.

Метод пошуку другого кореня, що дає нетривіальне співвідношення, у загальному випадку не знайдений.

Проте, знаючи показники у правій частині для кожного B-числа, можна виявити випадок, коли всі показники в їхньому добутку стануть парними. Тоді можна знайти другий корінь, зменшуючи показники вдвічі.

Алгоритм Діксона здійснює цілеспрямований пошук потрібних випадків, збільшуючи ймовірність одержання нетривіального співвідношення.

Приклад. Нехай необхідно факторизувати число $n = 1829$.

Як факторну базу B виберемо деяку підмножину простих чисел, які є меншими за 15, до яких додамо (-1): $B = \{-1, 2, 3, 5, 7, 11, 13\}$.

Необхідно знайти достатню кількість B-чисел. Такі числа b_i характеризуються умовою розкладу за елементами бази:

$$b_i^2 \bmod n = \prod_j p_j^{u_{i,j}}.$$

Будемо шукати їх серед чисел виду $\lfloor\sqrt{1829k}\rfloor$ і $\lfloor\sqrt{1829k}\rfloor + 1$, $k = 1, 2, ...$, поки не наберемо достатньо для виникнення необхідної ситуації.

Для $k = 1$ отримаємо два числа: $\lfloor\sqrt{1829k}\rfloor = 42$ і 43.

Оскільки $42^2 = 1764 = -65(1829)$, то 42 є B-числом. Дійсно $42^2 = (-1)^1 5^1 13^1 (1829)$. Аналогічно $43^2 = 2^2 5^1 (1829)$.

Зазначимо, що кожному B-числу b зручно поставити у відповідність вектор $a(b)$ показників розкладу $b^2 \bmod n$ за елементами бази.

Відсутнім у розкладі елементам бази, відповідає показник, що дорівнює нулю.

Таким чином, $a(42) = (1001001)$, $a(43) = (0201000)$.

Оскільки у ході алгоритму виникає необхідність обчислень сум векторів з точністю до парності компонент, тобто операцій над векторами за модулем два, введемо вектор $e(b) = a(b) \bmod 2$. Таким чином $e(42) = (1001001)$, $e(43) = (0001000)$.

Нашою метою є одержання стільки B-чисел, щоб з них можна було вибрати підмножину, для якої сума векторів виду $a(b)$ складалася би з парних координат. Це є еквівалентним лінійній залежності відповідних векторів виду $e(b)$ над $GF(2)$.

Тепер ясно, що необхідна кількість B-чисел не перевищує збільшеної на 1 розмірності векторів $e(b)$.

Можна впевнитись, що числа $42, 43, 61, 74, 85, 86$ є B-числами.

Випишемо таблицю відповідних векторів виду $e(b)$.

	-1	2	3	5	7	11	13
42	1	0	0	1	0	0	1
43	0	2	0	1	0	0	0
61	0	0	2	0	1	0	0
74	1	0	0	0	0	1	0
85	1	0	0	0	1	0	1
86	0	4	0	1	0	0	0

Очевидно, $e(43) \oplus e(86) = (0000000)$. Перемножимо квадрати відповідних B-чисел за модулем n.

Прирівнюємо результат до добутку розкладу квадратів відповідних чисел, одержаних на основі векторів $a(b)$ із таблиці: $43^2 \cdot 86^2 = 2^6 5^2 (\mathrm{mod} 1829)$.

Можна добути корені з обох частин та записати $(43 \cdot 86) = \pm 40 (\mathrm{mod} 1829)$, але ліва частина дорівнює $(43 \cdot 86) = 40(1829)$ і ми одержуємо тривіальне співвідношення. Необхідно продовжити пошук лінійно залежних векторів виду $e(b)$.

Зазначимо, що $e(42) \oplus e(43) \oplus e(61) \oplus e(85) = (0000000)$.

Тому випишемо порівняння $42^2 \cdot 43^2 \cdot 61^2 \cdot 85^2 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \pmod{1829}$, що дає співвідношення $1459^2 = 901^2 \pmod{1829}$, де $1459 \neq \pm 901 \pmod{1829}$.

Тому число НСД (1459+901,1829)=59 є дільником 1829.

3.9 Атаки на RSA, що не використовують факторизацію: спільний модуль, мультиплікативна атака на підпис, атака Франкліна

Відомою властивістю **криптосистеми RSA** є залежність її стійкості від властивостей співмножників модуля $n = pq$. При необґрунтованому виборі цих співмножників можливе повне дешифрування криптосистеми. Важливою особливістю криптосистеми RSA є можливість читання окремих повідомлень або підробка

цифрового підпису незалежно від властивостей співмножників модуля, наприклад, за рахунок невдалого вибору відкритого ключа.

Суттєвим може бути і те, що послабити стійкість системи можна без розкриття секретного ключа, використовуючи її для зашифрування сторонніх повідомлень з метою використання специфічних математичних співвідношень.

Таким чином, стійкість криптосистеми RSA може змінюватися залежно від особливостей її проектування та експлуатації.

Спільний модуль

Нехай в мережі використовується спільне значення модуля для декількох абонентів та перехоплені криптограми виду

$$c_1 = m^{e_1}(n), \quad c_2 = m^{e_2}(n),$$

де експоненти взаємно прості.

Якщо обчислити за допомогою розширеного алгоритму Евкліда значення r, s:

$$re_1 + se_2 = 1,$$

то маємо можливість визначити відкритий текст:

$$c_1^r c_2^s = m(n).$$

Покажемо необхідність вибору неспівпадаючих модулів при побудові криптосистеми RSA для різних користувачів довіреною особою. Уточнимо, що у цьому випадку числа p, q користувачам невідомі.

Нехай користувачі A і B використовують відповідно криптосистеми з параметрами (e_A, d_A, n) і (e_B, d_B, n). Очевидно, що, скажемо, користувач B у стані обчислити значення

$$e_B d_B - 1 = k\varphi(n),$$

хоча співмножники у правій частині йому невідомі. Виходячи з побудови криптосистеми,

$$(e_A, \varphi(n)) = 1,$$

отже, найбільший спільний дільник чисел e_A і $e_B d_B - 1$ співпадає з $d = (e_A, k)$. тому числа e_A і $\frac{e_B d_B - 1}{d}$ взаємно прості. Крім того,

$$\frac{e_B d_B - 1}{d} = \frac{k}{d}\varphi(n),$$

тобто ліва частина ділиться на $\varphi(n)$.

За допомогою алгоритму Евкліда можна знайти числа C і D, такі, що

$$\frac{e_B d_B - 1}{d} C + e_A D = 1,$$

тобто $e_A D = 1(\varphi(n))$. Таким чином розшифрування повідомлень користувача А можна здійснювати за допомогою ключа D.

Мультиплікативна атака на RSA

Нехай А - власник криптосистеми з параметрами (e, d, n).

Очевидно, якщо c — шифротекст, то розшифроване повідомлення має вигляд:

$$m = c^d(n).$$

Виберемо псевдовипадкове число x виду

$$x = r^e(n)$$

та обчислимо добуток

$$y = xc(n),$$

тобто замаскуємо шифротекст. Якщо за просьбою абонента В абонент А підпише повідомлення y: (y, y^d), то абонент В одержить значення

$$y^d = x^d c^d = rm(n),$$

звідки можна знайти m. Очевидно, використання геш-функції не дозволить скористатися цією лазівкою.

Атака Франкліна

При зашифруванні повідомлень з відомою за модулем n різницею, на стійкість криптосистеми може вплинути величина відкритого ключа.

Нехай $e = 3$, m_1, m_2 — повідомлення,

$$m_2 = m_1 + \Delta \pmod{n}$$

та відповідні шифротексти дорівнюють $a = m_1^e(n)$, $b = m_2^e(n)$.

Те ж саме, іншими словами, означає, що два многочлени $g(x) = x^3 - a$ і $f(x) = (x+\Delta)^3 - b$ мають спільний корінь $x = m_1(n)$. Звідси випливає, що m_1 є коренем найбільшого спільного дільника вказаних многочленів. Умова взаємної однозначності шифру дозволяє легко визначити корінь полінома НСД$(f(x), q(x))$ у випадку, коли його степінь більша за одиницю.

З великою ймовірністю виконуються також умови оборотності за модулем n деяких елементів (вони будуть очевидні по ходу викладання), при яких шуканий найбільший спільний дільник має вигляд $ux + \nu$ і його корінь може бути обчислений у кільці за модулем n.

Нагадаємо, що $d(x) =$НСД$(f(x), g(x))$, де степінь $f(x)$ не менша за степінь $g(x)$, можна знайти за допомогою алгоритму Евкліда:

$$r_1(x) = f(x) \bmod g(x),$$

$$r_2(x) = g(x) \bmod r_1(x),$$

$$r_3(x) = r_1(x) \bmod r_2(x)$$

і так далі, поки залишок від ділення не стане рівним нулю. У цьому випадку попередній залишок є $d(x)$.

Обчислимо НСД$(f(x), q(x))$ за модулем n явно, з невизначеними коефіцієнтами.

Маємо: $f(x) = (x + \Delta)^3 - b$, $g(x) = x^3 - a$, тобто

$$f(x) = x^3 + 3x^3\Delta + 3x\Delta^2 + \Delta^3 - b.$$

Поділивши $f(x)$ на $g(x)$, одержимо, що старший член частки дорівнює 1. Тому залишок від ділення дорівнює

$$r_1(x) = f(x) - 1 \cdot g(x),$$

где $r_1(x) = 3x^2\Delta + 3x\Delta^2 + \Delta^3 - b + a$.

Ясно, що $d(x) =$НСД$(r_1(x), g(x))$.

Ділимо $g(x)$ на $r_1(x)$, отримуємо старший член частки, що дорівнює $\frac{1}{3\Delta}x$.

Таким чином,

$$g(x) = \frac{1}{3\Delta}xr_1(x) + s_2(x),$$

де

$$s_2 = -x^2\Delta - \frac{1}{3\Delta}(\Delta^3 + a - b)x - a.$$

Отже, $d(x) =$НСД$(r_1(x), s_2(x))$. Тому далі ділимо $r_1(x)$ на $s_2(x)$ і одержуємо старший член частки, що дорівнює (-3). Обчислюємо залишок від ділення $r_1(x)$ на $s_2(x)$, який має вигляд:

$$d(x) = [3\Delta^2 - \frac{1}{\Delta}(\Delta^3 + a - b)]x + \Delta^3 - 2a - b.$$

Звідки одержуємо корінь полінома $d(x)$:

$$m_1 = x = \frac{\Delta(2a + b - \Delta^3)}{2\Delta^3 - a + b}.$$

Умови коректності обчислень очевидні: НСД$(\Delta, n) = 1$, НСД$(2\Delta^3 - a + b, n) = 1$.

3.10 Задача перевірки чисел на простоту. Решето Ератосфена. Тест на основі малої теореми Ферма. Властивості чисел Кармайкла

При створенні асиметричних криптосистем, а також при модифікації їхніх параметрів в ході експлуатації, виникає необхідність побудови надвеликих **псевдовипадкових простих чисел**, що мають деякі специфічні властивості.

Відповідні обчислювальні процедури включають алгоритми, що реалізують етап тестування чисел на простоту.

В основі тестів лежать так звані **критерії простоти**.

На практиці використовуються два типи критеріїв простоти: **детерміновані** та **ймовірнісні**. Детерміновані тести дозволяють довести, що число, яке підлягає тестуванню, є простим.

Детерміновані тести, що застосовуються на практиці, здатні дати відповідь не для кожного простого числа, оскільки використовують достатні умови простоти.

Ці тести більш корисні, коли необхідно побудувати велике просте число, а не перевірити простоту, скажемо, деякого окремого числа.

На відміну від детермінованих, ймовірнісні тести можна ефективно використати для тестування окремих чисел, проте їх результати, з деякою ймовірністю, можуть бути невірними. На щастя, ціною кількості повторень тесту з модифікованими вхідними даними, ймовірність помилки можна зробити довільно малою.

Широко відомий наступний метод послідовної побудови списку всіх простих чисел, що не перевищують заданого числа N. Цей метод називається **решетом Ератосфена**.

У списку L всіх чисел від 2 до N викреслимо числа, що кратні 2, більші за двійку. Із решти чисел вибираємо найменше (воно дорівнює 3), а з L викреслимо числа, що кратні 3 і більші за трійку і т.ін. Якщо чергове найменше число, що вибирається з L, $a > \lfloor\sqrt{N}\rfloor$, то роботу зупиняємо. Числа, що залишилися в L складають шуканий список простих чисел.

Чи існують взагалі критерії простоти, які є необхідними та достатніми?

Прикладом такого критерію є так званий **критерій Вільсона**: число n є простим тоді і тільки тоді, коли

$$(n-1)! = -1(n).$$

При побудові ймовірнісних критеріїв простоти виникає ряд типових питань, які зручно розглядати на прикладі **тесту на основі малої теореми Ферма**. Ця теорема стверджує, якщо n — просте, то для всіх a, взаємно простих з n, виконується умова (порівняння Ферма):

$$a^{n-1} = 1(n).$$

Таким чином, якщо умова **теореми Ферма** не виконана хоча би для одного числа в інтервалі $\{2, \ldots, n-1\}$, то a — складене.

Тест на основі **малої теореми Ферма** полягає у наступному.

Псевдовипадковим чином вибирається лишок $a \in \{2, \ldots, n-1\}$ та перевіряється умова $(a, n) = 1$. Перевіряємо умову теореми

Ферма. Якщо вона не виконується, то число n складене. Якщо виконується, то повторюємно тест для іншого значення a і так далі.

Існують складені числа n, для яких при деякому a виконується умова малої теореми Ферма, наприклад,

$$2^{240} = (2^{10})^{34} = 1(341), \quad 7^{24} = 1(25).$$

Назвемо непарне складене число n псевдопростим за основою a, якщо пара (a, n) задовольняє порівнянню $a^{n-1} = 1(n)$. Можна довести, що це визначення є еквівалентним умові, за якою $(a, n) = 1$ і $ord_n a|(n-1)$.

Відомо, що для будь-якого $a > 1$ існує нескінченно багато псевдопростих чисел за основою a.

Виявляється, якщо існує (невідома) основа a, за якою n не є псевдопростим, то при повторенні тесту Ферма ймовірність k-кратного виконання порівняння $a_k^{n-1} = 1(n)$ дорівнює $(1/2)^k$. У цьому випадку ймовірність помилки тесту наближається до нуля із збільшенням k.

Отже, проблема може виникнути тільки тоді, якщо n є псевдопростим для усіх (ненульових) основ.

Тим не менше, такі числа існують. Вони називаються **числами Кармайкла**. Наприклад, числом Кармайкла є число

$$n = 561 = 3 \cdot 11 \cdot 17.$$

Властивості чисел Кармайкла описуються наступною теоремою.

Теорема. Нехай n непарне складене число. Тоді

а) якщо $p^2|n$, $p > 1$, то n не є числом Кармайкла;

б) якщо $n = p_1, p_2, \ldots, p_k$, $p_i \neq p_j$ $(i \neq j)$, то n число Кармайкла тоді і тільки тоді, коли $\forall_i (p_i - 1)|(n-1)$;

в) якщо $n = p_1, p_2, \ldots, p_k$, $p_i \neq p_j$ $(i \neq j)$ — число Кармайкла, то $k \geq 3$.

Числа Кармайкла зустрічаються досить рідко. В межах до 100000 існує лише 16 чисел Кармайкла, але відомо, що множина чисел Кармайкла є нескінченною множиною.

3.11 Імовірнісні тести перевірки чисел на простоту. Тест Соловея-Штрассена

При тестуванні чисел на простоту за допомогою **ймовірнісного тесту**, основаного на малій теоремі Ферма, може виникнути ситуація, коли ймовірність помилки не знижується із збільшенням кількості повторювань тесту.

У цьому випадку вона дорівнює одиниці і в результаті тестування може бути прийняте невірне рішення. У зв'язку з цим розроблені та застосовуються на практиці ймовірнісні тести, вільні від вказаного недоліку.

Тест Соловея-Штрассена використовує **критерий Ейлера** для визначення значення **символу Лежандра** (квадратичного характеру числа за простим модулем). В обчисленнях, природно, використовується **символ Якобі**. Основою тесту є наступне твердження.

Теорема. Непарне ціле число n є простим тоді і тільки тоді, коли для всіх чисел a: $1 \leq a \leq n-1$ виконується порівняння виду

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \bmod n.$$

Назвемо вказане порівняння співвідношенням Ейлера.

Складене число n, що задовольняє співвідношенню Ейлера, називається ейлеровим псевдопростим за основою a. Відомо, що ейлерові псевдопрості є псевдопростими числами.

Із теореми видно, що складених чисел, які були би ейлеровими псевдопростими за будь-якою основою, не існує.

Тест Соловея-Штрасена є аналогічним **тесту Ферма**.

Псевдовипадковим чином вибираємо лише $a \in \{2, \ldots, n-1\}$, перевіряємо умову $(a, n) = 1$. Якщо умова не виконується, значить, n — складене. Перевіряємо співвідношення Ейлера. Якщо воно не виконується, то число n — складене. Інакше, перевіряємо тест для іншого значення a.

Якщо ми би змогли перевірити співвідношення Ейлера для всіх a, то ми змогли би точно визначити, чи є число n простим. Але для великих n це неможливо. Тому необхідно знати, як поводить себе ймовірність помилки із збільшенням числа k повторювань тесту.

Виявляється, що при повторюванні тесту Соловея-Штрассена k раз ймовірність невідбраковки складеного числа $\leq (1/2)^k$.

3.12 Ймовірнісні тести перевірки чисел на простоту. Тест Рабіна-Міллера

У **тесті Рабіна-Міллера** використовується критерій, оснований на факті, що для простого модуля квадратичними коренями з одиниці є лише числа ± 1, а для складеного непарного модуля $n = u\nu$, $(u, \nu) = 1$, число таких коренів більше двох.

Нехай n — непарне натуральне число. Тоді можна записати $n - 1 = 2^s t$, де t — непарне число і $s \geq 1$. Якщо число n — просте, то

$$a^{n-1} = 1(n)$$

при $(a, n) = 1$. Тому квадратні корені з одиниці мають вигляд: $a^{(n-1)/2} = \pm 1(n)$, де показник дорівнює $2^{s-1}t$.

При добування квадратних коренів із одиниці за простим модулем ми або весь час будемо одержувати одиницю, або виникне корінь, що дорівнює $-1(n)$.

Це означає, що в ряду лишків за модулем n чисел $a^t, a^{2t}, \ldots, a^{2^{s-1}t}$ або з'явиться $-1(n)$, або усі вони порівняні з одиницею, що можливо, коли $a^t = 1(n)$.

Якщо n — складене, то можливі й інші випадки.

Оснований на даному зауваженні тест Рабіна-Міллера полягає у наступному:

1) псевдовипадковим чином вибираємо лишок $a \in \{2, \ldots, n-1\}$, перевіряємо умову $(a, n) = 1$. Якщо умова не виконана, значить n — складене і робота закінчена;

2) обчислюємо $a^t (\mathrm{mod} n)$. Якщо $a^t = \pm 1(\mod n)$, то не виключено, що число n — просте і необхідно перейти на початок, щоб повторити тест для іншої основи;

3) обчислюємо послідовно лишки чисел $a^{2t}, \ldots, a^{2^{s-1}t}$ за модулем n, поки не з'явиться -1, або не закінчиться список.

4) якщо -1 виявлена у списку, то не виключено, що число n — просте і необхідно перейти на початок, щоб повторити тест для іншої основи;

5) якщо ні одне число із списку не порівняне з -1, то число n — складене і необхідно закінчити роботу.

Існують **складені числа**, які при відповідних a проходять тест Рабіна-Міллера.

Назвемо складене число $n = 2^s t+1$, де $s \geq 1, t$ непарне, **сильно псевдопростим** за основою $a > 1$, якщо виконується одна з двох умов: $a^t = \pm 1(n)$, або у послідовності $a^{2t}, \ldots, a^{2^{s-1}t}$ існує число, що є порівняним з -1 за модулем n.

Можна довести наступні основні властивості сильно псевдопростих чисел:

1) Число n сильно псевдопросте за основою a є ейлеровим псевдопростим за цією ж основою.

2) Для будь-якого $a > 1$ існує нескінченно багато сильно псевдопростих чисел n за основою a. Приклади: $a = 7$, $n = 25$, $a = 5$, $n = 781$.

3) Якщо непарне складене число n є сильно псевдопростим за основою a, то загальна кількість основ, за якими це число є сильно псевдопростим, не перевищує $(n-1)/4$.

Таким чином, при повторенні тесту Рабіна-Міллера k раз імовірність невідбраковки складеного числа $\leq (1/4)^k$.

Виявляється, що кількість повторень тесту, достатніх для практичних додатків, можна обмежити величиною $2\log_2^2 n$.

Слід відзначити, що простоту невеликих простих чисел можна перевірити, якщо використати декілька заздалегідь вказаних невеликих основ.

Приклади: якщо $n < 1373653$ — сильно псевдопросте за основами 2 і 3, то n — просте; якщо $n < 341550071728321$ — сильно псевдопросте за основами 2, 3, 5, 7, 11, 13, 17, то n — просте.

3.13 Детерміновані тести перевірки чисел на простоту. Теорема Поклінгтона. Узагальнення критерію Люка

Детерміновані тести перевірки чисел на простоту застосовуються для побудови псевдовипадкових простих чисел.

Загальна схема в даному випадку така: вибирається псевдови-

падкове число, яке тестується на простоту. Власне тест полягає у побудові членів деякої послідовності, які пов'язані з числом, що тестується, та мають особливості, якщо це число просте.

Оскільки аналогічні особливості можуть виникнути і при тестуванні деяких складених чисел, то необхідні додаткові умови, які є достатніми, щоб довести простоту числа, що тестується.

Подібні алгоритми називаються алгоритмами побудови доведено простих чисел.

Вказаний підхід передбачає, що при виборі великого випадкового числа існує можливість організувати в околі цього числа успішний пошук простих чисел. Така можливість забезпечується, наприклад, так званою **теоремою Дірихле**, яка стверджує, що в арифметичній прогресії виду

$$an + b, \quad n = 1, 2, ...,$$

де $(a, b) = 1$, існує нескінченно багато простих чисел.

Основою для переходу від ймовірнісних тестів до низки детермінованих тестів служить $(n-1)$-критерій Люка.

Відповідно до цього критерію, натуральне число n є простим у тому і тільки в тому випадку, якщо існує натуральне число a, що забезпечує виконання наступних умов для будь-якого нетривіального дільника q числа $n-1$:

$$a^{n-1} = 1(n),$$

$$\forall q \| (n-1) \;\; a^{(n-1)/q} \neq 1(n).$$

У **критерії Люка** не обов'язково розшукувати число a, що підходить для усіх q одночасно. Виявляється, що достатньо для кожного q вказати $a = a(q)$, проте вимога повної факторизації числа $n-1$ залишається у силі.

За допомогою теорем про вид простих дільників деяких типів цілих чисел можна обґрунтувати більш оптимальні тести, що використовують не усі, а лише частину дільників числа $n-1$.

Теорема Поклінгтона. Нехай

$$n = q^k R + 1 > 1,$$

де q — просте, що не ділить R і p — довільний простий дільник n. Якщо існує ціле a таке, що $a^{n-1} = 1(n)$ і НСД$(a^{(n-1)/q} - 1, n) = 1$, то кожний простий дільник p числа n має вигляд

$$p = q^k r + 1,$$

при деякому $r = r(p)$.

Важливе зауваження. Умова НСД$(a^{(n-1)/q} - 1, n) = 1$ є еквівалентною умові

$$\forall p \| n \quad a^{(n-1)/q} \neq 1(p).$$

Останній вираз є зручнішим для доведення теореми, проте, на відміну від першого, він не може бути безпосередньо перевіреним без знання p.

Доведення. Нехай p — простий дільник n. Тоді

$$a^{n-1} = 1(p)$$

і

$$a^{(n-1)/q} \neq 1(p).$$

Якщо m — порядок числа a за модулем p, то $n - 1 = md$, де d — ціле. Припустимо, що q ділить d. У цьому випадку

$$(n-1)/q = m(d/q),$$

де (d/q) — ціле, отже,

$$a^{(n-1)/q} = 1(p),$$

що є неможливим. Оскільки

$$n - 1 = md = q^k R,$$

то m ділиться на q^k. Проте m зобов'язане ділити число $p-1$. отже,

$$p = q^k r + 1$$

при деякому $r = r(p)$.

Теорема Поклінгтона дозволяє узагальнити критерій Люка на ситуацію, коли число $n-1$ факторизоване частково, скажемо, $n - 1 = FR$, де прості співмножники F відомі.

Теорема (узагальнення критерію Люка). Нехай $n = FR + 1 > 1$, де $1 < R < F$. Якщо для будь-якого простого дільника q числа F існує ціле $a = a(q)$, таке, що $a^{n-1} = 1(n)$ і НСД$(a^{(n-1)/q} - 1, n) = 1$, то число n — просте.

Проведемо доведення від протилежного. Нехай n складене, тоді існує його простий дільник p, такий, що $p \le \sqrt{n}$. Зафіксуємо $p \| F$. Нехай k максимальне число з умовою $q^k | F$, $k \ge 1$. Аналогічно, нехай q^h — максимальний степінь, що ділить FR.

Із умови теореми випливає, що $a^{n-1} = 1(p)$ і $a^{(n-1)/q} \ne 1(p)$. Нехай m — порядок числа a за модулем p, і $n - 1 = q^h R_1$. Як і при доведенні теореми Поклінгтона, одержимо, що число q^h ділить m. Отже, число $Q(q) = q^k$ ділить m.

Розглянемо число $b = b(q)$ виду $b = a^{m/Q}(p)$. Очевидно, $Q = Q(q)$ — порядок числа b за модулем p. Крім того, для дільників F $q_1 \ne q_2$, числа $Q(q_1)$ і $Q(q_2)$ взаємно прості.

Побудуємо для кожного $q \| F$ число $b(q)$. Добуток усіх таких чисел позначимо через B. Оскільки порядок числа B за модулем p дорівнює найменшому спільному кратному чисел $Q(q)$, то він дорівнює F. Але порядок будь-якого елемента за модулем p ділить $p - 1$, тому $F \le p - 1$. Отже,

$$p^2 \ge (F+1)^2 > R(F+1) > FR + 1 = n,$$

тобто $p > \sqrt{n}$, що неможливо.

Очевидно, що узагальнений критерій Люка можна використати для побудови детермінованого тесту на простоту.

Зауважимо, що, оскільки

$$n = FR + 1 > 1,$$

нерівність $1 < R < F$ виконується при $F > \sqrt{n}$.

Тому факторизацію числа $n - 1$ та перевірку умов теореми при тестуванні слід проводити лише до тих пір, поки $F \le \sqrt{n}$.

3.14 Детерміновані тести перевірки чисел на простоту. Теорема Димитко

Теорема Димитко дозволяє побудувати детермінований тест, оснований на перевірці умови

$$a^{(n-1)/q} \neq 1(n),$$

замість умови НСД$(a^{(n-1)/q}-1, n) = 1$, що використовується в узагальненому критерії Люка. Крім того, виходячи з теореми Димитко, можна обґрунтувати процедуру побудови псевдовипадкових доказово простих чисел.

Лема. Нехай

$$n = q^k R + 1 > 1,$$

де q — просте, що не ділить R. Якщо існує ціле a таке, що

$$a^{n-1} = 1(n)$$

і

$$a^{(n-1)/q} \neq 1(n),$$

то існує простий дільник p числа n виду

$$p = q^k r + 1,$$

при деякому $r = r(p)$.

Доведення. Нехай

$$n = \Pi_{i=1}^{k} p_i^{m_i}.$$

Оскільки

$$a^{(n-1)/q} \neq 1(n),$$

то не всі дільники n ділять $a^{(n-1)/q} - 1$. Тому існує i:

$$a^{n-1} = 1(p_i^{m_i}),$$

але

$$a^{(n-1)/q} \neq 1(p_i^{m_i}).$$

Отже, порядок t елемента a за модулем $p_i^{m_i}$ ділить $n-1$ і не ділить $(n-1)/q$. Тому $q^k|t$.

Відомо, що група лишків, оборотних за модулем $p_i^{m_i}$, має первісний елемент (циклічна). Її порядок дорівнює

$$\varphi(p_i^{m_i}) = p_i^{m_i-1}(p_i - 1).$$

Цей порядок має ділитися на t і, як наслідок, на q^k. Оскільки q ділить $n-1$, а p_i ділить n, то q і p_i взаємно прості. Тому

$$q^k|(p_i - 1),$$

тобто

$$p = q^k r + 1.$$

Теорема Димитко. Нехай

$$n = qR + 1 > 1,$$

де q — просте, R — парне і

$$R < 4(q+1).$$

Якщо існує ціле a таке, що

$$a^{n-1} = 1(n)$$

і

$$a^{(n-1)/q} \neq 1(n),$$

то число n — просте.

Доведення. Припустимо, що

$$n = \prod_{i=1}^{k} p_i^{m_i}, \quad k > 1.$$

За умовою,

$$n = q^h R_1 + 1,$$

де $h \geq 1$ і q не ділить R_1. Лема доводить, що існує таке таке i, для якого $q|(p_i - 1)$. Таким чином, $n = 1(q)$ і $p_i = 1(q)$.

Запишемо n у вигляді $n = p_i u$. Очевидно, $u = 1(q)$, тому, $u = 1 + Kq$ і $p_i = 1 + Sq$.

Зауважимо, що $K, S \geq 2$. Дійсно, n — непарне, оскільки за умовою R — парне число. Якщо $K = 0$, то n — просте, що за припущенням є невірним. Якщо $K = 1$, то n — парне, оскільки u парне.

Якщо $S = 0$, то $p_i = 1$, що суперечить припущенню. Якщо $S = 1$, p_i — парне, що також є неможливим. Отже, $u \geq 2q + 1$, $p_i \geq 2q + 1$, і як наслідок,

$$n = p_i u \geq (2q + 1)^2 = 4q(q + 1) + 1 > qR + 1 = n$$

— протиріччя, що знімається тільки за умови, що n — просте.

Теорема Димитко дозволяє будувати великі доказово прості числа. Нехай задане деяке число q, про яке відомо, що воно просте. Виберемо R — парне число, розрядність якого дорівнює розрядності q. У цьому випадку, очевидно,

$$R < 4(q + 1).$$

Побудуємо

$$n = qR + 1.$$

Якщо існує ціле a, таке, що

$$a^{n-1} = 1(n)$$

і

$$a^{(n-1)/q} \neq 1(n),$$

то число n — просте за теоремою Димитко. Розрядність n у два рази більша за розрядність числа q.

Якщо тепер за q прийняти просте число n, то можемо побудувати наступне просте число удвічі більшої розрядності, ніж початкове і т.д.

3.15 Основні умови вибору параметрів криптосистеми RSA

Нехай задана **криптосистема RSA** з параметрами (e, d, n), $n = pq$.

Коректність параметрів зв'язана з оцінкою стійкості системи і може бути визначена лише з точки зору практичної стійкості. Отже, коректні параметри повинні бути побудовані так, щоб мінімізувати збитки від відомих підходів до послаблення криптосистеми.

Слід ураховувати, що слабкість одного з параметрів практично не компенсується підсиленням властивостей інших параметрів.

Очевидно, що число $n = pq$ повинно бути великим.

Числа p, q не повинні міститися в списках відомих великих простих чисел, не повинні бути дуже близькими один до іншого, або суттєво розрізнятися за величиною. Вони не повинні будуватися за детермінованими алгоритмами з невеликим числом відомих варіантів початкових параметрів або мати закономірності у двійковій формі представлення.

У загальному випадку p, q, e і d не повинні відрізнятися від типових представників випадкових чисел.

Для будь-якого a, що взаємно просте з n, $ord_p a$ ділить $p-1$, а $ord_q a$ ділить $q-1$. Тому $ord_n a$ ділить $G = \text{НСК}(p-1, q-1)$. Отже, для побудови криптосистеми, замість побудови d з порівняння $ed = 1(\varphi(n))$, можна скористатися розв'язком порівняння $ed_1 = 1(G)$.

Нехай $g = \text{НСД}(p-1, q-1)$. Тоді $Gg = \varphi(n)$. Очевидно, що із співвідношення $ed = 1(\varphi(n))$ випливає $ed = 1(G)$, тому $d = d_1(G)$ і $d \neq d_1(\varphi(n))$. Цим умовам задовольняють ключі

$$d_1, d_1 + G, d_1 + 2G, ..., d_1 + (g-1)G,$$

що є криптоеквівалентними, таким чином, ключу d.

Отже, чим більший $\text{НСД}(p-1, q-1)$, тим більше **криптоеквівалентних ключів**, тим гірше для криптосистеми.

Для практики достатньо, щоб існував великий простий дільник числа $p-1$ виду $r = (p-1)/2j$. Щоб задовольнити цій умові, а також виключити можливість застосування так званих ($p \pm 1$ — методів факторизації, необхідно вимагати, щоб числа

$$p_1 = (p-1)/2, \;\; p_2 = (p+1)/2, \;\; q_1 = (q-1)/2, \;\; q_2 = (q+1)/2$$

не розкладалися у добуток степенів невеликих простих чисел. Ін-

шими словами, необхідно, щоб вони містили в розкладі велике просте число.

Подібні вимоги, сформульовані Р. Рівестом у найбільш сильній формі, полягають у тому, щоб числа p_1, p_2, q_1, q_2 були простими, причому у розкладі як $p_1 - 1$, так і $q_1 - 1$ містилося велике просте число.

Таким чином, необхідно виділити деякий специфічний клас простих чисел.

Визначення. Просте число p називається сильно простим, якщо виконуються умови:

$$p \equiv 1 \pmod{r}, \quad p \equiv -1 \pmod{s}, \quad r \equiv 1 \pmod{t},$$

де r, s, t — великі прості числа.

Оскільки числа p, r, s, t — непарні, то вони представляються у вигляді

$$p = 1 + 2jr, \quad p = -1 + 2ks, \quad r = 1 + 2lt.$$

Для наших цілей, чим менші числа j, k, l, тим краще.

Існує так званий метод Гордона для побудови великих сильно простих чисел. Зазначимо, що при реалізації методу, машинний алгоритм потребує відстеження низки особливих ситуацій. Це пов'язано з тим, що в методі неодноразово використовуються ймовірностні процедури побудови проміжних даних, а також застосовується тестування чисел на простоту. Дані процедури працюють тим краще, чим більша розрядність чисел, що використовуються в обчисленням.

Метод Гордона для побудови сильно простого числа p полягає у наступному.

1. Будуємо випадкове просте число s, виходячи із заздалегідь вибраної для нього розрядності. Для цього вибираємо псевдовипадкове число x із розрядністю, що дорівнює розрядності s і за допомогою методу пробного ділення залишаємо на проміжку $[x, x+\log_2 x]$ числа, що не мають малих дільників. Серед чисел, що залишилися, за допомогою тестів на простоту визначаємо просте число s.

2. Будуємо випадкове число t, аналогічно до побудови числа s.

3. За допомогою методу пробного ділення та тестів на простоту, аналогічно п.1, будуємо просте число $r = 1 + 2lt$, знаходячи l у проміжку $[1, \log_2 t]$ перебором.

4. Обчислюємо

$$u = u(r, s) = (s^{r-1} - r^{s-1}) \bmod rs.$$

Зазначимо, що це зручно зробити за допомогою китайської теореми про залишки, оскільки $u = 1(r)$ і $u = -1(s)$. Крім того, $u = p = 1(\mathrm{mod} r)$, $u = p = -1(\mathrm{mod} s)$.

5. Якщо число u — непарне, то призначаємо $p_0 = u$, у протилежному випадку — $p_0 = u + rs$.

6. Будуємо p — найближче просте число, яке порівняне з непарним числом p_0 за модулем rs, тобто тестуємо на простоту числа виду

$$p = p_0 + 2krs, \quad k = 0, 1, ...,$$

поки не знайдеться просте число (або спрацюють обмеження реалізації).

Приклад побудови сильно простого числа.

1. Будуємо випадкове просте число s, розміром, скажімо, у 6 бітів. Вибираємо псевдовипадковим чином $x = 46$. У проміжку $[46, 46 + 5]$ визначаємо просте число $s = 47$.

2. Будуємо випадкове просте число t, аналогічно до побудови числа s. Нехай $x = 25$. У проміжку $[25, 25 + 4]$ визначаємо просте число $t = 29$.

3. Будуємо просте число $r = 1 + 2lt$, вибираючи l у проміжку $[1, 4]$. Одержуємо $r = 59$.

4. Обчислюємо $u(r, s)$, розв'язуючи за допомогою китайської теореми про лишки систему: $u = 1(r)$, $u = -1(s)$.

За допомогою розширеного **алгоритму Евкліда** одержуємо співвідношення $4 \cdot 59 - 5 \cdot 47 = 1$, звідки: $59^{-1} \bmod 47 = 4$, $47^{-1} \bmod 59 = -5$.

Отже,

$$u(r, s) = 1 \cdot 47 \cdot 47^{-1} \bmod 59 + (-1) \cdot 59 \cdot 59^{-1} \bmod 47 = -471 = 2302(2773).$$

5. Число $u(r, s)$ парне, тому $p_0 = 2302 + 59 \cdot 47 = 5075$.

6. Будуємо просте число, порівняне з p_0 за модулем 2773, тестуючи на простоту числа виду

$$p = p_0 + 2 \cdot 2773 \cdot k.$$

При $k = 0, 1, 2, 3$ одержуємо відповідно: 5075, 10621, 11167, 21713. Лише останнє число є простим.

3.16 Загальні відомості про криптосистеми закордонного виробництва

Використання в Україні систем криптографічного захисту інформації, розроблених за кордоном, є наслідком широкого розповсюдження обчислювальної техніки та операційних систем закордонного виробництва. Найбільш часто пропонуються програмні **засоби криптографічного захисту інформації** (КЗІ).

У цілому, ринок закордонних криптозасобів дуже широкий: від криптосистем індивідуального використання до криптосистем воєнного призначення.

Порядок придбання та використання криптозасобів регулюється національним законодавством та міжнародними угодами.

Засоби КЗІ реалізуються апаратними, апаратно-програмними та програмними методами. Найбільш надійними криптосистемами є системи, засновані на апаратних засобах КЗІ. Апаратно-програмні та програмні засоби, з точки зору криптографії, переваг перед апаратними засобами КЗІ не мають.

Апаратні засоби дозволяють:

- реалізувати лише необхідні функції апаратури;
- максимально підвищити швидкість оброблення даних;
- забезпечити належний захист від побічних електромагнітних випромінювань та наведень;
- реалізувати вимоги з міцності щодо виробу;
- забезпечити заходи захисту від несанкціонованого доступу до вузлів апаратури, ключів та постійної інформації, що зберігається в електронних модулях;
- використати модульний принцип компонування криптозасобів, що дозволяє легко усувати несправності, здійснювати заміну

ключів, модифікацію криптосхем, забезпечувати сумісність з різними засобами зв'язку.

- виготовляти окремі екземпляри апаратури за індивідуальним замовленням.

При апаратній реалізації для шифрування використовуються як блокові, так і потокові шифри. Апаратні засоби шифрування часто називають шифраторами.

На ринку достатньо розповсюджені шифратори, призначені для організації **змішаних** (гібридних) **криптосистем**, що використовують для шифрування гамування за модулем два, а для розповсюдження ключів і організації зв'язку — асиметричне шифрування та криптопротоколи.

Залежно від прийнятої системи передачі інформації, існують шифратори попереднього шифрування та канальні **шифратори**.

При попередньому шифруванні повідомлення зашифровується повністю. Передавання його абоненту здійснюється або відразу після зашифрування, або може бути відкладеним на деякий термін.

Канальні шифратори використовуються для організації постійної роботи системи передавання інформації в захищеному режимі. Канал є захищеним, навіть якщо в ньому відсутня інформація. Дані шифруються та відправляються абоненту поелементно, по мірі їх появи.

Шифратори, крім того, поділяються на два типи за способом генерації гами.

Шифратори з внутрішнім носієм шифру генерують гаму в процесі шифрування самі, залежно від ключів.

Шифратори, що використовують послідовність гами, заготовлену заздалегідь іншими засобами, називаються змішувачами. Подібна гама іноді називається зовнішньою. Ключі змішувача вказують, який конкретно відрізок зовнішньої гами слід використати в даний момент.

Як правило, шифратори є інтелектуальними пристроями, які дозволяють вибирати конфігурацію системи секретного зв'язку, адаптуватися до різноманітних систем передачі інформації, вибирати засоби автоматичного форматування документів, а також забезпечувати виконання великої кількості інших сервісних та допоміжних функцій.

Ключі в шифраторах до початку шифрування завжди піддаються додатковим необернениим перетворенням.

Множина ключових елементів, порядок їх використання і закон формування ключів з ключових елементів складають та звану ключову систему шифру.

У **потокових шифрах** на теперішній час розповсюджені трирівневі та дворівневі ключові системи. Для трирівневої системи існують три види ключів: мережний, довготстроковий та сеансовий. Для дворівневої — **мережний ключ** відсутній. Мережний ключ є ключовим елементом, термін дії якого може бути необмеженим. Він заноситься при виготовлені конкретної партії пристроїв для мережі зв'язку. **Довгостроковий ключ** — це ключ, що діє протягом тривалого проміжку часу та змінюється, як правило, періодично.

Сеансовий ключ діє значно більш короткий інтервал часу, ніж довгостроковий. Звичайно один сеансовий ключ використовується на один сеанс зв'язку, тобто на групу повідомлень.

У випадку якщо на кожне повідомлення створюється один сеансовий ключ, він називається **разовим ключом**.

На теперішній час сеансові та разові ключі найчастіше співпадають. Сумарна довжина ключових елементів в потокових шифрах складає порядку 128-512 і більше бітів.

Додаток А
КОНТРОЛЬНІ ТЕСТИ

А.1 Контрольні тести до розділу 1

1) Що є основою побудови систем криптографічного захисту інформації (КЗІ)?

1. Складні алгоритми обробки та перетворення даних.
2. Методи приховування факту пересилки повідомлень.
3. Математичні перетворення з використанням секретних параметрів.

2) Що становить основну проблему криптології?

1. Необхідність регулярної модифікації засобів криптографічного захисту інформації.
2. Відсутність формальних критеріїв якості систем КЗІ.
3. Впровадження іноземних засобів КЗІ зі свідомо внесеними слабкостям.

3) Назвіть основні причини потенційної ненадійності систем КЗІ:

1. Відсутність формальних критеріїв якості систем КЗІ .
2. Неможливість виконання у повному обсязі умов, виходячи з яких обгрунтовується якість систем КЗІ.
3. Внаслідок масового застосування засобів КЗІ, проявляються малоймовірні ситуацій, коли якість криптоалгоритмів знижується.
4. Можливість впровадження засобів КЗІ зі свідомо внесеними слабкостями.

4) Що вивчає криптография?

1. Математичні методи перетворення інформації, що використовуються для приховування смислу даних, а також для захисту даних від несанкціонованого використання або підробки.
2. Методи обчислювальної математики, що прискорюють виконання арифметичних операцій.
3. Системи завадостійкого кодування для передачі інформації лініями зв'язку.

5) Кого називають криптоаналітиком?

1. Спеціаліста з криптології, який розробляє методику послаблення систем КЗІ у загальних та часткових випадках при невідомих секретних параметрах.

2. Спеціаліста з комп'ютерних технологій, який здійснює віддалений доступ до файлів даних, що містять секретні параметри.
3. Спеціаліста з технічного захисту інформації, що розробляє методику несанкціонованого доступу до інформації з використанням побічних електромагнітних випромінювань.

6) Що таке шифрування?

1. Перетворення повідомлення з метою приховування смислу даних від сторонніх осіб.
2. Перетворення повідомлення, що не дає змогу з'ясувати смисл даних сторонніми особами.
3. Взаємно однозначне перетворення повідомлення із застосуванням секретних параметрів з метою приховування смислу даних від сторонніх осіб.
4. Взаємно однозначне перетворення повідомлення з метою приховування смислу даних від сторонніх осіб.

7) Що таке розшифрування?

1. Операція зворотна до зашифрування.
2. Операція зворотна до зашифрування, що здійснюється при наявності секретних параметрів.
3. Процес відновлення повідомлення, виходячи з результату зашифрування.

8) Дайте найбільш повне визначення ключа:

1. Секретний параметр, що обов'язково використовується при розшифруванні та зашифруванні.
2. Секретний параметр, що використовується виключно при розшифруванні.
3. Секретний параметр, що використовується при розшифруванні, але при зашифруванні використовується не завжди.

9) Як називається вхідний текст повідомлення, який безпосередньо підлягає шифруванню?

1. Первинний текст.
2. Секретний текст.
3. Відкритий текст.

10) Що таке шифротекст?

1. Текст, призначений для шифрування.
2. Текст, призначений для розшифрування.
3. Результат зашифрування деякого відкритого тексту вказаною криптосистемою.

11) Що таке криптограма?

1. Шифротекст деякого повідомлення.
2. Шифротекст, оформлений за правилами передачі повідомлень відповідними лініями зв'язку.
3. Результат роботи алгоритму шифрування у вигляді двійкового файлу.

12) Що таке дешифрування криптограми?

1. Розшифрування шифротексту криптограми зловмисником.
2. Процес відновлення повідомлення аналітичним методом, виходячи з шифротексту без заздалегідь відомих ключів.
3. Відновлення відкритого повідомлення за рахунок доступу до відповідного файлу в оперативній пам'яті комп'ютера.

13) Назвіть основні положення моделі системи секретного зв'язку К.Шеннона:

1. Супротивник може перехопити ключ.
2. Супротивникові відомий алгоритм шифрування.
3. Супротивник не може перехопити ключ.
4. Супротивникові не відомий алгоритм шифрування.
5. На кожне повідомлення незалежно та рівноймовірно вибирається свій ключ шифрування.
6. В моделі надано та обгрунтовано безпечний механізм формування та розподілу ключів.
7. В моделі К. Шеннона ключі використовуються для здійснення зашифрування та розшифрування.
8. Для організації лінії шифрованого зв'язку кожний з абонентів має знати відповідні ключі.

14) Що таке практична стійкість шифрперетворення?

1. Час потрібний зловмиснику для розшифрування шифротексту криптограми.
2. Трудомісткість одержання відкритого тексту без знання ключа аналітичним способом, з використанням найкращого відомого на даний час алгоритму.
3. Час потрібний для перебору ключа з використанням самого потужного комп'ютера.

15) Що таке односпрямована (важкооборотна, однобічна) функція з лазівкою?

1. Вектор-функция з секретним параметром, що є точкою її екстремуму.
2. Функція, обчислення якої не є складним, але обчислення значення оберненої до неї функції обчислювально неможливе без знання додаткової інформації, яка називається лазівкою.

3. Функція, що реалізує стійке шифрперетворення з секретним ключем.

16) Назвіть основні властивості асиметричної криптосистеми:

1. Асиметричні криптосистеми побудовані на односпрямованих функціях.
2. Асиметрична криптосистема передбачає застосування секретного параметра (ключа), спільного для двох або декількох абонентів мережі зв'язку.
3. В асиметричній криптосистемі секретний ключ для зашифрування не використовується.
4. В асиметричній криптосистемі секретний ключ для розшифрування не використовується.
5. В асиметричній криптосистемі для зашифрування використовується несекретний параметр, який називається відкритим ключем.
6. В асиметричній криптосистемі секретний ключ відомий лише одержувачу повідомлень.

17) Що таке шифр простої заміни?

1. Шифр, при якому кожний знак вхідного алфавіту замінюється на деякій знак із того ж алфавіту.
2. Шифр, при якому кожний знак вхідного алфавіту взаємно однозначно замінюється на знак із довільного фіксованого алфавіту.
3. Шифр, при якому кожний знак вхідного алфавіту взаємно однозначно замінюється на деякій знак із того ж алфавіту.

18) Що таке шифр перестановки?

1. Шифр, при якому кожний знак відкритого тексту переходить на місце іншого знаку того ж тексту.
2. Шифр, при якому кожний знак відкритого тексту або залишається на місті, або переходить на місце іншого знаку того ж тексту.
3. Шифр, при якому знаки відкритого тексту переставляються між собою, причому однакові знаки переходять в однакові.

19) Що таке ключовий потік?

1. Послідовність номерів шифроперетворень, що вибираються під час шифрування на відповідних тактах.
2. Двійкова послідовність, що застосовується в якості джерела ключів для симетричної криптосистеми.

20) Назвіть основні типи шифрів:

1. Шифр заміни.
2. Шифр перестановки.
3. Потоковий шифр.

4. Блоковий шифр.

21) Назвіть основні властивості потокового шифру:

1. Потоковим шифром називається шифр, в якому на кожному такті використовується змінний алгоритм шифрування, що вибирається за допомогою елементів ключового потоку зі списку шифроперетворень.
2. У загальному випадку ключовий потік визначається ключовими даними шифру.
3. Ключовий потік визначається ключовими даними та номерами тактів шифрування, включно до того, що розглядається.

22) Назвіть основні властивості блокового шифру:

1. Блоковий шифр - це шифр простої заміни надвеликого алфавіту.
2. Блоковим шифром називається шифр, в якому на кожному такті використовується постійний алгоритм шифрування, що вибирається залежно від ключів до початку шифрування.
3. Блоковий шифр можна інтерпретувати як сукупність віртуальних таблиць заміни, з якої конкретна таблиця вибирається за допомогою ключа.

23) Назвіть основні властивості найбільшого спільного дільника: $d = (a, b)$ двох цілих чисел:

1. Найбільший спільний дільник $d = (a, b)$ це ціле число що ділить без залишку як a так і b.
2. Найбільший спільний дільник $d = (a, b)$ це найбільше ціле число що ділить без залишку як a так і b.
3. Найбільший спільний дільник $d = (a, b)$ можна записати у вигляді так званого діофантового рівняння виду $xa + yb = d$, де числа x, y — цілі.
4. Діофантове рівняння виду $xa + yb = d$ можна розв'язати за допомогою методів лінійної алгебри.
5. Діофантове рівняння виду $xa + yb = d$ можна розв'язати за допомогою розширеного алгоритму Евкліда.

24) Назвіть основні властивості порівняння за модулем та елемента, оборотного за модулем:

1. Цілі числа a і b порівняні за натуральним модулем m, якщо $a = bm$.
2. Цілі числа a і b порівняні за натуральним модулем m, якщо $a - b$ ділиться націло на m.
3. відношення порівняння записується у вигляді $a \,(\mathrm{mod} m) = b \,(\mathrm{mod} m)$.
4. Відношення порівняння записується у вигляді $a = b \,(\mathrm{mod} m)$, або $a = b \,(m)$.

5. Зворотний елемент до a за модулем m завжди існує: це дріб вигляду $1/a \bmod m$.
6. Зворотний елемент до a за модулем m існує тоді і тільки тоді, коли $d = (a, m) = 1$.
7. Зворотний елемент до a за модулем m є значенням x із розв'язку діофантового рівняння $xa + ym = 1$.
8. Зворотним елементом до a за модулем m є такий елемент b, що $ab = 1 \,(\mathrm{mod} m)$.

25) Укажіть вірні твердження щодо поняття порядку числа a за модулем m:

1. Це — кількість розрядів у двійковому записі значення $a \,(\mathrm{mod} m)$.
2. Порядок числа a за модулем m записується у вигляді $d = ord_m a$.
3. Це — мінімальне число d, таке, що $a^d = 1 \,(\mathrm{mod} m)$.
4. Порядок числа a за модулем m записується у вигляді $d = ord_a m$.
5. Це — мінімальне натуральне число d, таке, що $a^d = 1 \,(\mathrm{mod} m)$.
6. Для порядку числа a за простим модулем p часто застосовується назва "індекс числа за простим модулем" і використовується позначення $d = ind_p a$.

26) Визначення функції Ейлера $\varphi(m)$ натурального числа m:

1. Кількість простих чисел у послідовності $1, 2, \ldots, m-1$.
2. Кількість чисел у послідовності $1, 2, \ldots, m-1$, взаємно простих з m.
3. Кількість чисел у послідовності $1, 2, \ldots, m$, взаємно простих з m.

27) Назвіть властивості, яким задовольняє функція Ейлера:

1. $\varphi(ab) = \varphi(a)\,\varphi(b)$.
2. $\varphi(1) = 0$.
3. $\varphi(ab) = \varphi(a)\,\varphi(b)$, якщо $(a, b) = 1$.
4. Якщо $m = p_1^a p_2^b \ldots p_t^s$, то $\varphi(m) = p_1^{a-1} p_2^{b-1} \ldots p_t^{s-1} (p_1 - 1)(p_2 - 1) \ldots (p_t - 1)$, де p_i — прості числа, $p_i \neq p_j \,(i \neq j)$.
5. $a^{\varphi(m)} = 1 \,(\mathrm{mod} m)$, якщо $(a, b) = 1$.
6. Порядок довільного числа за модулем m ділить $\varphi(m)$.

28) Назвіть визначення та властивості яким задовольняє первісний елемент за простим модулем p:

1. Число (елемент) a називається первісним елементом за модулем p, якщо $ord_p a = \varphi(p)$.
2. Елемент a називається первісним елементом за модулем простого числа p, якщо $ord_p a = p - 1$.

3. Елемент $a \neq 0$ є первісним елементом за модулем простого числа p тоді і тільки тоді, якщо $\forall_i\ a^{(p-1)/p_i} \neq 1\,(\mathrm{mod} p)$, де $p-1 = \prod_{i=1}^{k} p_i^{a_i}$.
4. Елемент a є первісним елементом за модулем простого числа p тоді і тільки тоді, якщо $a^{(p-1)/2} = -1\,(\mathrm{mod} p)$.

29) Укажіть властивості порівнянь з одним невідомим:

1. Порівняння $ax = b\,(\mathrm{mod} m)$ має розв'язок, тоді і тільки тоді, коли існує $a^{-1}\,(\mathrm{mod} m)$.
2. Порівняння $ax = b\,(\mathrm{mod} m)$ може мати декілька розв'язків.
3. Порівняння $ax = b\,(\mathrm{mod} m)$ має розв'язок, тоді і тільки тоді, коли число $d = (a, m)$ ділить b.
4. Кількість коренів многочлена з коефіцієнтами за простим модулем p, які є лишками за модулем p, не перевищує степеня многочлена.
5. Кількість коренів многочлена з коефіцієнтами за простим модулем p, що є лишками за модулем p, дорівнює степеню многочлена.
6. Розв'язність порівняння $x^n = a\,(\mathrm{mod} p)$ за простим модулем p еквівалентна умові $a^{(p-1)/d} = 1\,(\mathrm{mod} p)$, $d = (n, p-1)$, $(a, p) = 1$.

30) Як обчислюється модуль в криптосистемі RSA?

1. У вигляді $n = pq$, $(p, q) = 1$.
2. У вигляді $n = pq$, де p і q — надвеликі прості числа.
3. У вигляді $n = pq$, де p і q — надвеликі прості числа, що мають практично однакову довжину двійкового запису.
4. У вигляді $n = pq$, де p і q — нерівні надвеликі прості числа, що мають практично однакову довжину двійкового запису.

31) Як можна вибрати відкритий ключ (e, n), для криптосистеми RSA?

1. e — додатне псевдовипадкове число, що не перевищує n.
2. e — додатнє надвелике псевдовипадкове число, що не перевищує n, за умови $(e, \varphi(n)) = 1$.
3. e — довільне надвелике додатнє число, що не перевищує n, за умови $(e, \varphi(n)) = 1$.

32) Як можна побудувати секретний (приватний) ключ d, для криптосистеми RSA?

1. d — додатне псевдовипадкове число, що не перевищує n.
2. d є розв'язком порівняння $ed = 1\,(\mathrm{mod} n)$.
3. d є розв'язком порівняння $ed = 1\,(\mathrm{mod} \varphi(n))$.

33) Як надійно організувати криптосистему RSA?

1. Побудувати відкритий та секретний ключі, зробити їх загальнодоступними.
2. Побудувати відкритий та секретний ключі, зробити відкритий ключ загальнодоступним, надати секретний ключ абонентам мережі зв'язку встановленим чином.
3. Побудувати відкритий та секретний ключі, зробити відкритий ключ загальнодоступним.
4. Побудувати відкритий та секретний ключі, зробити відкритий ключ загальнодоступним, знищити $p, q, \varphi(n)$ та результати проміжних обчислень.

34) Чи можна при побудові криптосистеми RSA замість функції $\varphi(n)$ використовувати найменше спільне кратне чисел $p-1$ і $q-1$?

1. Так.
2. Ні.

35) Як здійснюється зашифрування повідомлення в криптосистемі RSA?

1. $c = m^d \,(\mathrm{mod} n)$.
2. $c = md \,(\mathrm{mod} n)$.
3. $c = m^e \,(\mathrm{mod} n)$.

36) Як здійснюється розшифрування повідомлення в криптосистемі RSA?

1. $m = c^d \,(\mathrm{mod} n)$.
2. $m = cd^{-1} \,(\mathrm{mod} n)$.
3. $m = c^e \,(\mathrm{mod} n)$.

37) Укажіть область визначення та область значень геш-функції:

1. Геш-функція це перетворення, що дає на виході блок фіксованої довжини.
2. Геш-функція це перетворення з секретним ключам, що має на вході та виході блоки фіксованої довжини.
3. Геш-функція це перетворення двійкових рядків довільної довжини у двійкові блоки фіксованого розміру.

38) Із наступних трьох властивостей геш-функції $z = h(m)$ повідомлення m назвіть таку, що за умови виконання двох інших, можна не вимагати:

1. Відновлення m, виходячи зі значення $z = h(m)$, обчислювально неможливо.
2. Обчислювально неможливо, виходячи з m і $z = h(m)$ знайти повідомлення $m_1 \neq m$, щоб виконувалася рівність $h(m_1) = h(m)$.
3. Обчислювально неможливо знайти пару повідомлень $x \neq y$, для яких виконується рівність $h(x) = h(y)$.

39) Як визначається поняття дискретного логарифму в криптографії?

1. Це показник x порівняння $b = a^x \,(\mathrm{mod} n)$.
2. Це показник x порівняння $b = a^x \,(\mathrm{mod} p)$, де p — просте число, $a, b \neq 0 \,(\mathrm{mod} p)$.
3. Це показник x порівняння $b = a^x \,(\mathrm{mod} p)$, де p — просте число, a — первісний корень за модулем p, $b \neq 0 \,(\mathrm{mod} p)$.
4. Це показник x порівняння $b = a^x \,(\mathrm{mod} p)$, де p — просте число, a — первісний корень за модулем p, $b \neq 0 \,(\mathrm{mod} p)$, $0 \leq x < p - 1$.

40) Цифровий підпис повідомлення на основі RSA це:

1. Перетворене за допомогою відкритого ключа повідомлення m.
2. Блок даних, що формується за допомогою відкритого ключа та передається разом із повідомленням m.
3. Блок даних виду $s = h\,(m)^d \,(\mathrm{mod} n)$, що передається разом із повідомленням m, де $h\,(m)$ — геш-функція, а d — секретний ключ.

41) Що таке змішана криптосистема?

1. Криптосистема, в який використовуються два криптоалгоритми, у такий спосіб, що після зашифрування першим криптоалгоритмом результат перешифровується другим криптоалгоритмом.
2. Криптосистема, що побудована з асиметричної криптосистеми, відкритий ключ якої зроблено секретним.
3. Криптосистема, в якій для шифрування повідомлень використовується симетрична криптосистема, а для розповсюдження ключів — криптосистема з відкритим ключем.

42) Що таке ключова інформація?

1. Сукупність усіх діючих у криптосистемі ключів.
2. Сукупність інструкцій з обліку та використання ключів.

43) Що таке управління ключами?

1. Сукупність адміністративних заходів, щодо забезпечення секретності ключової інформації.
2. Система обробки і передачі інформації, що включає генерацію, зберігання і розподіл ключів.

44) Що таке розподіл ключів?

1. Розповсюдження ключів безпечним способом.
2. Призначення ключів та їх безпечна доставка призначеним абонентам.
3. Оперативна та вчасна доставка ключів.

45) Поняття транспортування ключів полягає:

1. У перевезенні ключів дипломатичною поштою.

2. У передаванні ключів у зашифрованому виді.

46) Поняття узгодження ключів використовується для визначення:

1. Списку ключів, спільного для абонентів лінії зв'язку, який складається заздалегідь та утримується в секреті.
2. Процесу синхронного виготовлення абонентами спільних ключів із псевдовипадкових секретних даних, сформованих перед початком сеансу шифрування.
3. Документу, який містить список ключів та порядок їх застосування конкретними абонентами.

A.2 Контрольні тести до розділу 2

1) Який режим роботи визначений у стандарті ГОСТ 28147-89 як основний?

1. Режим гамування.
2. Режим простої заміни.
3. Режим створення імітовставки.

2) До якого з основних типів шифрів відноситься режим простої заміни криптоалгоритму ГОСТ?

1. Блоковий шифр.
2. Потоковий шифр.

3) До якого типу елементарних шифрів відносяться шифроперетворення в режимах криптоалгоритму ГОСТ, що призначені для шифрування повідомлень?

1. До шифрів простої заміни з потужністю абетки 2^{32}.
2. До шифрів простої заміни з потужністю абетки 2^{256}.
3. До шифрів гамування з розміром блоку гами, що дорівнює 64-біта.
4. До шифрів гамування з розміром блоку гами, що дорівнює 32-біта.
5. До множини шифрів перестановки потужності 64!.

4) Ключова система криптоалгоритму ГОСТ складається з:

1. Мережного та сеансового ключів змінної довжини.
2. Мережного ключа S довжиною 512 бітів, довгострокового ключа K довжиною 256 бітів та сеансового ключа X довжиною 64 біта.
3. Довгострокового ключа K довжиною 512 та сеансового ключа X довжиною 64 біта.
4. Довгострокового ключа K довжиною 512 та сеансового ключа X довжиною 256 бітів.

5. Довгострокового ключа K довжиною 256 та сеансового X ключа довжиною 64 біта.
6. Мережного ключа S довжиною 64 біта, довгострокового ключа K довжиною 256 бітів та сеансового ключа X довжиною 64 біта.

5) Що таке синхропосилка у криптоалгоритмі ГОСТ?

1. Послідовність S із 64-х бітів, що задає дату-час формування криптограми для синхронізації сеансових ключів.
2. Псевдовипадковий блок S із 64-х бітів, призначений для синхронізації ключового потоку.
3. Псевдовипадковий блок S із 64-х бітів, що є параметром ітеративних перетворень в процесі шифрування.

6) Укажіть правильну структуру та призначення довгострокового ключа (блоку підстановки) K криптоалгоритму ГОСТ:

1. Ключ K реалізує потетрадну заміну 32-розрядних блоків на 32-розрядні за допомогою восьми вузлів тетрадної заміни.
2. Ключ K реалізує заміну 64-розрядних блоків на 32-розрядні за допомогою восьми вузлів тетрадної заміни.

7) Укажіть правильну структуру сеансового ключа X криптоалгоритму ГОСТ:

1. Ключ X складається з восьми підключів та реалізує потетрадну заміну 32-розрядних блоків на 32-розрядні.
2. Ключ X складається з конкатенації восьми підключів, які використовуються на восьми ітераціях режиму простої заміни.
3. Ключ X складається з конкатенації восьми підключів, які використовуються на тридцяти двох ітераціях режиму простої заміни.

8) Послідовності вибору підключів у криптоалгоритмі ГОСТ при зашифруванні та розшифруванні:

1. Співпадають.
2. Співпадають при записі у зворотному порядку.
3. Співпадають, за винятком останньої ітерації.

9) На проміжній ітерації криптоалгоритму ГОСТ послідовність перетворення вхідного блоку (L,R) у вихідний режиму простої заміни наступна:

1. Підблок R та підключ порозрядно додаються за модулем 2, сума перетворюється за допомогою блоку підстановки K, результат підстановки, попередньо зсунутий циклічно вліво на 11 розрядів, порозрядно за модулем 2 додається до підблоку L, у результаті чого виникає підблок R1, який разом з R утворює вихідний блок ітерації (R,R1).

2. Підблок R та підключ порозрядно додаються за модулем 2, сума перетворюється за допомогою блоку підстановки K, результат підстановки, попередньо зсунутий циклічно вліво на 11 розрядів, додається за модулем 2^{32} до підблоку L, у результаті чого виникає підблок R1, який разом з R утворює вихідний блок ітерації (R,R1).
3. Підблок R та підключ додаються за модулем 2^{32} , сума перетворюється за допомогою блоку підстановки K, результат підстановки, попередньо зсунутий циклічно вліво на 11 розрядів, порозрядно за модулем 2 додається до підблоку L, у результаті чого виникає підблок R1, який разом з R утворює вихідний блок ітерації (R,R1).

10) Процес перетворення блоку $U_{-2} \parallel U_{-1}$ в режимі простої заміни криптоалгоритму ГОСТ можна записати:

1. Як послідовність з 34-х підблоків, що пов'язані ланцюговою залежністю виду $U_{i-2} \oplus F_i\left(U_{i-1}\right) = U_i$, за умови перестановки останніх двох підблоків місцями.
2. Як послідовність з 34-х підблоків, що пов'язані ланцюговою залежністю виду $U_{i-2} \oplus F_i\left(U_{i-1}\right) = U_i$.
3. Як послідовність з 32-х підблоків, що пов'язані ланцюговою залежністю виду $U_{i-2} \oplus F_i\left(U_{i-1}\right) = U_i$, за умови перестановки останніх двох блоків місцями.

11) Чи реалізує шифрування в режимі простої заміни криптоалгоритму ГОСТ взаємно однозначне перетворення, якщо блок підстановки K містить лише нулі?

1. Так.
2. Ні.

12) Якщо блок підстановки K містить лише одиниці, то результат зашифрування блоку (L,R) в режимі простої заміни криптоалгоритму ГОСТ дорівнює:

1. Блоку (R, L).
2. Блоку (L, R).
3. Блоку (L$\oplus$11...1, R$\oplus$11...1).

13) Що таке сильний ключ?

1. Це ключ, який неможливо знайти повним перебором ключового простору.
2. Це ключ, який забезпечує належний (заявлений розробником криптосистеми) рівень безпеки інформації.
3. Це ключ, за допомогою якого формується шифротекст, дешифрувати який неможливо.

14) Що таке область сильних ключів?

1. Сукупність сильних ключів, яку виділено кореспондентам для організації шифрозв'язку.
2. Підмножина множини сильних ключів, достатньо велика, щоб протистояти методу повного перебору.
3. Підмножина множини сильних ключів.

15) Чи є криптоалгоритм ГОСТ стійким для довільного блоку підстановки К?

1. Так.
2. Ні, у випадку режиму простої заміни.
3. Ні.

16) Чи існують блоки відкритого тексту, що співпадають з відповідними блоками шифротексту при зашифруванні криптоалгоритмом ГОСТ в режимі простої заміни?

1. Ні.
2. Так, при специфічному виборі блоку підстановки К.
3. Так, при специфічному виборі сеансового ключа.

17) Існує методика побудови області сильних довгострокових ключів для алгоритму ГОСТ, яка побудована на властивостях блоку підстановки К, що розглядається як:

1. Матриця 16×32 повного рангу з простим спектром.
2. Матриця 16×32, що складається з двох ортогональних підматриць розміром 16×16.
3. Матриця 16×32, кожний стовбець якої розглядається як функція від чотирьох двійкових змінних.

18) Неформально шифр С називається скомпрометованим:

1. Якщо відомий метод, що з малою ймовірністю помилки дозволяє визначити, чи одержана задана послідовність в результаті зашифрування шифром С, чи ні.
2. Якщо відомий метод, що дозволяє визначити, чи одержана задана послідовність в результаті зашифрування шифром С.

19) Чому порозрядну суму вхідного підблоку та результату його заміни за допомогою блоку підстановки алгоритму ГОСТ 28147-89 називають псевдогамою?

1. Тому що в цьому шифроперетворенні гама за модулем 2 не є випадковою, бо залежить від ключів обмеженої довжини.
2. Тому що в цьому шифроперетворенні гама за модулем 2 є псевдовипадковою.
3. Тому що в цьому шифроперетворенні гама за модулем 2 залежить від відкритого тексту.

20) Двійковий регістр зсуву з лінійним зворотним зв'язком генерує:

1. Двійкову послідовність, параметри якої неможливо відновити без знання ключів.
2. Довільну двійкову рекурентну послідовність, залежно від параметрів.
3. Рекурентну послідовність виду $x_{i+0} \oplus x_{i+k} \ldots \oplus x_{i+t} = x_{i+n}$, $i = 1, 2 \ldots$, де через $\oplus$ позначено додавання за модулем два.
4. Рекурентну послідовність виду $x_{i+0} \oplus x_{i+k} \ldots \oplus x_{i+t} = x_{i+n}$, $i = 1, 2 \ldots$, параметри якої дуже важко відновити без знання ключів (знак $\oplus$ — сума за модулем два).

21) Чи задовольняє послідовність 1010001 рекурентному співвідношенню $x_0 \oplus x_2 = x_5$?

1. Так.
2. Ні.

22) Чи можна кожний знак лінійної рекурентної послідовності $x_{i+0} \oplus x_{i+k} \ldots \oplus x_{i+t} = x_{i+n}$ записати як лінійну комбінацію відповідних знаків, що становлять підмножину довільної фіксованої сукупності розташованих поспіль n знаків рекуренти?

1. Так.
2. Ні.

23) На практиці двійкові регістри зсуву з лінійним зворотним зв'язком застосовують:

1. Безпосередньо для генерації двійкової гами.
2. Для побудови генераторів гами на основі комбінацій залежних регістрів зсуву, що взаємно впливають на формування своїх послідовних станів.
3. Для формування двійкової гами, що дорівнює порозрядній сумі декількох незалежних регістрів зсуву з лінійним зворотним зв'язком.

24) Імовірність одержати нульове значення функції $x_0 x_1 \oplus x_1 x_2$ при випадковому рівноймовірному виборі двійкових аргументів дорівнює:

1. 1/2.
2. 1/4.
3. 3/4.

25) Нелінійні фільтр-генератори генерують вихідну послідовність:

1. Як нелінійну функцію від довільної послідовності векторних аргументів.
2. Як нелінійну функцію від станів одного й того ж регістру зсуву з лінійним зворотним зв'язком.
3. Як нелінійну функцію від виходів декількох регістрів зсуву з лінійним зворотним зв'язком.

26) Спотворена лінійна рекурентна послідовність відрізняється від неспотвореної тим, що:

1. Співвідношення $x_{i+0} \oplus x_{i+k} \ldots \oplus x_{i+t} = x_{i+n}$ не виконується для довільних $i = 1, 2 \ldots$.
2. Співвідношення $x_{i+0} \oplus x_{i+k} \ldots \oplus x_{i+t} = x_{i+n}$ не виконується для частини заданих індексів $i \in (1, 2 \ldots)$.
3. Співвідношення $x_{i+0} \oplus x_{i+k} \ldots \oplus x_{i+t} = x_{i+n}$ не виконується для невідомих індексів $i \in (1, 2 \ldots)$, які розподілені випадково з відомою ймовірністю.

27) Твердження, що спотворену лінійну рекурентну послідовність не можна відновити, якщо ймовірність викривлення одного біта $p = 1/2$:

1. Невірне.
2. Вірне.

А.3 Контрольні тести до розділу 3

1) Двочленне квадратичне порівняння — це порівняння відносно x виду:

1. $x^2 + ax + b = 0\,(n)$.
2. $x^2 = a\,(n)$.
3. $ax = b^2\,(n)$.

2) Ціле число a називається квадратичним лишком:

1. Якщо воно є повним квадратом.
2. Якщо порівняння $x^2 = a\,(n)$ є розв'язним.
3. Якщо порівняння за простим модулем $x^2 = a\,(p)$ є розв'язним.

3) Кількість квадратичних нелишків за простим модулем:

1. Співпадає з кількістю квадратичних лишків.
2. Більше кількості квадратичних лишків.
3. Співпадає з кількістю ненульових квадратичних лишків.

4) Порівняння $x^2 = a^2\,(n)$, $a \neq 0$:

1. Має точно два розв'язки.
2. Має точно два розв'язки, якщо n — просте число.
3. Не завжди має розв'язки.

5) Символ Лежандра цілого числа a за модулем p позначається:

1. $\left(\frac{a}{p}\right)$, де p непарне число.

2. $\left(\frac{a}{p}\right)$, де p просте число.
3. $\left(\frac{a}{p}\right)$, де p непарне просте число;.
4. $\left(\frac{a}{p}\right)$, де p довільне ціле число.
5. $\left(\frac{a}{p}\right)$, де p непарне просте число, $a \neq 0\,(p)$.

6) Символ Лежандра призначений для позначення:

1. Спеціального випадку раціонального дробу виду $\frac{a}{p}$.
2. Запису цілої частини дробу у вигляді $\left(\frac{a}{p}\right)$.
3. Запису результату алгоритму, що відповідає на питання, чи є число a квадратичним лишком за простим модулем p.

7) Символ Лежандра $\left(\frac{a}{p}\right)$ приймає значення:

1. 0, 1, коли a є відповідно квадратичним лишком (квадратичним нелишком) за модулем p.
2. 1, -1, коли a є відповідно квадратичним лишком (квадратичним нелишком) за модулем p.
3. 1, -1, 0, коли a є відповідно квадратичним лишком, квадратичним нелишком, або нулем за модулем p.

8) Укажіть властивості, що притаманні символу Лежандра $\left(\frac{a}{p}\right)$:

1. Чисельник символу Лежандра можна зводити за модулем знаменника.
2. Символ Лежандра можна обчислити за формулою $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$.
3. При обчисленні символу Лежандра можна застосовувати співвідношення $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{4}}$.
4. При обчисленні символу Лежандра для будь-яких непарних простих чисел p і q можна застосовувати співвідношення $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{8}}$.
5. При обчисленні символу Лежандра можна застосовувати співвідношення $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
6. При обчисленні символу Лежандра для будь-яких непарних простих чисел p і q можна застосовувати співвідношення $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$.

9) Символ Якобі $\left(\frac{a}{n}\right)$ є деякою функцією від a і n, властивості якої необхідно відмітити у наданому нижче списку:

1. Числа a і n — довільні цілі.
2. Числа a і n — довільні натуральні.
3. a і n — довільні непарні цілі числа.
4. a довільне ціле число, n — довільне непарне число.
5. Символ Якобі — окремим випадок символу Лежандра.
6. Символ Якобі є узагальненням символу Лежандра.
7. a довільне ціле число, n — довільне непарне число, що перевищує одиницю.

10) Укажіть властивості символу Якобі $\left(\frac{a}{n}\right)$, де $n = \prod_{i=1}^{k} p_i^{a_i}$:

1. Символ Якобі означає запис результату алгоритму, що відповідає на питання, чи є число a квадратичним лишком за складеним модулем n.
2. Символ Якобі означає значення добутку $\left(\frac{a}{p_1}\right)^{a_1} \ldots \left(\frac{a}{p_k}\right)^{a_k}$, де $\left(\frac{a}{p_i}\right)$ — відповідні символи Лежандра.
3. Якщо значення символу Якобі дорівнює (-1), то число a не є квадратичним лишком за модулем n і навпаки.
4. Символ Якобі можна обчислити без розкладу числа n на співмножники.

11) Укажіть властивості, що притаманні символу Якобі $\left(\frac{a}{n}\right)$:

1. Чисельник символу Якобі можна зводити за модулем знаменника.
2. Символ Якобі можна обчислити за формулою $\left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n$.
3. При обчисленні символу Якобі для будь-яких непарних взаємно простих чисел $m > 1$ і $n > 1$ можна застосовувати співвідношення $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$.
4. При обчисленні символу Якобі можна застосовувати співвідношення $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

12) Алгоритм знаходження квадратного кореня у простому полі можна застосовувати для:

1. Розв'язування порівняння виду $x = y^2\,(p)$ відносно y для довільного непарного p.
2. Розв'язування порівняння виду $x = y^2\,(p)$ відносно y для непарного простого p.

13) Чи є алгоритм розв'язування порівняння $x = y^2\,(p)$ для простого p є детермінованим?

1. Так.
2. Ні.

14) Алгоритм розв'язування порівняння виду $x = y^2\,(p)$, залежно від p:

1. Розділяється на випадки $p = 4k + 3$, $p = 4k + 1$.
2. Розділяється на випадки $p = 4k + 3$, $p = 8k + 5$, $p = 8k + 1$.
3. Розділяється на випадки $p = 4k + 3$, $p = 8k + 3$, $p = 8k + 1$.
4. Розділяється на випадки $p = 4k + 3$, $p = 8k + 3$, $p = 8k + 7$.

15) Чи потребує знання довільного квадратичного нелишку за модулем p алгоритм розв'язування порівняння виду $x = y^2\,(p)$, $p = 8k + 1$?

1. Так.
2. Ні.

16) Основна ідея алгоритму розв'язування порівняння виду $x = y^2\,(p)$, для випадку $p = 8k + 1 = 2^l h + 1$:

1. Побудувати співвідношення виду $x^h \cdot a^{2m} = 1\,(p)$, h — непарне, a — квадратичний лишок, та помножити обидві частини порівняння на x.
2. Побудувати співвідношення виду $x^h \cdot a^{2m} = 1\,(p)$, h — парне, a — квадратичний лишок та помножити обидві частини порівняння на x.
3. Побудувати співвідношення виду $x^h \cdot a^{2m} = 1\,(p)$, h — непарне, a — квадратичний нелишок та помножити обидві частини порівняння на x.

17) Укажіть властивості криптосистеми Ель-Гамаля:

1. Криптосистема Ель-Гамаля не є асиметричною.
2. В криптосистемі Ель-Гамаля ключ зашифрування є несекретним.
3. В криптосистемі Ель-Гамаля ключ розшифрування є несекретним.
4. В криптосистемі Ель-Гамаля використовується тільки арифметика за модулем p.
5. В криптосистемі Ель-Гамаля поряд з арифметикою за модулем p застосовується арифметика за модулем $p - 1$.

18) Укажіть властивості деяких параметрів, що використовуються у криптосистемі Ель-Гамаля:?

1. Параметр p є дуже великим простим числом.
2. Основа для обчислення степенів (параметр g) має бути первісним коренем за модулем p.
3. Основа для обчислення степенів (параметр g) має бути елементом дуже великого порядку, наприклад, первісним коренем за модулем p.
4. Секретний ключ (параметр x) має бути великим псевдовипадковим лишком за модулем p.

5. Секретний ключ (параметр x) має бути великим псевдовипадковим лишком за модулем $p-1$.
6. Секретний ключ (параметр x) має бути великим псевдовипадковим лишком за модулем $\varphi(p)$, де φ — функція Ейлера.
7. Відкритий ключ складається з трьох величин: $p, g, y = g^x (p-1)$.
8. Відкритий ключ складається з трьох величин: $p, g, y = g^x (p)$.

19) Укажіть, які дії потрібно виконати для зашифрування блоку даних $m \,(\mathrm{mod} p)$ за допомогою сформованої криптосистеми Ель-Гамаля:

1. Вибрати рандомізатор $k \,(\mathrm{mod} p-1)$ — псевдовипадкове велике число.
2. Вибрати рандомізатор $k \,(\mathrm{mod} p)$ — псевдовипадкове велике число, взаємно просте з $p-1$.
3. Вибрати рандомізатор $k \,(\mathrm{mod} p-1)$ — секретне псевдовипадкове велике число взаємно просте з $p-1$.
4. Вибрати рандомізатор $k \,(\mathrm{mod} p)$ — секретне псевдовипадкове велике число.
5. З метою економії часу, зберегти рандомізатор k у захищеному вигляді для застосування в іншому сеансі шифрування.
6. Записати криптограму у вигляді $\left(g^k (p), y^k m (p)\right)$.
7. Записати криптограму у вигляді $\left(g^k \,(\mathrm{mod} p), (y+m) \,(\mathrm{mod} p)\right)$.

20) Укажіть, які параметри та обчислення використовуються в механізмі цифрового підпису Ель-Гамаля, що застосовується для підпису повідомлення m:

1. Використовуються параметри $p, g, y = g^x (p)$, як у криптосистемі Ель-Гамаля.
2. Використовується рандомізатор k і параметри $p, g, y = g^x (p)$, як у криптосистемі Ель-Гамаля.
3. Використовується рандомізатор k, параметри $p, g, y = g^x (p)$, як у криптосистемі Ель-Гамаля, та геш-функція повідомлення $m \,(\mathrm{mod} p)$.
4. Використовується рандомізатор k, параметри $p, g, y = g^x (p)$, як у криптосистемі Ель-Гамаля, та геш-функція $h(m)$ повідомлення m.

21) Укажіть властивості цифрового підпису (ЦП) Ель-Гамаля, що застосовується для підпису повідомлення m:

1. ЦП Ель-Гамаля представляється у вигляді двох блоків (r, s), кожний з яких є лишком за модулем $p-1$.
2. ЦП Ель-Гамаля представляється у вигляді двох блоків (r, s), перший з яких є лишком за модулем p.
3. Блок r не залежить від повідомлення m, та обчислюється через рандомізатор у вигляді $r = g^k (p)$.

4. Блок r залежить від повідомлення m, та обчислюється через рандомізатор у вигляді $r = mg^k\,(p)$.
5. Блок s залежить від повідомлення m, та обчислюється через секретний ключ, геш-функцію та рандомізатор у вигляді $s = xg^k + hm\,(p)$.
6. Блок s залежить від повідомлення m, та обчислюється через секретний ключ, геш-функцію та рандомізатор з порівняння $h\,(m) = xr + ks\,(p-1)$.
7. Блок s залежить від повідомлення m, та обчислюється через секретний ключ, геш-функцію та рандомізатор з порівняння $h\,(m) = xr + ks\,(p)$.
8. Для перевірки ЦП використовується співвідношення $g^h = y^r r^s\,(p)$.
9. Для перевірки ЦП використовується співвідношення $g^h = y^r x^s\,(p-1)$.

22) Укажіть, які властивості рандомізатора k знижують стійкість ЦП Ель-Гамаля:

1. Якщо k відомий, то завжди можна однозначно розкрити секретний ключ.
2. Якщо k відомий, блок r взаємно простий з параметром p, то завжди можна однозначно розкрити секретний ключ.
3. Якщо k відомий, блок r взаємно простий з числом $p-1$, то завжди можна однозначно розкрити секретний ключ.
4. Якщо підписи для двох різних повідомлень відомі, а рандомізатори при цьому були вибрані однаковими, то з великою ймовірністю можна однозначно розкрити і спільний рандомізатор і секретний ключ.

23) Укажіть істинні твердження щодо алгоритму Сільвера-Полліга-Хеллмана:

1. Алгоритм Сільвера-Полліга-Хеллмана призначений для факторизації чисел.
2. Алгоритм Сільвера-Полліга-Хеллмана призначений для розв'язування загальної задачі дискретного логарифмування в скінченних полях $GF\,(q)$.
3. Алгоритм Сільвера-Полліга-Хеллмана призначений для розв'язування задачі дискретного логарифмування в скінченних полях $GF\,(q)$, де число $q-1$ не перевищує деякої великої границі.
4. Алгоритм Сільвера-Полліга-Хеллмана призначений для розв'язування задачі дискретного логарифмування в скінченних полях $GF\,(q)$, де число $q-1$ є гладким.
5. Алгоритм Сільвера-Полліга-Хеллмана призначений для розв'язування задачи дискретного логарифмування в скінченних полях $GF\,(q)$, де число $q-1$ є гладким і не перевищує деякої великої границі.

24) Укажіть умови застосування алгоритму Сільвера-Полліга-Хеллмана:

1. При застосуванні алгоритму Сільвера-Полліга-Хеллмана в скінченному полі $GF(q)$ канонічний розклад числа $q-1$ на прості співмножники має вид $q-1=\prod_p p^{a(p)}$, де числа p^a не перевищують деякої великої границі.
2. При застосуванні алгоритму Сільвера-Полліга-Хеллмана в скінченному полі $GF(q)$ канонічний розклад числа $q-1$ на прості співмножники має вид $q-1=\prod_p p^{a(p)}$, де прості числа p не перевищують деякої великої границі.
3. При застосуванні алгоритму Сільвера-Полліга-Хеллмана в скінченному полі $GF(q)$ канонічний розклад числа $q-1$ на прості співмножники має вид $q-1=\prod_p p^{a(p)}$, де числа $a(p)$ не перевищують деякої великої границі.

25) Для розв'язування задачі дискретного логарифмування $y=b^x$ в полі $GF(q)$ в алгоритмі Сільвера-Полліга-Хеллмана:

1. x визначається перебором.
2. x визначається за допомогою аналізу дільників числа $b-1=\prod_p p^{a(p)}$.
3. x визначається за допомогою китайської теореми про залишки, для чого попередньо обчислюються залишки виду $x\left(\mathrm{mod} p^{a(p)}\right)$, де $q-1=\prod_p p^{a(p)}$.
4. Систематично застосовується процедура побудови чисел, які є коренями степенів p з одиниці в полі, що мають вид $b^{j(q-1)/p}$, $q-1=\prod_p p^{a(p)}$.
5. Систематично застосовується процедура побудови чисел, які є коренями степеня h з одиниці з одиниці в полі, що мають вид $b^{(q-1)(p-1)/h}$, $p-1=\prod_p p^{h(p)}$.
6. Використовується факт, що шукане значення x можна записувати у системах числення за основами p, що входять в розклад, $q-1=\prod_p p^{a(p)}$.
7. Критичним параметром є не швидкодія, а обсяг оперативної пам'яті комп'ютера.
8. Критичним параметром є не обсяг оперативної пам'яті, а швидкодія комп'ютера.

26) Укажіть властивості ро-методу факторизації Полларда:

1. Метод спрямований на знаходження власного дільника складеного числа n.
2. Назва методу пов'язана з тим, що оцінка істинності розв'язку аналогічна обчисленню питомої ваги ρ суміші декількох речовин.
3. Назва методу пов'язана з тим, що графічний вигляд послідовностей, що виникають в ході роботи алгоритму, нагадують грецьку літеру ρ.
4. Ефективність знаходження власного дільника складеного числа n суттєво залежить від швидкодії комп'ютера.
5. Ефективність знаходження власного дільника складеного числа n суттєво залежить від обсягу зовнішніх накопичувачів комп'ютера.

27) Суть ро-методу Полларда факторизації числа n полягає:

1. У знаходженні критичних пар, тобто співпадаючих елементів з різними індексами в послідовності $x_{j+1} = f(x_j) \bmod n$, де f — поліном.
2. У знаходженні критичних пар, тобто співпадаючих елементів з різними індексами в послідовності $x_{j+1} = f(x_j) \bmod r$, де f — поліном, а r — невідомий шуканий дільник числа n.
3. У знаходженні критичних пар, тобто елементів $x_i = x_j$ з мінімальними індексами $i \neq j$ в послідовності $x_{j+1} = f(x_j) \bmod r$, де f — поліном, а r — невідомий шуканий дільник числа n.

28) Суттєва оптимізація ро-методу Полларда факторизації числа полягає:

1. У підвищенні ефективності обчислення критичних пар x_i, x_j.
2. У спеціальній процедурі вибору полінома $f(x)$.
3. У спеціальній процедурі вибору критичних пар x_i, x_j для обчислення НСД$(x_j - x_i, n)$.

29) Укажіть постановку задачі для $(p-1)$ - алгоритму факторизації Полларда:

1. Знайти власний дільник натурального числа n.
2. Знайти власний дільник натурального числа $n = pq$, де p, q — прості числа.
3. Знайти власний дільник непарного натурального числа $n = pq$, де p, q — прості числа.
4. Знайти власний дільник непарного натурального числа $n = pq$, де p простий дільник числа n, за умови, що число $p - 1$ є гладким.
5. Знайти власний дільник непарного натурального числа n.
6. Знайти власний дільник непарного натурального числа $n = pq$, де p простий дільник числа n.

30) Укажіть ідею $(p-1)$ — алгоритму Полларда факторизації числа $n = pq$:

1. Вибрати випадкове число a, НСД$(a,n) = 1$, знайти число ν що ділиться на $ord_p a$, де p — простий дільник числа n, обчислити $r =$НСД$(a^\nu - 1, n)$ та вибрати нове значення , якщо $r = 1$, або $r = n$.
2. Вибрати випадкове число a, НСД$(a,n) = 1$, знайти число ν для якого $a^\nu = 1\,(n)$, обчислити $r =$НСД$(a^\nu - 1, n)$ та вибрати нове значення a, якщо $r = 1$, або $r = n$.
3. Вибрати випадкове число a, НСД$(a,n) = 1$, намагатися знайти число ν для якого $a^\nu \neq 1\,(n)$, але $a^\nu = 1\,(p)$, де p — простий дільник числа n, обчислити $r =$НСД$(a^\nu - 1, n)$ та вибрати нове значення a, якщо $r = 1$, або $r = n$.

31) Укажіть основні риси алгоритму факторизації Діксона:

1. Алгоритм спрямований на знаходження дільника складеного числа n.
2. Алгоритм спрямований на знаходження дільника p складеного непарного числа n.
3. Для факторизації числа n в алгоритмі Діксона достатньо знайти пару чисел x, y, що задовольняють співвідношення $x^2 - y^2 = 0\,(n)$.
4. Для факторизації числа n в алгоритмі Діксона достатньо знайти пару чисел x, y, що задовольняють так зввне нетривіальне співвідношення: $x^2 - y^2 = 0\,(n)$, $x \neq \pm y\,(n)$.
5. для факторизації числа n в алгоритмі Діксона достатньо знайти пару чисел x, y, що задовольняють так зване нетривіальне співвідношення: $x^2 - y^2 = 0\,(p)$, $x \neq \pm y\,(p)$, де p — невідомий дільник n.
6. Числа x, y, що задовольняють співвідношення $x^2 - y^2 = 0\,(n)$, знаходяться перебором їхніх значень до заданої границі M, множина B значень x, y називається факторною базою.
7. Числа x, y, що задовольняють співвідношення $x^2 - y^2 = 0\,(n)$, знаходяться, виходячи з множини B відносно невеликих простих чисел, що не перевищують заданої границі M, множина B називається факторною базою.

32) Укажіть правильне визначення, за умови, що число n підлягає факторизації:

1. Число b називається B-числом, якщо воно належить до факторної бази B.
2. B-числом називається добуток деяких елементів факторної бази B.
3. B-числом називається добуток степенів деяких елементів факторної бази B за модулем числа n.
4. Число b називається B-числом, якщо воно дорівнює добутку степенів деяких елементів факторної бази B за модулем n.
5. Число b називається B-числом, якщо b^2 за модулем числа n дорівнює добутку степенів деяких елементів факторної бази B.

33) Укажіть правильне твердження щодо алгоритму факторизації Діксона числа n:

1. В алгоритмі суттєво використовується, що розклад B-чисел на степені простих є однозначним.
2. В алгоритмі суттєво використовується, що розклад квадратів B-чисел на степені простих не є однозначним.
3. В алгоритмі суттєво використовується, що розклад лишків квадратів B-чисел за модулем n є однозначним.
4. В алгоритмі суттєво використовується, що розклад лишків квадратів B-чисел за модулем n не є однозначним.

34) В алгоритмі факторизації Діксона числа n задача зводиться до запису квадрату відомого числа у вигляді добутку як парних так і непарних степенів елементів факторної бази за модулем n:

1. Так.
2. Ні.

35) Чи завжди вимагає дешифрування повідомлення криптосистеми RSA факторизації модуля n?

1. Так.
2. Ні.

36) Якщо два абоненти використовують криптосистеми RSA з параметрами (e_1, d_1, n) та (e_2, d_2, n), то чи можуть вони читати листування одне одного?

1. Так.
2. Ні.

37) Якщо відкритий ключ криптосистеми RSA дуже малий, порівняно з модулем, то:

1. Це підвищує якість криптосистеми за рахунок зростання швидкості піднесення до степеня.
2. Це може призвести до дешифрування окремих повідомлень.

38) Укажіть істинні твердження, щодо атаки Франкліна:

1. Атака застосовується до криптосистеми RSA (e, d, n) з дуже малим відкритим ключем, скажімо, $e = 3$.
2. При $e = 3$ атака дозволяє дешифрувати довільні криптограми.
3. При $e = 3$ атака дозволяє дешифрувати деякі одиночні криптограми.
4. При $e = 3$ атака дозволяє дешифрувати пари криптограм, відкриті тексти яких m_1 та m_2 залежні: $m_2 = m_1 + \Delta(n)$.
5. При $e = 3$ атака дозволяє дешифрувати пари криптограм, відкриті тексти яких m_1 та m_2 залежні: $m_2 = m_1 + \Delta(n)$, а значення Δ відоме.

6. При $e = 3$ і $a = m_1^e(n)$, $b = m_2^e(n)$, атака основана на знаходженні НСД многочленів $x^3 - a$ та $(x + \Delta)^3 - b$.
7. При $e = 3$ і $a = m_1^e(n)$, $b = m_2^e(n)$, дешифрування здійснюється за формулою $m_1 = \frac{\Delta(2a+b-\Delta^3)}{\Delta^3-a+b}$.
8. При $e = 3$ і $a = m_1^e(n)$, $b = m_2^e(n)$, атака основана на знаходженні кубічного кореня з a за модулем n.
9. При $e = 3$ і $a = m_1^e(n)$, $b = m_2^e(n)$, знаходження m_1 вимагає етапу перебору значної кількості варіантів.
10. При $e = 3$ і $a = m_1^e(n)$, $b = m_2^e(n)$, дешифрування здійснюється за формулою $m_1 = \frac{\Delta(2a+b-\Delta^3)}{2\Delta^3-a+b}$.

39) Укажіть властивості детермінованих тестів перевірки чисел на простоту:

1. Детерміновані тести призначені для доведення простоти чисел.
2. На практиці зустрічаються детерміновані тести, які не можна застосувати для довільних простих чисел, оскільки вони використовують лише достатні умови простоти.
3. Детерміновані тести доводять простоту чисел з довільно малою ймовірністю помилки.
4. Усі детерміновані тести, можна застосувати для довільних простих чисел та отримати однозначну відповідь щодо їхньої простоти.

40) Укажіть властивості ймовірнісних тестів перевірки чисел на простоту:

1. Імовірнісні тести призначені для доведення простоти чисел.
2. На практиці зустрічаються ймовірнісні тести, які не можна застосувати для довільних простих чисел.
3. Імовірнісні тести доводять простоту чисел з довільно малою ймовірністю помилки.
4. Імовірнісні тести, можна застосувати для довільних простих чисел та отримати однозначну відповідь щодо їхньої простоти.

41) Число n називається:

1. Псевдопростим за основою a, якщо пара (a, n) задовольняє співвідношення $a^{n-1} = 1\,(n)$.
2. Псевдопростим за основою a, якщо пара (a, n) задовольняє співвідношення $a^{p-1} = 1\,(n)$, де p — деякий дільник числа n.
3. Числом Кармайкла за основою a, якщо пара (a, n) задовольняє співвідношення $a^{n-1} = 1\,(n)$.
4. Числом Кармайкла, якщо для довільних $a \neq 0$ $a^{n-1} = 1\,(n)$.

42) Укажіть властивості тесту Ферма перевірки числа n на простоту:

1. Тест Ферма є детермінованим.
2. Тест Ферма є імовірнісним.
3. Як критерій в тесті Ферма на кожному кроці використовується співвідношення Ферма $a^{n-1} = 1\,(n)$, де a — псевдовипадковий лишок за модулем n.
4. Як критерій в тесті Ферма на кожному кроці використовується співвідношення Ферма $a^{n-1} = 1\,(n)$, $(a, n) = 1$, де a — псевдовипадковий лишок за модулем n.
5. Імовірність помилки за k кроків тесту Ферма дорівнює $(1/2)^k$.
6. Імовірність помилки за k кроків тесту Ферма дорівнює $(1/4)^k$ якщо n не є числом Кармайкла.
7. Імовірність помилки за k кроків тесту Ферма дорівнює $(1/2)^k$, якщо n не є числом Кармайкла.
8. Імовірність помилки за k кроків тесту Ферма дорівнює $(1/2)^k$ якщо n є числом Кармайкла.

43) Укажіть істинні твердження щодо властивостей чисел Кармайкла:

1. Число n з канонічним розкладом виду $n = p_1p_2p_3p_4$ не може бути числом Кармайкла.
2. Число n з канонічним розкладом виду $n = p_1p_2p_3p_4$ може бути числом Кармайкла.
3. Число n з канонічним розкладом виду $n = p_1p_2$ не може бути числом Кармайкла.
4. Число n з канонічним розкладом виду $n = p_1p_2$ може бути числом Кармайкла.
5. Число n з канонічним розкладом виду $n = p_1^2p_2p_3p_4$ не може бути числом Кармайкла.
6. Число n з канонічним розкладом виду $n = p_1^2p_2p_3p_4$ може бути числом Кармайкла.

44) Число 1309 не є числом Кармайкла:

1. Вірно.
2. Невірно.

45) Число n називається ейлеровим псевдопростим за основою a, якщо:

1. Воно є псевдопростим Ферма і має розклад виду $n = p_1p_2p_3$.
2. Воно задовольняє критерій виду $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \bmod n$.
3. Воно є складеним і задовольняє критерій виду $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \bmod n$.

46) Множина псевдопростих Ферма:

1. Співпадає з множиною ейлерових псевдопростих чисел.

2. Є підмножиною множини ейлерових псевдопростих чисел.
3. Містить в собі множину ейлерових псевдопростих чисел.

47) Тест Соловея-Штрассена:

1. Є детермінованим тестом перевірки чисел на простоту.
2. Виявляє, чи є задані числа квадратичними нелишками.
3. Є імовірнісним тестом перевірки чисел на простоту.

48) Властивості тесту Соловея-Штрассена:

1. За схемою аналогічний тесту Ферма, але на кожному кроці перевіряється інше співвідношення.
2. На відміну від тесту Ферма, вимагає вибору на кожному кроці елементу, що є квадратичним нелишком.
3. Гарантує, що ймовірність невідбраковки складеного числа за k кроків $\leqslant (1/2)^k$.
4. Гарантує, що ймовірність невідбраковки складеного числа за k кроків $\leqslant (1/4)^k$.

49) Тест Рабіна-Міллера:

1. Є окремим детермінованим тестом перевірки чисел на простоту.
2. Є комбінацією тестів Ферма і Соловея-Штрассена.
3. Є окремим імовірнісним тестом перевірки чисел на простоту.

50) Властивості тесту Рабіна-Міллера:

1. За схемою аналогічний тесту Ферма, але на кожному кроці перевіряється інше співвідношення.
2. Гарантує, що ймовірність невідбраковки складеного числа за k кроків $\leqslant (1/2)^k$.
3. гарантує, що ймовірність невідбраковки складеного числа за k кроків $\leqslant (1/4)^k$.
4. Для тестування числа n достатня для практики кількість повторень тесту $\leqslant \log_2 n$.
5. Для тестування числа n достатня для практики кількість повторень тесту $\leqslant 2\log_2^2 n$.
6. За схемою аналогічний тесту Ферма, але на кожному кроці може перевіряється декілька умов.

51) Число n називається сильно псевдопростим за основою a якщо:

1. Воно є одночасно псевдопростим Ферма і ейлеровим псевдопростим за основою a.
2. Воно є складеним і проходить тест Рабіна-Міллера.

3. Воно є складеним і проходить один крок тесту Рабина-Миллера для числа n, з відповідним числом a в якості основи.

52) Формулювання критерію Люка простоти числа n:

1. Число n є простим тоді і тільки тоді, коли існує число a, таке що $a^n = 1\,(n)$ і для довільного нетривіального дільника q числа $n-1$ виконується співвідношення $a^{n-1/q} = 1\,(n)$.
2. Число n є простим тоді і тільки тоді, коли існує число a, таке що $a^{n-1} = 1\,(n)$ і для довільного нетривіального дільника q числа $n-1$ виконується співвідношення $a^{n-1/q} \neq 1\,(n)$.

53) При застосуванні критерію Люка для перевірки простоти числа n необхідно:

1. Знати розклад числа n на степені простих чисел.
2. Знати всі прості дільники числа $n-1$.
3. Знати частину простих дільників числа $n-1$, що задовольняють деякі умови.

54) Уточнення критерію Люка простоти числа n:

1. Число n є простим тоді і тільки тоді, коли для кожного нетривіального дільника q числа $n-1$ існує число a, таке що $a^{n-1} = 1\,(n)$, $a^{n-1/q} \neq 1\,(n)$.
2. Число n є простим тоді і тільки тоді, коли існує число a, таке що $a^{n-1} = 1\,(n)$ і для довільного нетривіального дільника q числа$n-1$ виконується співвідношення $a^{n-1/q} \neq 1\,(n)$.

55) Узагальнення критерію Люка простоти числа n:

1. Число n є простим, якщо існує число a, таке що $a^n = 1\,(n)$ і для довільного нетривіального дільника виду q^2 числа $n-1$ виконується співвідношення $a^{n-1/q} = 1\,(n)$.
2. Нехай $n = FR + 1 > 1$, де $1 < R < F$ і для будь-якого простого дільника q числа F знайдеться число a, що $a^{n-1} = 1\,(n)$, $\text{НСД}\big(a^{n-1/q} - 1, n\big) = 1$, тоді число n просте.

56) При застосуванні узагальненого критерію Люка для перевірки простоти числа n необхідно:

1. Знати розклад числа n на степені простих чисел.
2. Знати всі прості дільники числа $n-1$.
3. Знати частину простих дільників числа $n-1$, що задовольняють деякі умови.

57) Укажіть істинне твердження щодо характеристики теореми Димитко:

1. Теорема Димитко дозволяє протестувати довільне натуральне число $n > 1$ на простоту, якщо розклад $n-1 = \prod_{i=1}^{k} p_i^{a_i}$ містить просте $q < \sqrt{n}$.
2. Теорема Димитко дозволяє протестувати на простоту натуральне число $n > 1$, для якого розклад $n-1 = \prod_{i=1}^{k} p_i^{a_i}$ не містить квадратів.
3. Теорема Димитко дозволяє протестувати на простоту натуральне число $n > 1$, якщо $n = qR + 1$, де q — просте, $R < 4(q+1)$, R — парне.
4. Теорема Димитко дозволяє протестувати на простоту натуральне число $n > 1$, якщо $n = qR + 1$, де q — просте, $R > 4(q+1)$, R — парне а q, R — взаємно прості числа.
5. Теорема Димитко дозволяє протестувати на простоту натуральне число $n > 1$, якщо $n = qR + 1$, де q — просте, $R < 4(q+1)$, R — непарне, а q, R — взаємно прості числа.

58) Укажіть істинні твердження про вимоги щодо вибору простих дільників p, q $(q > p)$ модуля n криптосистеми RSA:

1. Найбільший спільний дільник $(p-1, q-1)$ має бути максимально великим.
2. Найбільший спільний дільник $(p-1, q-1)$ має бути як найменший.
3. Різниця $q - p$ має бути як найменшою.
4. Різниця $q - p$ має бути дуже великою.
5. p, q — псевдовипадкові, розміру $\approx \sqrt{n}$.
6. Число $n - 1$ має ділитися на велике просте число.
7. Жодне з чисел $(p-1, q-1)$ не розкладається в добуток степенів невеликих простих чисел.
8. Кожне з чисел $(p+1, q+1)$ не розкладається в добуток степенів невеликих простих чисел.

59) Укажіть істинні твердження щодо сильно простих чисел:

1. Сильно просте число p за основою a — це число, що проходить один крок тесту Рабіна-Міллера, з відповідним числом a в якості основи.
2. Просте число p називається сильно простим якщо виконуються умови: $p = 1 (\mathrm{mod} r)$, $p = -1 (\mathrm{mod} s)$, де r, s — великі прості числа.
3. Просте число p називається сильно простим якщо виконуються умови: $p = 1 (\mathrm{mod} r)$, $p = -1 (\mathrm{mod} s)$, $r = 1 (\mathrm{mod} t)$, де r, s, t — великі прості числа.
4. Метод Гордона служить для побудови сильно простих чисел.

60) Апаратно реалізовані засоби криптографічного захисту інформації називаються:

1. Кодеками.
2. Криптосхемами.
3. Шифраторами.

61) При апаратній реалізації для шифрування використовуються:

1. Тільки блокові шифри.
2. Тільки потокові шифри.
3. Як блокові, так і потокові.

62) Апаратні засоби, що використовують послідовність гами, заготовлену заздалегідь іншими способами, називаються:

1. Трансляторами.
2. Змішувачами.
3. Кодеками.
4. Скремблерами.

63) Укажіть властивості мережного ключа:

1. Мережний ключ захищає апаратні засоби шифрування від несанкціонованого вимикання живлення.
2. Мережний ключ змінюється тільки за узгодженням з усіма абонентами мережі.
3. Мережний ключ може мати необмежений термін дії.
4. Термін дії мережного ключа не перебільшує року.
5. Мережний ключ не може бути секретним.
6. Мережний ключ заноситься при виготовлені партії пристроїв і є секретним криптографічним параметром.

64) Довгостроковий ключ:

1. Діє тільки на групу повідомлень.
2. Є секретним криптографічним параметром.
3. Змінюється, як правило, періодично.
4. Має тривалий термін дії.

65) Сеансовий ключ:

1. Діє тільки на групу повідомлень.
2. Є секретним криптографічним параметром.
3. Змінюється, як правило, періодично.
4. Може змінюватися на кожне повідомлення.
5. На відміну від разового ключа не може змінюватися на кожне повідомлення.
6. Має тривалий термін дії.

Додаток В

ВІДПОВІДІ ДО КОНТРОЛЬНИХ ТЕСТІВ

В.1 Відповіді до контрольних тестів розділу 1

1) — 3. 2) — 2. 3) — 1, 2, 3, 4. 4) — 1. 5) — 1. 6) — 4. 7)— 2. 8) — 3. 9) — 3. 10) — 3. 11) — 2. 12) — 2. 13) — 2, 3, 5, 7, 8. 14) — 2. 15) — 2. 16) 1, 3, 5, 6. 17) — 3. 18) — 2. 19) — 1. 20) — 3, 4. 21) — 1, 3. 22) — 1, 2, 3. 23) — 2, 3, 5. 24) — 2, 4, 6, 7, 8. 25) — 2, 5, 6. 26) — 3. 26) — 3. 27) — 4, 5, 6. 28) — 1, 2, 3. 29) — 2, 3, 4, 6. 30) — 4. 31) — 2. 32) — 3. 33) — 4. 34) — 2. 35) — 3. 36) — 1. 37) — 3. 38) — 2. 39) — 4. 40) — 3. 41) — 3. 42) — 1. 43) — 2. 44) — 2. 45) — 2. 46) — 2.

В.2 Відповіді до контрольних тестів розділу 2

1) — 2. 2) — 1. 3) — 3. 4) — 4. 5) — 3. 6) — 1. 7) — 3. 8) — 2. 9) — 3. 10) — 1. 11) — 1. 12) — 1. 13) — 2. 14) — 2. 15) — 3. 16) — 3. 17) — 3. 18) — 1. 19) — 3. 20) — 3. 21) — 2. 22) — 1. 23) — 2. 24) — 3. 25) — 2. 26) — 3. 27) — 2.

В.3 Відповіді до контрольних тестів розділу 3

1) — 2. 2) — 2. 3) — 3. 4) — 2. 5) — 3. 6) — 3. 7) — 3. 8) — 1, 2, 5, 6. 9) — 6, 7. 10) — 2, 3, 4. 11) — 1, 3, 4. 12) — 2. 13) — 2. 14) — 2. 15) — 1. 16) — 3. 17) — 2, 5. 18) — 1, 3, 5, 6, 8. 19) — 3, 6. 20) — 4. 21) — 2, 3, 6, 8. 22) — 3, 4. 23) — 4. 24) — 2. 25) — 3, 4, 6, 7. 26) — 1, 3, 4. 27) — 2. 28) — 3. 29) — 4. 30) — 3. 31) — 2, 4, 7. 32) — 5. 33) — 4. 34) – 1. 35) — 2. 36) — 1. 37) — 2. 38) — 1, 5, 6, 10. 39) — 1, 2. 40) — 3. 41) — 1, 4. 42) — 2, 4, 7. 43) — 2, 3, 5. 44) — 1. 45) — 3. 46) — 3. 47) — 3. 48) — 1, 3. 49) — 3. 50) — 3, 5, 6. 51) — 3. 52) — 2. 53) — 2. 54) — 1. 55) — 2. 56) — 3. 57) — 3. 58) — 2, 4, 5, 7, 8. 59) — 3, 4. 60) — 3. 61) — 3. 62) — 2. 63) — 3, 6. 64) — 2, 3, 4. 65) — 2, 4.

Предметний покажчик

Література

1. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник / За ред. проф. Кривуци В.Г. — К.: ООО “Д.В.К.”, 2004. — 508 с.

2. Вербицький О.В. Вступ до криптографії. Львів: Видавництво науково-технічної літератури, 1998. 248 с.

3. Виноградов И.М. Основы теории чисел. — 9-е изд., перераб. — М.: Наука, 1981. — 124 с.

4. Введение в криптографию / Под общей редакцией В.В. Ященко. — М.: МЦНМО: "Че Ро", 1999. 272 с.

5. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Изд-во стандартов, 1989. — 26 с.

6. Дэвенпорт Г. Высшая арифметика. М.: Наука, 1965.

7. Коблиц Н. Курс теории чисел в криптографии — М.: Научное издательство ТВП, 2001.

8. Математичні основи криптографії: Навч. посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. — Дніпропетровськ: Національний гірничий університет, 2004. — 391 с.

9. Мухачов В.А., Хорошко В.А. Методы практической криптографии. — К.: ООО “ПолиграфКонсалтинг”, 2005. — 215 с.

10. Саломаа А. Криптография с открытым ключом — М.: Мир, 1996. — 324 с.

11. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. — 104 с.

12. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Изд-во ТРИУМФ,2002. — 816 с.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Богуш Володимир Михайлович
Мухачов Владислав Андрійович

Криптографічні застосування елементарної теорії чисел

Навчальний посібник

Підписано до друку 30.06.2006 р. Формат 60×90/16, папір типограф.
Друк офсетний. Ум. фарбовідб. 8. Ум. друк. арк. 7,86.
Обл.-вид. арк. 9. Наклад 500 прим.
Замовлення 259/2
Видавництво ДУІКТ
03110, Київ, вул. Солом'янська, 7.
Надруковано "Видавництво ДУІКТ"
03110, Київ, вул. Солом'янська, 7