Державний комітет зв'язку та інформатизації України

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ім. О. С. ПОПОВА

М.В. Захарченко, Л.Г. Йона, Ю.В. Щербина, О.В. Онацький

РОЗВИНЕННЯ КРИПТОЛОГІЇ ТА ЇЇ МІСЦЕ В СУЧАСНОМУ СУСПІЛЬСТВІ

Частина I

КЛАСИЧНІ МЕТОДИ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ

Навчальний посібник

з дисципліни

Захист інформації в телекомунікаційних системах і мережах

для спеціальностей 6.092400, 7.090703, 7.092401,7.092402

ЗАТВЕРДЖЕНО
методичною радою
ОНАЗ ім. О.С. Попова
Протокол № 10
від 11 березня 2004 р.

Одеса 2004

УДК 003.26

План НМВ 2004 р.

Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце в сучасному суспільстві : Навч. посібник. – Одеса: ОНАЗ ім. О. С. Попова, 2003. – 80 с.

Першу частину посібника призначено для вивчення шифрів з симетричним ключем і розраховано на тих, хто вперше знайомиться з криптологією. Розглянуто питання дешифрування найпростіших шифрів. Містить систематичне викладення наукових основ від найпростіших прикладів та основних понять до сучасних криптографічних концепцій.

Посібник призначено для студентів, котрі вивчають дисципліну "Захист інформації в телекомунікаційних системах і мережах".

За редакцією **М.В. Захарченка**

Рецензент – доцент **А.Л. Федоров**

СХВАЛЕНО
на засіданні кафедри
документального електрозв’язку
і рекомендовано для друку
Протокол № 6
від 26.12.2003 р.

ЗМІСТ

ВСТУП

Проблема захисту інформації шляхом перетворення, яке виключає можливість її прочитування сторонньою особою, хвилювала людський розум з давніх часів. Питаннями захисту інформації шляхом її перетворювання займається ***криптологія*** (kryptos – таємний, logos – наука). Криптологія поділяється на два напрямки – криптографію й криптоаналіз. Цілі цих напрямків є прямо протилежні. Взаємини криптографії й криптоаналізу є очевидні: криптографія – захист, тобто розробляння шифрів, а криптоаналіз – напад, тобто атака на шифри. Однак ці дві дисципліни є щільно пов'язані, й не буває кваліфікованих криптографів, котрі не володіли б методами криптоаналізу.

Криптографія – одноліток історії людської мови. Більш того, спочатку писемність власне сама була криптографічною системою, тому що в стародавніх суспільствах нею володіли лише обрані.

Із зародженням людської цивілізації виникло вміння повідомляти інформацію певним особам у такий спосіб, аби вона не ставала відомою для інших. Допоки люди використовували для передавання повідомлень винятково голос і жести, зробити це зазвичай не становило великих труднощів: треба було лише запобігти присутності в безпосередній близькості від співбесідників тих людей, для кого ці відомості не призначалися. Однак іноді зовнішні чинники накладали на поводження співрозмовників обмеження, котрі не дозволяли їм сховатися від сторонніх вух та очей для проведення конфіденційної бесіди. Для чинення в подібних обставинах була створена, а точніше склалася сама собою, система кодованих мовою чи жестами повідомлень. У різноманітних ситуаціях вона мала цілковито відмінний характер – від окремого таємного знака, який свідчив про настання певної події, до розвинених таємних мов, котрі дозволяли передавати думки практично будь-якої складності.

З виникненням писемності завдання забезпечення таємності й автентичності передаваних повідомлень стало надто актуальним. Насправді, повідомлення, передаване голосом чи жестами, є доступне для стороннього лише того короткого проміжку часу, поки воно "в дорозі", а щодо його авторства й автентичності в одержувача жодних сумнівів виникати не могло, оскільки він бачив свого співрозмовника. Записане на папері повідомлення існує в матеріальному світі набагато довше, і в людей, котрі бажають ознайомитися з його змістом всупереч волі відправника й одержувача, виникає набагато більше шансів зробити це. Тому саме після виникнення писемності з'явилося мистецтво тайнопису, мистецтво "таємно писати" – набір методів, призначених для секретного передавання записаних повідомлень від однієї людини до іншої.

З широким розповсюдженням писемності криптографія стала формуватися як самостійна наука. Дані про перші способи тайнопису є вельми уривчасті. Припускається, що криптографія була відома в давньому Єгипті й Вавілоні. До нашого часу дійшли свідчення про те, що мистецтво секретного письма використовувалося в давній Греції. Перші насправді вірогідні відомості з описанням методу шифрування належать до періоду зміни старої й нової ери.

Перші криптосистеми виникають вже на початку нової ери. Приміром, Цезар у своєму листуванні використовував уже більш-менш систематичний шифр, котрий дістав його ім'я.

Бурхливого розвинення криптографічні системи набули роками першої й другої світових війн минулого сторіччя. Розпочинаючи з післявоєнного часу й по нинішній день розвинення обчислювальних засобів прискорює розробляння й удосконалювання криптографічних методів.

Чому проблема використання криптографічних методів в інформаційних системах (ІС) стала сьогодні надто актуальна?

З одного боку, розширилося використання комп'ютерних мереж, зокрема глобальної мережі Інтернет, якими передаються потужні обсяги інформації державного, військового, комерційного та приватного характеру, що вона не припускає можливості доступу до неї сторонніх осіб.

З іншого боку, поява нових потужних комп'ютерів, технологій мережних та нейронних обчислень уможливила дискредитацію криптографічних систем, котрі ще донедавна вважалися за стійкі.

Наведемо історичний приклад. Вважається, що в Біблії поряд з описанням різноманітних подій, які мали місце в далекому минулому, є ще певний таємний зміст, чи, інакше кажучи, зашифрований зміст [8], зокрема пророкування про важливі події в житті людства й окремих людей. Для того щоби довідатися про цей зміст, потрібно знати ключ. Впродовж століть пошуками такого ключа займалися багато богословів і вчених. Але віднайти його не вдавалося нікому. У наші дні таку спробу зробила група ізраїльських математиків, очолювана професором Іньяхо Ріпсом. Для свого дослідження ізраїльські вчені взяли п'ять головних книг Нового Завіту і розставили всі літери, що вони містяться в цих книгах, одну за одною в єдиний ланцюг. Утворився ланцюг з 304 805 приголосних (голосних літер в івриті немає). Потім за допомогою комп'ютера весь масив стали аналізувати за всілякими алгоритмами. Наприклад, зчитували кожну сьому літеру чи 2011-ту, змінювали відправні й навпаки. "Прочісували" весь масив за допомогою різноманітних матриць і таблиць вертикаллю й діагоналлю. Тобто застосовували всі способи, які відомі в сучасній криптографії.

Врешті-решт в масиві став виявлятися певний зміст. Після додаткового математичного опрацювання дешифрувальники почали здобувати уривки зв'язного тексту, котрий містив згадування про найрізноманітніші речі. Наприклад, в царині техніки це були згадування про перший політ братів Райт, створення телефону, автомобіля й інші винаходи. Щодо подій політичного характеру Біблія поки що нічого не повідомила. Принаймні ізраїльські вчені це не оприлюднили. Однак, за їхніми словами, коли за ключ (а точніше коротку гамму) було взято ім'я тодішнього ізраїльського прем'єр-міністра Іцхака Рабина, матриця з кроком у 4772 літери в підсумку сполучила їх до такого прогнозу: "Буде вбито". Прогноз було здобуто 1994 року, і про нього одразу ж повідомили прем'єра, але той лише посміявся з біблійного попередження. А 1995 року він, як відомо, насправді став жертвою замаху. Пророкування, на жаль, збулося. Які ще таємниці вдасться розшифрувати вченим і що внаслідок цього очікує на людство?

Останнім часом повідомляють, що ще Ньютон зробив певні розшифровування другого шару Біблії, зокрема щодо того, що певна наддержава нападе на малу саме нашого часу і що кінець світу очікується 2060 року.

Криптографія займається пошуком і дослідженням математичних методів перетворювання інформації.

Криптографія – це наука про способи перетворювання (шифрування) інформації з метою її захисту від неправочинних користувачів.

Сфера інтересів криптоаналізу – дослідження можливості дешифрування інформації без знання ключів.

Криптоаналіз – це наука про методи і способи розкривання шифрів.

Інший підхід захисту інформації від неправочинних користувачів – не приховувати власне факту передавання повідомлення, але зробити його неприступним для сторонніх. Для цього повідомлення має бути записане у такий спосіб, аби з його вмістом не міг ознайомитися ніхто, за винятком самих кореспондентів, – у цьому й полягає суть шифрування. І криптографія виникла власне як практична дисципліна, котра вивчає й розробляє способи шифрування повідомлень.

Об'єктом криптографії є інформація (новини, вміст повідомлень) в перебігу передавання її каналами зв'язку.

Слід пам'ятати, що криптографія необхідна лише для інформації, котра потребує захисту. Зазвичай в таких випадках говорять, що інформація містить таємницю, чи є захищуваною, секретною, конфіденційною. Тому, як правило, вивчення криптографії як науки розпочинають з вивчення властивостей відкритої інформації.

Криптографи дають таке означення: ***відкрита інформація*** – це незасекречена (незашифрована) інформація, призначена для передавання каналом зв'язку.

Відкрита інформація неодмінно має бути зафіксована на певному матеріальному носії (папері, фотоплівці, перфострічці тощо). У цьому разі її називають ***відкритим повідомленням***. Поняття відкритого повідомлення в криптографічній літературі розуміється подвійно: або це змістовний текст, котрий піддається смисловому читанню, або це текст, котрий підлягає зашифровуванню.

Повернімося до історії. Що жвавіше провадилося листування в суспільстві, тим більше відчувалася потреба в засобах його засекречування. Відповідно виникали усе більш складні й хитромудрі шифри. Спочатку при зацікавлених особах з'явилися шифрувальники, потім – групи з кількох шифрувальників, а потім – і цілі шифрувальні відділи. Коли обсяги підлягаючої утаємниченню інформації стали критичними, на допомогу людині було створено механічні пристрої для шифрування.

Вочевидь, що термін "криптографія" далеко відійшов від свого первісного значення – "тайнопис", "таємний лист". Сьогодні це наукова дисципліна, яка поєднує методи захисту інформаційних взаємовпливів різноманітного характеру, які спираються на перетворення даних за секретними алгоритмами, включаючи алгоритми, котрі використовують секретні параметри. Термін "інформаційний взаємовплив", чи "процес інформаційного взаємовпливу" тут позначає такий процес взаємовпливу двох і більш суб'єктів, основним змістом якого є передавання та/чи опрацьовування інформації. Приміром, за криптографічну може вважатися будь-яка функція перетворювання даних, секретна сама собою чи залежна від секретного параметра K:

$$T' = f(T), \text{ або } T' = f(T, K).$$

Перетворення T_k визначається відповідним алгоритмом і значенням параметра *K*. Ефективність зашифровування з метою захисту інформації залежить від зберігання таємниці ключа та криптостійкості шифру.

Криптостійкістю називається характеристика шифру, котра визначає його стійкість до дешифрування без знання ключа (тобто до криптоаналізу). Є кілька показників криптостійкості, серед яких:

- кількість усіх можливих ключів;
- середній час, необхідний для криптоаналізу.

Як вважають вітчизняні й зарубіжні фахівці, 90 % інформації, яка не призначена для сторонніх очей та вух, таємно знімається з апаратів і мереж телефонного, телеграфного й комп'ютерного зв'язку. Чи великі при цьому є втрати? За даними зарубіжних джерел, втрата 20 % інформації, котра становить комерційну таємницю і стала „здобиччю" конкурентів, впродовж одного-півтора місяців у майже половині випадків призводить до розорення фірми.

Припустімо, що відправник хоче надіслати повідомлення одержувачеві. Більш того, відправник прагне засекретити це повідомлення, аби ніхто, окрім одержувача, не зміг його прочитати. Для цього він повинен захистити інформацію, яка міститься в повідомленні.

Завдання захисту інформації розв'язується у три основні способи:

1 *Створити абсолютно надійний (неприступний для інших) канал зв'язку поміж абонентами.*

Одразу ж прокоментуємо, що за сучасного рівня розвинення науки й техніки створити такий канал зв'язку поміж віддаленими абонентами для неодноразового передавання великих обсягів інформації практично є нереально.

2 *Використовувати загальнодоступний канал зв'язку, але приховувати сам факт передавання інформації.*

Одразу ж зауважимо, що розробляннням засобів та методів приховування факту передавання повідомлення займається ***стеганографія***.

Приміром, в часи давньогрецького історика Геродота (V ст. до н. е.) голову раба голили, на шкірі голови писали повідомлення й, коли волосся відросталo, раба доправляли до адресата. Ще є відомий такий спосіб утаємничування письмового повідомлення. Передаваний текст "розчиняється" у повідомленні більшого розміру із зовсім "стороннім" змістом, але якщо за певним правилом вилучити з цього тексту певні символи, то можна дістати таємне повідомлення (передаване повідомлення може бути приховане також в графічному файлі).

Добре відомі є випадки, коли секретні послання записувалися невидимим *симпатичним* чорнилом (у тому числі й на краватках, носовиках, нижній білизні тощо). Чорнило знову ставало видимим після обробляння спеціальним хімічним реактивом чи освітлення променями певної частини спектра, зазвичай ультрафіолетом.

3 *Використовувати загальнодоступний канал зв'язку, але передавати ним потрібну інформацію в перетвореному у такий спосіб вигляді, аби відновити її міг лише адресат.*

Процес криптографічного перетворення відкритого тексту з метою зробити незрозумілим його зміст для сторонніх називається ***шифруванням***. Вибір конкретного типу перетворення визначається ключем зашифровування. Інакше кажучи, шифрування – це процес перетворення відкритого повідомлення на закрите (шифртекст).

Зауважимо, що шифрування й кодування – це різні речі.

При шифруванні треба знати шифр (алгоритм) і секретний ключ (тип перетворення).

При кодуванні ж немає нічого таємного, є лише певна заміна літер чи слів на заздалегідь окреслені символи. Методи кодування спрямовано НЕ НА ТЕ, аби приховати відкрите повідомлення, а НА ТЕ, аби подати його в більш зручному вигляді для передавання технічними засобами зв'язку, для зменшення довжини повідомлення, зменшення надлишковості, підвищення пропускної здатності каналу тощо.

Процес оберненого перетворення шифртексту на відкрите повідомлення на підставі ключа називається ***розшифровуванням***.

Отже, криптографія займається методами перетворювання інформації, які не дозволяли б неправочинному користувачеві вилучити її з перехоплюваних повідомлень. При цьому каналом зв'язку передається вже не сама захищувана інформація, а результат її перетворення за допомогою шифру, тобто для неправочинного користувача виникає складне завдання розкриття шифру.

Розкриття (зламування) шифру – процес здобування захищуваної інформації із зашифрованого повідомлення без знання застосованого ключа.

Однак, окрім перехоплення й розкриття шифру, неправочинний користувач може намагатися здобути захищувану інформацію багатьма іншими способами, коли криптографія просто неспроможна цю інформацію захистити (наприклад, за агентурного способу, тобто за правочинного користувача, схиленого до співробітництва; або неправочинний користувач може намагатися не здобути, а знищити чи змодифікувати в перебігу передавання захищувану інформацію тощо).

Отже, на шляху від одного правочинного користувача до іншого інформацію має бути захищувано у різноманітні способи від всіляких погроз. Неправочинний користувач прагнутиме віднайти найслабшу ланку в цьому ланцюзі, аби з найменшими витратами добутися до інформації. Тому правочинні користувачі мають враховувати "принцип рівноміцності захисту", тобто всі ланки одного ланцюга має бути захищено однаково.

Не слід забувати ще про одне: про проблему співвідношення ціни інформації, витрат на її захист та витрат на її здобуття.

Перш ніж вдаватися до захисту інформації, варто задати два запитання:

1 чи є вона для неправочинного користувача більш вартісною, аніж вартість атаки?

2 чи є вона для правочинного користувача більш вартісною, аніж вартість захисту?

Саме зазначені міркування і є вирішальними при обиранні придатних засобів захисту: фізичних, стеганографічних, криптографічних та ін.

Сучасна криптографія містить у собі чотири великих розділи:

1 Симетричні криптосистеми.

2 Криптосистеми з відкритим ключем.

3 Системи електронного підпису.

4 Керування ключами.

Про них йтиметься у другій частині цього навчального посібника.

Другу частину посібника спрямовано на вивчення сучасних шифрів з симетричним ключем. Розглянуто системи шифрування з відкритим ключем, а також питання забезпечення безпеки електронних платіжних систем.

1 ШИФРИ ПЕРЕСТАВЛЯННЯ

Шифр переставляння здійснює перетворення переставлення літер у відкритому тексті. Типовим прикладом шифру переставляння є шифр Сцитала. Зазвичай відкритий текст розбивається на відрізки однакової довжини і кожен відрізок шифрується незалежно. Нехай, наприклад, довжина відрізків дорівнює n та δ – взаємнооднозначне відбиття множини $\{1, 2, ..., n\}$ в собі. Тоді шифр переставляння впроваджується у такий спосіб: відрізок відкритого тексту $x_1...x_n$ перетворюється на відрізок шифрованого тексту $x_{\delta(1)}...x_{\delta(n)}$.

Оберемо ціле додатне число, скажімо, 5; розташуємо числа від 1 до 5 у дворядковий запис, в якому другий рядок – довільне переставляння чисел верхнього рядка:

1	2	3	4	5
3	2	5	1	4

Цю конструкцію називають підставлянням, а число 5 – його ступенем.

Зашифруємо фразу «ДО БУЛАВИ ТРЕБА ГОЛОВИ». У цій фразі 19 літер. Доповнимо її довільною літерою (наприклад Ь) до найближчого числа, кратного до 5, тобто 20. Випишемо цю доповнену фразу без пропусків, водночас розбивши її на п’ятизнакові групи:

ДОБУЛ АВИТР ЕБАГО ЛОВИЬ

Літери кожної групи переставимо відповідно до зазначеного дворядкового запису за таким правилом: перша літера ставиться на третє місце, друга – на друге, третя – на п’яте, четверта – на перше і п’ята – на четверте. Здобутий текст виписуємо без пропусків:

УОДЛБТВАРИГБЕОАИОЛЬВ

При розшифровуванні текст розбивається на групи по п’ять літер, які переставляються у зворотному порядку: перша – на четверте місце, друга – на друге, третя – на перше, четверта – на п’яте і п’ята – на третє. Ключем шифру є обране число 5 і порядок розташування чисел у нижньому рядку дворядкового запису.

1.1 Прилад Сцитала

Одним з перших фізичних приладів, які зреалізовують шифр переставляння, є так званий прилад Сцитала. Його було винайдено у давній "варварській" Спарті за часів Лікурга (V ст. до н. е.). Рим швидко скористався цим приладом. Для зашифровування тексту використовувався циліндр заздалегідь обумовленого діаметра. На циліндр намотувався тонкий ремінець з пергамента, і текст виписувався порядково вздовж осі циліндра. Потім ремінець змотувався й доправлявся одержувачеві повідомлення. Останній намотував його на циліндр

того самого ж діаметра і зчитував текст по осі циліндра. У цьому прикладі ключем шифру є діаметр циліндра та його довжина, котрі, власне кажучи, породжують дворядковий запис, аналогічний до того, що його наведено вище.

Шифр Сцитала зреалізовує один з варіантів сучасного так званого шифру маршрутного переставляння. Зміст цього шифру полягає в такому.

Відкритий текст виписується в прямокутну таблицю з n рядків та m стовпців. Припускається, що довжина тексту $t \le nm$ (у противному разі ділянка тексту, що залишилася, шифрується окремо за тим самим шифром). Якщо t є строго менше за nm, то порожні клітинки, що залишилися, заповнюються довільним набором літер абетки. Шифртекст виписується за цією таблицею заздалегідь обумовленим "маршрутом" – шляхом, що він проходить одноразово через усі клітинки таблиці. Ключем шифру є числа n та m і окреслений маршрут.

У такому трактуванні шифр Сцитала набуває описаного нижче вигляду. Нехай m – кількість обвитків ремінця на циліндрі; n – кількість літер, розташованих на одному обвитку. Тоді відкритий текст, виписаний порядково в зазначену таблицю, шифрується шляхом послідовного зчитування літер за стовпцями. Оскільки маршрут є відомий і незмінний, то ключем шифру є числа m та mn, зумовлені діаметром циліндра й довжиною ремінця. При перехопленні повідомлення (ремінця) єдиним секретним ключем є діаметр.

Винахід дешифрувального пристрою – Антисцитала – приписують великому Аристотелю. Він запропонував використовувати конусоподібний "спис", на який намотувався перехоплюваний ремінець; цей ремінець пересувався віссю доти, аж допоки не з'являвся осмислений текст.

В часи середньовіччя європейська криптографія набула сумнівного розголосу, який відлунює й дотепер. Криптографію стали ототожнювати з чорною магією, з певною формою окультизму, астрологією, алхімією, єврейською каббалою. До зашифровування інформації долучалися містичні сили. Приміром, рекомендувалося використовувати так звані "магічні квадрати".

1.2 "Магічні квадрати"

"Магічними квадратами" називають квадратні таблиці з вписаними в їхні клітинки послідовними натуральними числами, розпочинаючи від 1, що вони дають у сумі по кожному стовпцю, кожному рядку і кожній діагоналі одне й те саме число.

Кількість "магічних квадратів" швидко зростає зі збільшенням розміру квадрата. Кількість "магічних квадратів" 4×4 становить 880, а кількість "магічних квадратів" 5×5 – близько 250 000.

Уперше ці квадрати виникли в Китаї, де їм було надавано певної "магічної" сили. Наведемо приклад: у квадрат розміром 4×4 вписуються цифри від 1 до 16.

Зашифровування за "магічним квадратом" здійснюється у такий спосіб.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Наприклад, треба зашифрувати фразу: «ПРИЛІТАЮ СЬОГОДНІ». Літери цієї фрази вписуються послідовно до квадрата відповідно до записаних в них чисел, а в порожні клітинки (якщо такі є) проставляють довільні літери.

16**І**	3**И**	2**Р**	13**О**
5**І**	10**Ь**	11**О**	8**Ю**
9**С**	6**Т**	7**А**	12**Г**
4**Л**	15**Н**	14**Д**	1**П**

Після цього зашифрований текст записується вже в рядок:

ІИРОІЬОЮСТАГЛНДП

При розшифровуванні текст вписується до квадрата – й відкритий текст читається в послідовності чисел "магічного квадрата".

Даний шифр – звичайний шифр пересталяння, але вважалося, що особливої стійкості йому надає чаклунство "магічного квадрата".

1.3 Приклади розв'язування криптографічних завдань за допомогою шифрів переставляння

Шифр, перетворювання з якого змінюють лише порядок слідування символів вихідного тексту, але не змінюють їх самих, називається шифром переставляння.

1.3.1 Шифрування за допомогою класичних шифрів переставляння

Розглянемо перетворювання з шифром переставляння, призначене для зашифровування повідомлення довжиною n символів. Його можна подати за допомогою таблиці

$$\begin{matrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n, \end{matrix}$$

де i_1 – номер місця шифртексту, на котре потрапляє перша літера вихідного повідомлення за обраного перетворення; i_2 – номер місця для другої літери й т. д. У верхньому рядку таблиці виписано одне за одним числа від 1 до n, а в нижньому – ті ж самі числа, але в довільному порядку. Така таблиця називається підставлянням ступеня n.

Знаючи підставляння, котре задає перетворення, можна здійснювати як зашифровування, так і розшифровування тексту.

Наприклад, якщо для перетворення використовується підставляння

1 2 3 4 5
5 2 3 1 4

і відповідно до нього зашифровується слово **УЧЕНЬ**, то виходить **НЧЕЬУ**.

1.3.2 Шифрування за допомогою табличних шифрів переставляння

Одним з найпримітивніших табличних шифрів переставляння є просте переставляння, для якого за ключ слугує розмір таблиці. Цей метод шифрування є подібний до шифру Сцитала.

Наприклад, повідомлення

МАЄШ ГОЛОВУ, МАЙ ЖЕ РОЗУМ

записується в таблицю по черзі по стовпцях. Розглянемо результат заповнення таблиці з п’яти рядків і чотирьох стовпців:

М	**О**	**М**	**Р**
А	**Л**	**А**	**О**
Е	**О**	**Й**	**З**
Ш	**В**	**Ж**	**У**
Г	**У**	**Е**	**М**

Після заповнення таблиці текстом повідомлення по стовпцях для формування шифртексту зчитують уміст таблиці по рядках. Якщо шифртекст записувати групами по п’ять літер, виходить таке шифроване повідомлення:

МОМРА ЛАОЕО ЙЗШВЖ УГУЕМ

Природно, відправник і одержувач повідомлення повинні заздалегідь домовитися про спільний ключ у вигляді розміру таблиці. Слід зауважити, що сполучення літер шифртексту в п’ятилітерні групи не входить до ключа шифру і здійснюється для зручності запису шифртексту. При розшифровуванні дії виконуються у зворотному порядку.

1.3.3 Шифрування за допомогою шифрів маршрутного переставляння

Широкого розповсюдження набули шифри переставляння, котрі використовують певну геометричну фігуру. Перетворення з цього шифру полягають у тому, що до фігури вихідний текст уписується в перебігу одного маршруту, а потім – в перебігу іншого – виписується з неї. Такий шифр називають ***маршрутним переставлянням***. Наприклад, можна вписувати вихідне повідомлення до прямокутної таблиці, обравши такий маршрут: по горизонталі, розпочинаючи з лівого верхнього кута по черзі в напрямках ліворуч → праворуч та праворуч → ліворуч. В порожні клітинки проставляють довільні літери. Виписуватимемо ж повідомлення за іншим маршрутом: по вертикалі, розпочинаючи з верхнього правого кута і рухаючись по черзі зверху донизу і знизу догори.

Зашифруємо, наприклад, зазначеним способом фразу:

ПРИКЛАД МАРШРУТНОГО ПЕРЕСТАВЛЯННЯ

Використовуючи прямокутник розміру 4×8, дістанемо таблицю:

П	Р	И	К	Л	А	Д	М
О	Н	Т	У	Р	Ш	Р	А
Г	О	П	Е	Р	Е	С	Т
Ь	Я	Н	Н	Я	Л	В	А

Зашифрована фраза має вигляд:

МАТАВСРДАШЕЛЯРРЛКУЕННПТИРНОЯЬГОП

Теоретично маршрути можуть бути значно більш витонченими, однак заплутаність маршрутів ускладнює використання таких шифрів.

1.3.4 Шифрування за допомогою шифрів одиночного переставляння за ключем

Метод шифрування, називаний ***одиночним переставлянням за ключем***, полягає в тім, що стовпці таблиці переставляються за ключовим словом, фразою чи набором чисел довжиною в рядок таблиці.

Застосуємо за ключ, наприклад, слово ПЕЛИКАН. Заповнимо текстом повідомлення і ключовим словом таблицю:

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Після переставляння дістанемо:

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
О	А	А	Д	Р	Н	Е
В	Т	Е	Ь	И	О	Р
П	О	Т	М	Б	Ч	М
О	Р	С	О	Ы	Ь	И

У верхньому рядку даної таблиці записано ключ, а номери під літерами ключа визначено відповідно до природного порядку відповідних літер ключа в абетці. Якби в ключі зустрілися однакові літери, їх було б пронумеровано в порядку ліворуч $\rightarrow$ праворуч.

У здобутій таблиці стовпці переставлено відповідно до упорядкованих номерів літер ключа. При зчитуванні її вмісту по рядках і записуванні шифртексту групами по п’ять літер дістанемо шифроване повідомлення:

ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЬЬИ

Для забезпечення додаткового утаємничення можна вдруге зашифрувати повідомлення, яке вже пройшло шифрування. Такий метод шифрування називається ***подвійним переставлянням*.** У разі подвійного переставляння стовпців і рядків таблиці переставляння визначаються окремо для стовпців і окремо для рядків. Спочатку в таблицю записується текст повідомлення, а потім по черзі переставляються стовпці, а за ними рядки. При розшифровуванні порядок переставлянь має бути зворотним.

1.3.5 Шифрування за допомогою поворотних ґрат

Для використання шифру, називаного поворотними ґратами, виготовляється трафарет з прямокутного аркуша паперу розміру $2m \times 2k$ клітинок. У трафареті вирізано mk клітинок у такий спосіб, що при накладенні його на чистий аркуш паперу того самого розміру у чотири можливих способи його вирізи цілковито покривають усю площу аркуша.

Літери повідомлення послідовно вписуються у вирізи трафарету (по рядках, у кожнім рядку в напрямку ліворуч→праворуч) при кожнім з чотирьох його можливих положень у заздалегідь установленому порядку.

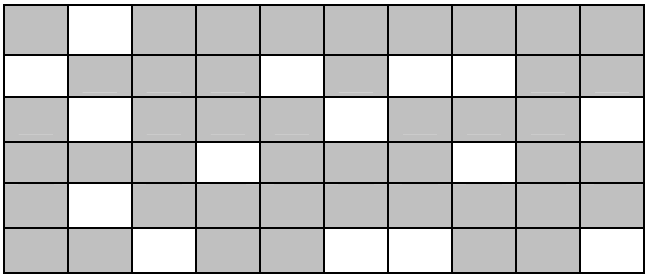


Рисунок 1.1 Шифрування за допомогою поворотних ґрат

Пояснімо процес шифрування на прикладі. Нехай за ключ використовуються ґрати 6×10, які наведено на рис. 1.1.

Зашифруємо за їхньою допомогою текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМС-
ЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ

Наклавши ґрати на аркуш паперу, вписуємо перші п’ятнадцять (за кількістю вирізів) літер повідомлення:

ШИФРРЕШЕТКАЯВЛЯ …

Знявши ґрати, ми побачимо текст, поданий на рис. 1.2. Повернімо ґрати на 180°. У „віконечках” з’являться нові, ще не заповнені клітинки. Вписуємо в них наступні п’ятнадцять літер. Вийде запис, наведений на рис. 1.3. Потім повертаємо ґрати на інший бік і зашифровуємо залишок тексту в аналогічний спосіб (рис. 1.4 та 1.5).

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я			В	Л			Я

Рисунок 1.2

Е	Ш		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
Т			Т	Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

Рисунок 1.3

Е	Ш	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

Рисунок 1.4

Е	Ш	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	Е
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

Рисунок 1.5

Одержувач повідомлення, котрий має точно такі самі ґрати, без утруднень прочитає вихідний текст, накладаючи ґрати на шифртекст по порядку у чотири способи.

Можна довести, що кількість можливих трафаретів, тобто кількість ключів шифру "ґрати", становить $T = 4^{mk}$. Цей шифр призначено для повідомлень довжини $n = 4mk$. Кількість всіх переставлянь у тексті такої довжини становитиме $(4mk)!$, що в багато разів більше за кількість T. Однак вже при розмірі трафарету 8×8 кількість можливих ґрат перевершує чотири мільярди.

1.3.6 Практичне застосовування шифрів переставляння в системах зв'язку

Практичну реалізацію шифру переставляння в системах зв'язку може бути подано на такому прикладі.

Особливістю телефонного зв'язку є те, що акустичний сигнал у телефонному терміналі перетворюється на електричний і потім після опрацьовування й посилення передається лініями зв'язку. На приймальному кінці електричний сигнал знову перетворюється на акустичний; при цьому вихідна форма сигналу більш-менш зберігається. Акустичний і, відповідно, електричний сигнали схарактеризовуються частотним спектром. Їх можна розглядати в розгорненні в часі й за спектром.

Відомі є кілька типових перетворювань аналогового сигналу, котрі може бути легко зреалізовано інженерними методами. Зазначимо головні з них.

Переставляння частот. За допомогою системи фільтрів уся ширина смуги стандартного телефонного каналу може бути поділена на певну кількість частотних смуг, котрі потім може бути переставлено поміж собою (рис. 1.6 та 1.7).

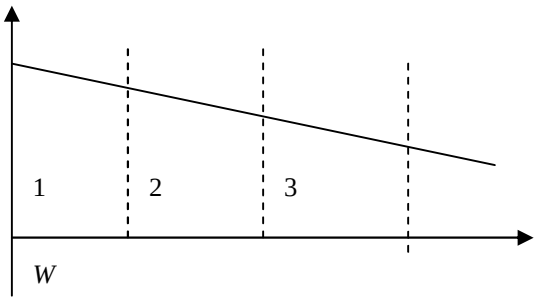


Рисунок 1.6

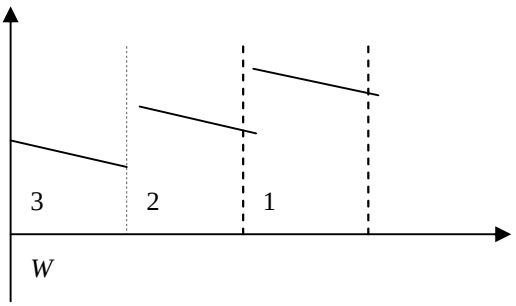


Рисунок 1.7

Найпростіший скремблер обмежує захист уведенням подібних найпростіших частотних перетворень. Серійний скремблер переставляє діапазони 250...675 Гц, 675...1100 Гц, 1100...1525 Гц та 1950...2375 Гц.

У даній схемі на вхід вузла накладання шифру подається одне й те саме керування, що воно зорганізовує переставляння.

Інвертування спектра. Більш складні скремблери додатково здійснюють інвертування спектра (рис. 1.8).

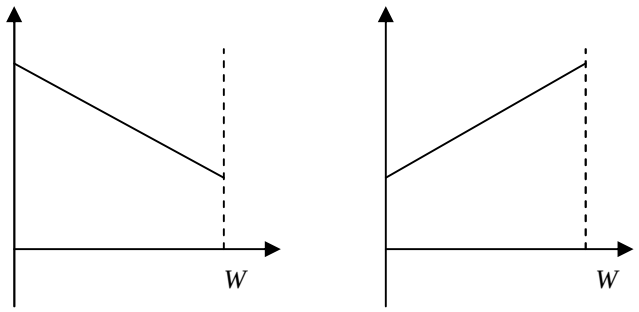


Рисунок 1.8

Частотно-часові переставляння. Ще більш складні системи розбивають сигнал на часовому інтервалі 60...500 мс і на кожнім інтервалі використовують у комбінації власні аналогові перетворення. Зміною перетворень у різні часові інтервали керує послідовність, яка надходить на вузол накладання шифру з блока ускладнювання. Той, хто просто послухає дешифроване аналоговим сигналом мовлення, почує якийсь булькіт, шум. Про складність завдання зашифрововування й розшифровування аналогових повідомлень писав Солженіцин у своєму «В круге первом»: «…Клиппирование, демпфирование, амплитудное сжатие, электронное дифференцирование и интегрирование привольной человеческой речи были таким же инженерным издевательством над ней, как если бы кто-нибудь взялся расчленить Новый Афон или Гурзуф на кубики вещества, втиснуть в миллиард спичечных коробков, перевезти самолетом в Нерчинск, на новом месте распутать, неотличимо собрать и воссоздать субтропики, шум прибоя, южный воздух и лунный свет. То же, в некоторых импульсах, надо было сделать и с речью, даже воссоздать ее так, чтобы не только было понятно, но Хозяин мог бы по голосу узнать, с кем говорит…». Так само барвисто й дещо зневажливо Солженіцин відгукувався про власне роботу з розробляння вітчиз-

няних засобів захисту телефонної інформації. Однак тут він був неправий. На думку висококваліфікованих фахівців, того часу робота йшла вельми цілеспрямовано й апаратуру насправді випускали в призначений термін. Це – апаратура часової стійкості. За наявності спецтехніки типу видимого мовлення зміст перемов удається відновити. Якщо забути про інверсії, то ми маємо шифр переставляння. Апаратура видимого мовлення зводить завдання дешифрування до відновлення певного рисунка, зашифрованого шифром переставляння.

Для гарантованого засекречування телефонного мовлення його спочатку оцифровують – переводять у двійкову послідовність, а потім опрацьовують так само, як і будь-яке текстове повідомлення.

На практиці використовується апаратура як аналогового, так і цифрового засекречування. Цифрова апаратура забезпечує гарантовану надійність захисту, але вона є більш вимоглива до каналів зв'язку. Аналогова апаратура є менш стійка, але більш дешева, більш портативна, менш вимоглива до каналів зв'язку.

1.4 Завдання для самоперевірки

Завдання 1.1 Розшифруйте повідомлення Я ′ В О З К З, здобуте внаслідок перетворення за допомогою підставляння

1	2	3	4	5	6	7
4	3	2	6	1	7	5

Завдання 1.2 Зашифруйте за допомогою „магічного квадрата" 4×4 фразу: «БЕРЕЖІТЬ ДРУЗІВ!».

Завдання 1.3 Розшифруйте повідомлення

ОИРМ ЕОСЮ ВТАЬ ЛГОП,

здобуте за допомогою „магічного квадрата" 4×4.

Завдання 1.4 Зашифруйте методом подвійного переставляння повідомлення

ПОЧИНАТИ ПЕРЕДАЧУ

Ключем до шифру слугує послідовність номерів стовпців 4132 й номерів рядків 3142 вихідної таблиці.

Шифртекст зчитувати порядково блоками по чотири літери.

Завдання 1.5 Шифртекст

ТЮАЕ ООГМ РЛИП ОЬСВ

здобуто методом подвійного переставляння з ключем, наведеним у завданні 1.4. Віднайти вихідне повідомлення.

2 ШИФРИ ПРОСТОЇ ЗАМІНИ (ОДНОАБЕТКОВОГО ПІДСТАВЛЯННЯ)

Як відкритий текст, так і шифртекст утворюються з літер, котрі входять у кінцеву множину символів, називаних *абеткою*. Прикладами абеток є кінцева множина усіх великих літер, кінцева множина усіх великих і малих літер та цифр і т. п. У загальному вигляді певну абетку $\sum$ можна подати в такий спосіб:

$$\sum = \{a_0 + a_1 + a_2 + \ldots + a_{m-1}\}.$$

Поєднуючи за певним правилом літери з абетки $\sum$, можна створити нові абетки:

- абетку $\sum^2$, яка має m^2 біграм a_0a_0, a_0a_1, …, $a_{m-1}a_{m-1}$;
- абетку $\sum^3$, яка має m^3 триграм $a_0a_0a_0$, $a_0a_0a_1$,…, $a_{m-1}a_{m-1}a_{m-1}$.

Тоді, поєднуючи по n літер, дістаємо абетку $\sum^n$**,** яка має m^n n-грам.

Наприклад, англійська абетка

$$\sum = \{\text{ABCDEFGH … WXYZ}\},$$

яка містить $m = 26$ літер, дозволяє згенерувати за допомогою операції конкатенації абетку з $26^2 = 676$ біграм

AA, AB, …, YZ, ZZ,

абетку з $26^3 = 17576$ триграм

AAA, AAB, …, ZZY, ZZZ

тощо.

При виконанні криптографічних перетворень корисно замінювати літери абетки на цілі числа – 0, 1, 2, 3, ... Це дозволяє спростити виконання необхідних алгебраїчних маніпуляцій. Наприклад, можна установити взаємно однозначну відповідність поміж українською абеткою

$$\sum_{\text{укр}} = \{\text{АБВГГ′Д … ЮЯ}\}$$

та множиною цілих

$$\overline{Z}_{33} = \{0, 1, 2, 3, \ldots, 32\};$$

поміж російською абеткою

$$\sum_{\text{рос}} = \{\text{АБВГДЕ … ЮЯ}\}$$

та множиною цілих

$$\overline{Z}_{32} = \{0, 1, 2, 3, \ldots, 31\};$$

поміж англійською абеткою

$$\sum_{\text{англ}} = \{\text{ABCDEF … YZ}\}$$

та множиною цілих

$$\overline{Z}_{26} = \{0, 1, 2, 3, \ldots, 25\}$$

(див. табл. 2.1, 2.2 та 2.3).

Надалі буде зазвичай використовуватися абетка

$$\overline{Z}_m = \{0, 1, 2, 3, \ldots, m-1\},$$

яка містить m «літер» (у вигляді чисел).

Заміна літер традиційної абетки числами дозволяє більш чітко сформулювати основні концепції та прийоми криптографічних перетворень. Водночас у більшості ілюстрацій використовуватиметься абетка природної мови.

Таблиця 2.1 – Відповідність поміж українською абеткою та множиною цілих $\overline{Z}_{33} = \{0, 1, 2, 3, \ldots, 32\}$

Літера	Число	Літера	Число	Літера	Число	Літера	Число
А	0	З	9	О	18	Ч	27
Б	1	Й	10	П	19	Ш	28
В	2	І	11	Р	20	Щ	29
Г	3	Ї	12	С	21	Ь	30
Ґ	4	Й	13	Т	22	Ю	31
Д	5	К	14	У	23	Я	32
Е	6	Л	15	Ф	24		
Є	7	М	16	Х	25		
Ж	8	Н	17	Ц	26		

Таблиця 2.2 – Відповідність поміж російською абеткою та множиною цілих $\overline{Z}_{32} = \{0, 1, 2, 3, \ldots, 31\}$

Літера	Число	Літера	Число	Літера	Число	Літера	Число
А	0	И	8	Р	16	Ш	24
Б	1	Й	9	С	17	Щ	25
В	2	К	10	Т	18	Ь	26
Г	3	Л	11	У	19	Ы	27
Д	4	М	12	Ф	20	Ъ	28
Е	5	Н	13	Х	21	Э	29
Ж	6	О	14	Ц	22	Ю	30
З	7	П	15	Ч	23	Я	31

Таблиця 2.3 – Відповідність поміж англійською абеткою та множиною цілих $\overline{Z}_{26} = \{0, 1, 2, 3, \ldots, 25\}$

Літера	Число	Літера	Число	Літера	Число
A	0	J	9	S	18
B	1	K	10	T	19
C	2	L	11	U	20
D	3	M	12	V	21
E	4	N	13	W	22
F	5	O	14	X	23
G	6	P	15	Y	24
H	7	Q	16	Z	25
I	8	R	17		

Текст з n літерами абетки $\overline{Z}_m$ можна розглядати як n-граму

$$\bar{x} = (x_0, x_1, x_2, \ldots, x_{n-1}),$$

де $x_i \in \overline{Z}_m$, $0 \le i < n$, для певного цілого $n = 1, 2, 3, \ldots$

Через $\overline{Z}_{m,n}$ позначатимемо множину n-грам, утворених з літер множини $\overline{Z}_m$.

Криптографічне перетворення E являє собою сукупність перетворень

$$E = \{E^{(n)}: 1 \le n < \infty\};$$

$$E^{(n)}: \overline{Z}_{m,n} \to \overline{Z}_{m,n}.$$

Перетворення $E^{(n)}$ визначає, як кожна n-грама відкритого тексту $\bar{x} \in \overline{Z}_{m,n}$ замінюється на n -граму шифртексту $\bar{y}$, тобто

$$\bar{y} = E^{(n)}(\bar{x}), \ \bar{x}, \bar{y} \in \overline{Z}_{m,n};$$

при цьому неодмінною є вимога взаємної однозначності перетворення $E^{(n)}$ на множину $\overline{Z}_{m,n}$.

Криптографічна система може трактуватися як сімейство криптографічних перетворень

$$\overline{E} = \{E_K : K \in \overline{K}\},$$

позначених параметром K, називаним *ключем*.

Множина значень ключа утворює ключовий простір $\overline{K}$.

Класичні методи шифрування відрізняються симетричною функцією зашифровування. До них відносять шифри переставляння, шифри простої й складної заміни, а також певні їхні модифікації й комбінації. Слід зазначити, що комбінації шифрів переставлянь й шифрів заміни утворюють усе різноманіття застосовуваних на практиці симетричних шифрів.

Відомості про шифри кожної групи, котрі наводяться в посібнику, подаються за можливості в порядку, що дозволяє поступово входити в сферу криптографії. Як відомо, вельми складно зрозуміти концептуальну схему науки, її моделі й методи дослідження, якщо не мати хоча б загального уявлення про історію розвинення цієї науки.

Великий вплив на розвинення сучасної криптографії справили роботи американського математика Клода Шеннона, котрі з'явилися в середині XX сторіччя. У цих роботах закладено основи теорії інформації, а також було розроблено математичний апарат для досліджень у багатьох областях науки, пов'язаних з інформацією. Більш того, узвичаєно вважати, що теорія інформації як наука народилася 1948 року після опублікування праці К. Шеннона "Математична теорія зв'язку".

У своїй праці "Теорія зв'язку в секретних системах" Клод Шеннон узагальнив накопичений до нього досвід розробляння шифрів. Виявилося, що навіть у надто складних шифрах як типові компоненти можна виокремити такі прості шифри, як шифри переставляння, шифри заміни чи їхні сполучення.

Шифр заміни є найпростішим та найбільш популярним шифром. Як випливає з самої назви, шифр заміни здійснює перетворення (заміну) літер чи інших "частин" відкритого тексту на аналогічні "частини" шифрованого тексту.

Легко навести математичний опис шифру заміни. Нехай X и Y – дві абетки (відкритого й шифрованного тексту відповідно), котрі складаються з однакової кількості символів. Нехай також $g : X \to Y$ – взаємно однозначне відбиття X в Y. Тоді шифр заміни впливає у такий спосіб: відкритий текст $x_1x_2\ldots x_n$ перетворюється на шифрований текст $g(x_1)\, g(x_2)\ldots g(x_n)$.

2.1 Шифр Цезаря

Історичним прикладом шифру заміни є шифр Цезаря (I ст. до н. е.), описаний істориком давнього Риму Светонієм. Гай Юлій Цезар використовував у своєму листуванні шифр власного винайдення. Стосовно сучасної української мови він полягав у такому. Виписувалась абетка: А, Б, В, Г, …; потім під нею виписувалась та ж сама абетка, але з циклічним зсуненням на три літери ліворуч:

А Б В Г Ґ Д Е Є Ж З И І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ь Ю Я
Г Ґ Д Е Є Ж З И І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ю Я А Б В Г

При зашифровуванні літера А замінювалася на літеру Г, В – замінювалася на Д, У – на Ц й т. д. Приміром, слово РИМ перетворювалося на УЙП. Одержувач повідомлення УЙП шукав ці літери в нижньому рядку і по літерах над ними відновлював вихідне слово РИМ. Ключем у шифрі Цезаря є величина зсунення нижнього рядка абетки.

Природне розвинення шифру Цезаря є очевидне: нижній рядок дворядкового запису літер абетки може бути з довільним розташуванням цих літер. Якщо в абетковому розташуванні літер у нижньому рядку існує всього 33 варіанти ключів (кількість літер в українській абетці), то за їхнього довільного розташування кількість ключів стає величезною. Вона становить 33! (33 факторіали), тобто приблизно 10^{35}. Цей момент є надто важливий. Якщо неправочинний користувач здогадався чи одержав відомості про використаний шифр (а шифри використовуються тривалого часу), то він може спробувати перебрати усі варіанти можливих секретних ключів при дешифруванні перехопленої криптограми. Навряд чи віднайдеться дешифрувальник, котрий навіть у наші дні обрав би цей шлях дешифрування. Однак у часи Цезаря, коли панувала суцільна неграмотність населення, сама можливість побачити осмислене повідомлення за "абракадаброю", навіть складеною зі знайомих літер, здавалася нездійсненною. Принаймні давньоримський історик Светоній не наводить випадків дешифрування переписування Цезаря. Нагадаємо, що сам Цезар усе життя використовував один і той самий ключ (зсунення – 3). Цим шифром він користувався, зокрема, для обміну посланнями з Цицероном.

У художній літературі класичним прикладом шифру заміни є відомий шифр "Танцюючі чоловічки" (К. Дойла). У ньому літери тексту замінювалися на символічні фігурки людей. Ключем такого шифру були постави чоловічків, котрі замінювали літери.

Існували й інші способи захисту інформації, розроблені в античні часи.

2.2 Винаходи Енея

Одне з перших історичних імен, котре згадується у зв'язку з криптографією, це ім'я Енея – легендарного полководця, захисника Трої. В царині тайнопису Енеєві належать два винаходи.

2.2.1 Диск Енея

Перший з винаходів – так званий "диск Енея". Принципи його побудови й дії є вельми прості. На диску діаметром 10...15 см і товщиною 1...2 см висверд-лювалися отвори за кількістю літер абетки. В центрі диска містилася "котушка" з намотаною на ній ниткою потрібної довжини. При зашифровуванні нитка "витягалася" з котушки і послідовно протягалася через отвори відповідно до літер зашифровуваного тексту. Диск був посланням. Одержувач послання послідовно витягав нитку з отворів, що дозволяло йому зчитувати передаване повідомлення, але в зворотному порядку слідування літер. При перехоплянні диска неправочинний користувач мав можливість прочитати повідомлення у той самий спосіб, що й одержувач. Але Еней передбачав можливість легкого знищення передаваного повідомлення в разі загрози захоплення диска. Для запобігання цьому досить було висмикнути "котушку" із закріпленим на ній кінцем нитки до повного виходу всієї нитки з отворів диска.

2.2.2 Лінійка Енея

Ідея Енея була використана при створюванні й інших оригінальних шифрів заміни. Наприклад, в одному з варіантів замість диска використовувалася лінійка з кількістю отворів, дорівнюваних кількості літер абетки. Кожен отвір позначався власною літерою; літери по отворах розташовувалися в довільному порядку. До лінійки було прикріплено котушку з намотаною на неї ниткою. Поруч з котушкою був проріз. При шифруванні нитка протягалася через проріз, а потім через отвір, котрий відповідав першій літері зашифровуваного тексту, при цьому на нитці зав'язувався вузлик у місці проходження її через отвір; потім нитка поверталася до прорізу – й аналогічно зашифровувалася друга літера тексту й т. д.

Після закінчення зашифровування нитка витягалася і передавалася одержувачеві повідомлення. Той, маючи ідентичну лінійку, протягав нитку через прорізи отворів, зумовлених вузлами, і відновлював вихідний текст за літерами отворів. Цей пристрій дістав назву ***лінійки Енея***. Шифр, зреалізовуваний лінійкою Енея, є одним з прикладів шифру заміни: у ньому літери замінюються на певній відстані поміж вузликами на нитці. Ключем шифру був порядок розташування літер по отворах у лінійці. Неправочинний користувач, котрий здобув нитку (навіть маючи лінійку, але без нанесених літер), не міг прочитати передаване повідомлення.

Аналогічне до лінійки Енея так зване "вузелкове письмо" ("кіпу") набуло поширення в індіанців Центральної Америки. Свої повідомлення вони також

передавали у вигляді нитки, на якій зав'язувалися різнобарвні вузлики, котрі визначали зміст повідомлення.

2.2.3 Книжковий шифр

Помітним внеском Енея до криптографії є запропонований ним так званий ***книжковий шифр***, описаний у творі "Про оборону укріплених місць". Еней запропонував проколювати малопомітні дірки в книзі чи в іншому документі над літерами таємного повідомлення. Варто відзначити, що в першій світовій війні минулого сторіччя німецькі шпигуни використовували аналогічний шифр, замінивши дірки на крапки, які наносилися спеціальними чорнилами на літери газетного тексту.

Винайдення друкарства Йоганном Гуттенбергом (1440, Німеччина, м. Майнц) помітно позначилось на підвищенні грамотності населення. Пожвавішало листування, став зростати обсяг обміну секретною інформацією. З іншого боку, доступні для всіх книги самі собою спричинилися до застосовування книжкових шифрів, використовуваних і в даний час.

Суть книжкового шифру полягає в заміні літер на номер рядка і номер цієї літери в рядку в заздалегідь обумовленій сторінці певної книги. Ключем такого шифру є сама книга й використовувана сторінка в ній. Існує чимало способів використання книги для таємного обміну повідомленнями. Наприклад, якщо адресати заздалегідь домовилися поміж собою про використання дублікатів однієї й тієї самої книги як ключа шифру, то їхні таємні послання могли б складатися з таких елементарних одиниць: $n|m|t$, де n – номер сторінки книги, m – номер рядка, t – номер літери в рядку; по цих літерах і читається таємне послання. Поряд з нумерацією літер можуть використовуватися позначення слів і навіть цілих фраз.

Книжковий шифр став "довгожителем" і застосовувався навіть у часи другої світової війни минулого сторіччя.

2.3 Полібіанський квадрат

Ще один винахід древніх греків – так званий квадрат Полібія (Полібій – грецький державний діяч, полководець, історик, III сторіччя до н. е.). Стосовно сучасної латинської абетки з 26 літер шифрування за цим квадратом здійснюється у такий спосіб. До квадрата розміром 5×5 клітинок виписуються всі літери абетки, при цьому літери I та J не розрізнюються (J ототожнюється з літерою I):

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Зашифровувана літера замінюється на координати квадрата, у якому вона записана. Приміром, B замінюється на AB, F – на BA, R – на DB і т. д. При розшифровуванні кожна така пара визначає відповідну літеру повідомлення. Зауважимо, що секретом у даному разі є сам спосіб замінювання літер. Ключ у цій системі є відсутній, оскільки використовується фіксований порядок слідування літер.

Ускладнений варіант шифру Полібія полягає в записуванні літер до квадрата у довільному (неабетковому) порядку. Цей довільний порядок і є ключем. Тут, однак, виникла й певна незручність. Довільний порядок літер важко запам'ятати, тому користувачеві шифру було необхідно постійно мати при собі ключ – квадрат. Виникла небезпека щодо таємного ознайомлення з цим ключем сторонніх осіб. Як компромісне рішення в якості ключа було запропоновано пароль. Легко запам'ятовуваний пароль виписувався без повторювання літер у квадрат; у клітинки, котрі залишилися порожніми, за абеткою виписувалися літери абетки, відсутні в паролі. Приміром, нехай паролем є слово THE TABLE. Тоді квадрат має вигляд

T	**H**	**E**	**A**	**B**
L	**C**	**D**	**F**	**G**
I	**K**	**M**	**N**	**O**
P	**Q**	**R**	**S**	**U**
V	**W**	**X**	**Y**	**Z**

Такий квадрат уже не треба мати при собі. Досить запам'ятати ключ-пароль. Зауважимо до речі, що в такий самий спосіб можна запам'ятовувати порядок розташування літер при використанні лінійки Енея, а також шифру заміни Цезаря (за довільного розташування літер у нижньому рядку). Цікаве употужнення шифру Полібія було запропоновано одним криптографом-аматором вже XIX сторіччя. Зміст цього ускладнення з'ясуємо на прикладі.

Нехай маємо такий квадрат Полібія:

	1	**2**	**3**	**4**	**5**
1	**E**	**K**	**T**	**L**	**B**
2	**H**	**I,J**	**A**	**D**	**U**
3	**M**	**S**	**G**	**C**	**V**
4	**F**	**P**	**Q**	**R**	**W**
5	**O**	**Y**	**X**	**Z**	**N**

Зашифруємо за ним слово THE APPLE. Дістанемо шифрований текст:

13.21.11.23.42.42.14.11. (2.1)

На цьому зашифровування за Полібієм завершено. Це був шифр простої заміни типу шифру Цезаря, в якому кожна літера відкритого тексту замінювалася на

певне двознакове десяткове число, і ця заміна не змінювалася по всьому тексту. Кількість ключів цього шифру дорівнює 25!

Ускладнений варіант полягає в такому. Здобутий первинний шифртекст зашифровується вдруге. При цьому він виписується без розбивання на пари:

1321112342421411 (2.2)

Здобута послідовність цифр зсувається циклічно ліворуч на один крок:

3211123424214111

Ця послідовність знову розбивається на біграми:

32.11.12.34.24.21.41.11.

й за таблицею замінюється на остаточний шифртекст:

SEKCDHFE (2.3)

Кількість ключів у цьому шифрі залишається тією самою (25!), але він є вже значно стійкіший. Зауважимо, що цей шифр вже не є шифром простої заміни (літера E відкритого тексту переходить у різні літери: K, E; літера P – у літери D, H). Було виявлено й негативний момент. Якщо в шифрі простої заміни шифртекст буде написано з однією помилкою (наприклад у тексті (2.1) замість четвертої літери 23 буде написано 32), то розшифрований текст міститиме лише одну помилку: THE SPPLE, що вона легко виправляється одержувачем повідомлення. Якщо ж у тексті (2.3) буде спотворено четверту літеру (літеру C замінено, приміром, на K), то в розшифрованому тексті буде вже два спотворення: THE HIPLE, що вже утруднює відновлення вихідного повідомлення.

Аналогічно обстоїть справа з помилками виду "пропускання літер". Нехай у тексті (2.3) пропущено літеру C. Шифртекст набере вигляду SEKDHFE, чи

32.11.12.24.21.41.11.

Після розшифровування здобудемо THE IPLE, тобто поряд з пропущенням літери в розширеному тексті наявне й спотворення іншої літери. За пропущення в (2.3) першої літери при розшифровуванні здобудемо EE APPLE.

Слід зауважити, що в дещо зміненому вигляді шифр Полібія добувся до наших днів і дістав своєрідної назви "тюремний шифр". Для його використання потрібно знати лише природний порядок розташування літер абетки (як у зазначеному вище прикладі квадрата Полібія для англійської мови). Сторони квадрата позначаються не літерами (ABCDE), а цифрами (12345). Цифра 3, наприклад, передається шляхом потрійного стукоту. При передаванні літери спочатку "відстукується" цифра, котра відповідає рядкові, в якому міститься літера, а потім – номер відповідного стовпця. Наприклад, літера F передається подвійним стукотом (другий рядок) і потім – одноразовим (перший стовпець).

Із застосовуванням цього шифру пов’язано певні історичні казуси. Приміром, декабристи, впроваджені до в’язниці після невдалого повстання, не спромоглися встановити зв’язок з князем Одоєвським, який перебував у „одиночці”.

Виявилося, що князь (добре освічена для свого часу людина) не пам'ятав природного порядку розташування літер у російській та французькій абетках (іншими мовами він не володів). Декабристи для російської абетки використовували прямокутник розміром 5×6 (5 рядків і 6 стовпців) і скорочену до 30 літер абетку.

„Тюремний шифр", строго кажучи, – не шифр, а спосіб перекодовування повідомлення з метою його приведення до вигляду, зручного для передавання „каналом зв'язку" (через стінку). Річ у тім, що в таблиці використовувався природний порядок розташування літер абетки. Отже, секретом є сам шифр (а не ключ), як у Полібія.

2.4 Спосіб шифрування Тритемія та його застосовування

У XV сторіччі абат Тритемій (Німеччина) зробив дві новаторські пропозиції в царині криптографії: він запропонував шифр "Аве Марія" й шифр, на підставі ключа, котрий періодично зсувається.

Шифр "Аве Марія" грунтовано на принципі заміни літер зашифровуваного тексту на заздалегідь обумовлені слова. З цих слів складалося зовнішньо "безневинне" повідомлення. Наведемо приклад.

Замінимо літери Н, І на такі слова:

Н = *ЗЕЛЕНИЙ, МІЙ*; *БІЛЯ*
І = *КЛЮЧ, МОРЕ, ГАЙ*

Тоді негативна секретна відповідь **НІ** на задане запитання може мати кілька "безневинних" варіантів: *Біля моря, Мій ключ, Зелений гай.*

Найбільш вагома пропозиція Тритемія щодо захисту інформації, котра дійшла до наших днів, полягає у створеній ним таблиці – таблиці Тритемія. Еквівалент її для англійської абетки наведено в додатку А.

У додатку А перший рядок є водночас і рядком літер відкритого тексту. Перша літера тексту зашифровується за першим рядком, друга літера – за другим рядком і т. д.; після використання останнього рядка – знову повертаються до першого рядка. Приміром, слово "fight" (боротьба) набуває вигляду "fjikx".

Зреалізовування таблиці Тритемія не потребувало використання якихось механічних пристосувань; шифрабетка з кожним кроком зашифровування зсувається на одиницю ліворуч. Однак у первинному варіанті в шифрі Тритемія був відсутній ключ. Секретом був сам спосіб шифрування. Надалі ускладнювання шифру пішло двома шляхами:

- уведення довільного порядку розташовування літер вихідної абетки зашифровуваного тексту замість лексикографічно упорядкованої абетки;
- застосовування ускладнюваного порядку вибору рядків таблиці при зашифровуванні.

Ці ускладнення дозволили застосовувати ключові множини значного обсягу. Відзначимо, що шифр простої заміни є варіантом шифру Тритемія: у ньому всі літери зашифровуються за одним і тим самим рядком таблиці.

2.4.1 Шифр Белазо

Наступний крок у розвиненні запропонованого Тритемієм способу шифрування було зроблено італійцем Джованні Белазо. 1553 року виходить друком його брошура "Шифр сеньйора Белазо". У цьому шифрі ключем був так званий пароль – легко запам'ятовувані фраза чи слово. Пароль записувався періодично над літерами відкритого тексту. Літера пароля, розміщена над відповідною літерою відкритого тексту, зазначала номер рядка в таблиці Тритемія, за якою треба було проводити заміну (зашифровування) цієї літери. Отже, якщо паролем є слово ROI, то при зашифровуванні слова FIGHT здобуваємо WWOYH. Аналогічні ідеї щодо зашифровування використовуються й сьогодні.

2.4.2 Шифр «братерства франкмасонів»

Шифр "братерства франкмасонів", чи "вільних каменярів", що вони використовували для спілкування поміж собою, за сучасними поняттями і всупереч поширеній думці, зовсім не є стійкий, але становить певний інтерес. Наведемо невеликий приклад (стосовно англійської мови). Нарисуємо три фігури такого вигляду:

A:	**B:**	**C:**
D:	**E:**	**F:**
G:	**H:**	**I:**

J.	**K.**	**L.**
M.	**N.**	**O.**
P.	**Q.**	**R.**

S	**T**	**U**
V	**W**	**X**
Y	**Z**	

Відповідно до цих фігур літери набувають такого геометричного подання:

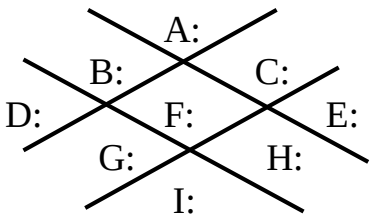
A= B= C= J= R= S=

Фраза "We talk about" при зашифровуванні набуває вигляду

Геометричне подання може змінюватися, наприклад, на

A = , D = , I =

Тоді



Варто зауважити, що при поході на Росію Наполеон використовував у нижчих ланках свого зв'язку подібні шифри. Їх було розкрито російськими фахівцями, що вельми вплинуло на перебіг бойових дій.

2.5 Шифрувальні таблиці Трисемуса

1508 року абат з Німеччини Йоганн Трисемус надрукував працю з криптології за назвою "Поліграфія". У цій книзі він уперше систематично описав застосовування шифрувальних таблиць, заповнюваних абеткою у довільному порядку. Для дістання такого шифру заміни зазвичай використовувались таблиці для записування літер абетки й ключове слово (чи фраза). У таблицю спочатку вписувалося по рядках ключове слово, причому повторювані літери відкидалися. Потім ця таблиця доповнювалася літерами абетки, які не ввійшли до неї одна за одною. Оскільки ключове слово чи фразу легко зберігати в пам'яті, то такий підхід спрощував процеси зашифровування чи розшифровування.

Цей метод зашифровування докладно розглянуто у розд. 2.9.8.

2.6 Біграмний шифр Плейфейра

Шифр Плейфейра, винайдений 1854 року, є найбільш відомим біграмним шифром заміни. Він застосовувався Великобританією під час першої світової війни. Основою шифру Плейфейра є шифрувальна таблиця з довільно розташованими літерами абетки вихідних повідомлень.

Для зручності запам'ятовування шифрувальної таблиці відправникові та одержувачеві повідомлень можна використовувати ключове слово (чи фразу) при заповнюванні початкових рядків таблиці. У цілому структура шифрувальної таблиці системи Плейфейра є цілковито аналогічна до структури таблиці Трисемуса. Тому для процедур зашифровування й розшифровування в системі Плейфейра можна користуватися таблицею Трисемуса.

Процедура зашифровування включає такі кроки:

1 Відкритий текст вихідного повідомлення розбивається на пари літер (біграми). Текст повинен мати парну кількість літер, і в ньому не повинно бути біграм, які містили б дві однакові літери. Якщо ці вимоги не виконано, то текст змодифіковується навіть через незначні орфографічні помилки.

2 Послідовність біграм відкритого тексту перетворюється за допомогою шифрувальної таблиці на послідовність біграм шифртексту за такими правилами:

2а Якщо дві літери відкритого тексту не потрапляють до одного рядка чи стовпця, тоді відшукують літери в кутах прямокутника, визначуваного даною парою літер. Послідовність літер у біграмі шифртексту має бути дзеркально розташована стосовно послідовності літер у біграмі відкритого тексту.

2б Якщо обидві літери біграми відкритого тексту належать до одного стовпця таблиці, то за літери шифртексту вважаються літери, котрі містяться під ними. Якщо при цьому літера відкритого тексту міститься в нижньому рядку, то для шифртексту береться відповідна літера з верхнього рядка того ж самого стовпця.

2в Якщо обидві літери біграми відкритого тексту належать до одного рядка таблиці, за літери шифртексту вважаються такі, котрі містяться праворуч від них. Якщо при цьому літера відкритого тексту міститься в крайньому правому

стовпці, то для шифру беруть відповідну літеру з лівого стовпця в тому самому рядку.

Цей метод шифрування докладно розглянуто в розд. 2.9.9.

Слід зазначити, що шифрування біграмами різко підвищує стійкість шифрів до розкриття.

2.7 Криптосистема Хілла

Алгебричний метод, котрий узагальнює афінне підставляння Цезаря (див. розд. 2.9.6)

$$E_{a,b}\colon \rightarrow \overline{Z}_m \rightarrow \overline{Z}_m;$$
$$E_{a,b}\colon t \rightarrow E_{\text{a,б}}(t);$$
$$E_{a,b}(t) = at + b \pmod m,$$

де a, b – цілі числа, $0 \le a, b < m$; НСД (найбільший спільний дільник) $(a, m) = 1$, для визначення n-грам було сформульовано Лестером Хіллом.

Множина цілих $\overline{Z}_m$, для якої визначено операції додавання, віднімання та множення за модулем m, являє приклад кільця. Кільце являє собою алгебричну систему, в якій визначено операції додавання, віднімання та множення пар елементів.

Нехай $\overline{A}$ є лінійним перетворенням, описуваним квадратною матрицею, причому

$$\overline{A}\colon \overline{Z}_m \rightarrow \overline{Z}_m.$$

Криптосистема, розроблена Хіллом, базується на лінійній алгебрі.

Нехай простори вихідних повідомлень та криптотекстів збігаються і дорівнюють $\sum$, де $\sum$ – англійська абетка. Надамо літерам номери відповідно до порядку їхнього слідування в абетці:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Всі арифметичні операції виконуються за модулем 26 (кількість літер в абетці). Це означає, що 26 ототожнюється з 0, 27 – з 1, 28 – з 2 і т. д.

Оберемо ціле число $d \ge 2$. Воно зазначає розмірність використовуваних матриць. У процедурі зашифровування набори з d літер вихідного повідомлення зашифровуються разом. Візьмемо $d = 2$.

Нехай тепер A – квадратна $d \times d$ матриця. Елементами A є цілі числа від 0 до 25. Вимагатимемо далі, аби матриця A була невиродженою, тобто існувала обернена матриця A^{-1}. Наприклад,

$$A = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \quad \text{та} \quad A^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}.$$

Нагадаємо, що арифметичні операції провадяться за модулем 26. Це дає, приміром,

$$2 \cdot 17 + 5 \cdot 9 = 79 = 1 + 3 \cdot 26 = 1,$$

тобто, як і мало бути, одиницю на головній діагоналі одиничної матриці (докладніше див. розд. 2.9.10).

Зашифровування здійснюється за допомогою рівняння

$$AP = C,$$

де P та C – d-розмірні вектори-стовпці. Більш докладно: кожен набір з d літер вихідного повідомлення визначає вектор P, компонентами якого є номери літер. Врешті, C знову інтерпретується як набір d літер криптотексту.

Наприклад, HELP визначає два вектори:

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad \text{та} \quad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

З рівнянь

$$AP_1 = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = C_1 \quad \text{та} \quad AP_2 = \begin{pmatrix} 0 \\ 19 \end{pmatrix} = C_2$$

дістаємо криптотекст HITE.

Розглянемо тепер сферу діяльності криптоаналітика. Припустімо, що аналітик здогадався, що $d = 2$. Йому потрібно віднайти матрицю A чи, ще краще, обернену матрицю A^{-1}. З цією метою він обирає вихідне повідомлення HELP і довідується, що відповідний криптотекст є HITE. Криптоаналітикові відомо, що

$$A \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} \quad \text{та} \quad A \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 19 \end{pmatrix}.$$

Це може бути записано у вигляді

$$A = \begin{pmatrix} 7 & 0 \\ 0 & 19 \end{pmatrix} \begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 0 \\ 8 & 19 \end{pmatrix} \begin{pmatrix} 19 & 19 \\ 14 & 21 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}.$$

Обернена матриця A^{-1} одразу ж обчислюється з матриці A. Після цього який завгодно криптотекст може бути розшифровано за допомогою M^{-1}.

Важливим моментом у цих обчисленнях є існування оберненої матриці до $\begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}$. З іншого боку, наш криптоаналітик обрав вихідне повідомлення HELP, котре породжує матрицю $\begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}$, тобто він здійснює вибір у такий спосіб, аби результуюча матриця мала обернену.

Припустімо тепер, що криптоаналітик працює з іншою початковою постановкою – "відоме є певне вихідне повідомлення". Більш докладно: нехай криптоаналітикові відомо, що CKVOZI – криптотекст, який відповідає вихідному повідомленню SAHARA. Хоча ми маємо тут приклад довшого повідомлення, аніж раніше, однак добуваної з нього інформації є набагато менше.

Насправді, тепер рівняння для повідомлення криптотексту мають вигляд

$$A \begin{pmatrix} 18 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 10 \end{pmatrix}, \quad A \begin{pmatrix} 7 \\ 0 \end{pmatrix} = \begin{pmatrix} 21 \\ 14 \end{pmatrix} \quad \text{та} \quad A \begin{pmatrix} 17 \\ 0 \end{pmatrix} = \begin{pmatrix} 25 \\ 8 \end{pmatrix}.$$

Не існує оберненої квадратної матриці, котру може бути утворено з трьох векторів-стовпців, які з'являються як коефіцієнти M.

Криптоаналітик виявляє, що кожна обернена квадратна матриця

$$A' = \begin{pmatrix} 3 & x \\ 2 & y \end{pmatrix}$$

може бути базисом криптосистеми, оскільки вона шифрує SAHARA як CKVOZI. Отже, криптоаналітик може зупинитися на матриці

$$A' = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix},$$

для якої оберненою є матриця

$$(A')^{-1} = \begin{pmatrix} 1 & 25 \\ 24 & 3 \end{pmatrix}.$$

Криптоаналітик є готовий до перехоплення криптотексту. Він дістає текст NAFG й одразу обчислює

$$\begin{pmatrix} 1 & 25 \\ 24 & 3 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \quad \text{та} \quad \begin{pmatrix} 1 & 25 \\ 24 & 3 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 25 \\ 8 \end{pmatrix}.$$

Два вектори-стовпці породжують вихідне повідомлення NAZI. Однак легальний користувач знає оригінальну матрицю A та її обернену матрицю й обчислює

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \quad \text{та} \quad \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 21 \\ 24 \end{pmatrix},$$

що дає вихідне повідомлення NAVY.

Криптоаналітик припустився прикрої помилки, котра могла спричинитися до хибних кроків.

2.8 Математичний аналіз шифру простої заміни

Виконаємо математичний аналіз шифру простої заміни (підставляння) на підставі понять, уведених вище.

Підставляння в абетці $\overline{Z}_m$ є взаємно однозначним відбиттям π з $\overline{Z}_m$ на $\overline{Z}_m$:

$$\pi\colon t \to \pi(t),$$

яке замінює літеру t відкритого тексту на літеру $\pi(t)$ шифртексту. Множина всіх підставлянь на $\overline{Z}_m$ називається ***симетричною групою*** й позначається $\overline{SYM}\,(\overline{Z}_m)$.

Симетрична група $\overline{SYM}\;(\overline{Z}_m)$ має такі властивості:

Замкненість. Добуток підставлянь $\pi_1\pi_2$ є підставлянням:

$$\pi : \overline{Z}_m \xrightarrow{\pi_2} \overline{Z}_m \xrightarrow{\pi_1} \overline{Z}_m,$$

$$\pi\colon t \to \pi_1(\pi_2(t)).$$

Асоціативність. Обидва способи взяття в дужки добутку підставлянь $\pi_1\pi_2\pi_3$

$$\pi_1(\pi_2\pi_3) = (\pi_1\pi_2)\pi_3$$

дають однаковий результат.

Існування одиничного елемента. Підставляння δ, визначуване як

$$\delta(t) = t,\ 0 \le t < m,$$

є єдиним одиничним елементом групи $\overline{SYM}\ (\overline{Z}_m)$ з множення:

$$\delta\pi = \delta\pi \text{ для всіх } \pi \in \overline{SYM}\ (\overline{Z}_m).$$

Існування обернених елементів. Для кожного підставляння π існує взаємно однозначно визначене обернене підставляння, позначуване π^{-1}, яке задовольняє співвідношенню

$$\pi\pi^{-1} = \delta.$$

Зазначені властивості є аксіомами групи.

Ключ K підставляння для абетки $\overline{Z}_m$ являє собою послідовність елементів симетричної групи з $\overline{Z}_m$:

$$K = (\pi_0, \pi_1, ..., \pi_{n-1}),\ \pi_n \in \overline{SYM}\ (\overline{Z}_m),\ 0 \le n < \infty.$$

Підставляння, зумовлюване ключем K, є криптографічним перетворенням $E_к$, котре шифрує n-граму $(y_0, y_1, y_2, ..., y_{n-1})$ шифртексту, де

$$y_i = \pi_i\ (x_i),\quad 0 \le i < n,$$

для кожного n; $n = 1, 2, 3, \ldots$

Криптографічне перетворення $E_к$ називається ***одноабетковим підставлянням***, якщо значення π_i є однакове для кожного i, $i = 1, 2, 3, ...$; у противному разі перетворення $E_к$ називається ***багатоабетковим підставлянням***.

На рис. 2.1 подано схему реалізації підставляння $E_к$.

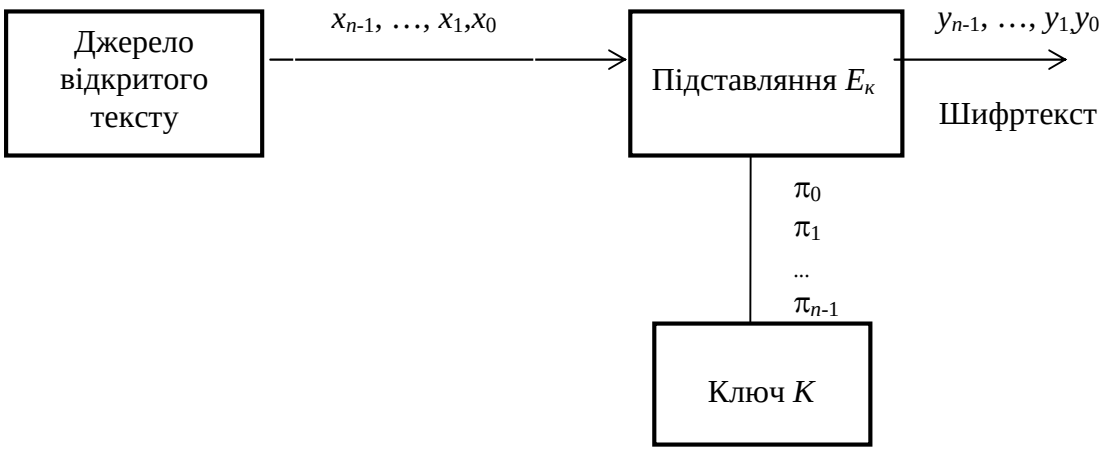


Рисунок 2.1 – Схема підставляння $E_к$

Зазначимо характерні риси підставляння $E_к$:

- відкритий текст зашифровується політерно (літера за літерою);
- i-та літера y_i шифртексту є функцією лише i-тої компоненти π_i ключа K та i-тої літери x_i відкритого тексту;
- зашифровування n-грами $(x_0, x_1, \ldots, x_{n-1})$ здійснюється відповідно до формули

$$(y_0, y_1, \ldots, y_{n-1}) = E_к(x_0, x_1, \ldots, x_{n-1}).$$

Система Цезаря являє собою одноабеткове підставляння, котре шифрує n-граму $(x_0, x_1, \ldots, x_{n-1})$ відкритого тексту на n-граму $(y_0, y_1, \ldots, y_{n-1})$ шифртексту відповідно до такого правила:

$$y_i = E_к(x_i), \quad 0 \le i < n;$$

$$E_к: j \rightarrow (j + K) \pmod{n}, \; 0 \le K < m,$$

де j – числовий код літери відкритого тексту; $j + K$ – числовий код відповідної літери шифртексту.

На відміну від шифру Цезаря, система шифрування Цезаря утворює сімейство одноабеткових підставлянь для обираних значень ключа K, причому $0 \le K < m$.

Достоїнством системи шифрування Цезаря є простота зашифровування й розшифровування. До недоліків системи Цезаря слід віднести такі:

- підставляння, виконувані відповідно до системи шифрування Цезаря, не маскують частості з'являння різних літер вихідного відкритого тексту;
- зберігається абетковий порядок у послідовності тих літер, котрими замінюють; за зміни значення K змінюються лише початкові позиції такої послідовності;
- кількість можливих ключів K є мала;
- шифр Цезаря легко розкривається на підставі аналізу частості з'явлення літер у шифртексті.

Криптоаналітична атака проти системи одноабеткової заміни розпочинається з підрахунку частості з'явлення символів: визначається кількість з′являнь кожної літери в шифртексті. Потім дістаний розподіл частості літер у шифртексті порівнюється з таким самим розподілом частості літер в абетці вихідних повідомлень. Літера з найвищою частістю з'явлення в шифртексті замінюється на літеру з найвищою частістю з'явлення в мові й т. д. Імовірність успішного розкриття системи шифрування підвищується зі збільшенням довжини шифртексту.

2.9 Приклади розв'язування криптографічних завдань за допомогою шифрів одноабеткового підставляння

Шифри заміни схарактеризовуються тим, що окремі частини повідомлення (літери, слова тощо) замінюються на певні інші літери, числа, символи і т. д.

При цьому заміна здійснюється у такий спосіб, аби потім за шифрованим повідомленням можна було однозначно відновити передаване повідомлення.

2.9.1 Шифрування одноабетковим підставлянням

Нехай зашифровується повідомлення українською мовою й при цьому заміні підлягає кожна літера повідомлення. Формально в цьому разі шифр заміни можна описати в такий спосіб. Для кожної літери *а* вихідної абетки будується певна множина символів M_a, аби множини M_a та $M_в$ попарно не перетинались за $а \neq в$, тобто будь-які дві різні множини не містили однакових елементів. Множина M_a називається множиною шифропозначань для літери *а*.

Таблиця 2.4 є ключем шифру заміни. Знаючи її, можна здійснювати як зашифровування, так і розшифровування.

Таблиця 2.4 – Зашифровування літер відкритого повідомлення за допомогою будь-якого символу з множини M_j

а	*б*	*в*	…	*я*
M_a	$M_б$	$M_в$	…	$M_я$

При зашифровуванні кожна літера *а* відкритого повідомлення, розпочинаючи з першої, замінюється на будь-який символ з множини M_a . Якщо в повідомленні міститься кілька літер *а*, то кожна з них замінюється на будь-який символ з M_a. За рахунок цього за допомогою одного ключа (див. табл. 2.5) можна дістати різноманітні варіанти зашифрованого повідомлення для одного й того самого відкритого повідомлення. Наприклад, якщо ключем є таблиця 2.5, то повідомлення «мені відомі шифри заміни» може бути зашифровано кожним з трьох способів, поданих в цій таблиці.

Таблиця 2.5 – Зашифровування літер відкритого повідомлення за допомогою одного з трьох числових символів множини M_j

а	*б*	*в*	*г*	*д*	*е*	*є*	*ж*	*з*	*и*	*і*	*к*	*л*	*м*	*н*	*о*	*п*
21	37	14	22	01	24	74	62	73	46	65	23	12	08	27	53	35
40	26	63	47	31	83	17	88	30	02	34	91	72	32	77	68	60
10	03	71	82	15	70	42	11	55	90	92	69	38	61	54	09	84

р	*с*	*т*	*у*	*ф*	*х*	*ц*	*ч*	*ш*	*щ*	*ь*	*ї*	*ю*	*я*
04	20	13	59	25	75	43	19	29	06	48	36	28	16
44	52	39	07	49	33	85	58	80	50	56	78	64	41
45	89	67	93	76	18	51	87	66	81	79	86	05	57

м	е	н	і	в	і	д	о	м	і	ш	и	ф	р	и	з	а	м	і	н	и
08	24	54	65	14	34	31	53	32	92	09	61	89	29	90	30	40	08	65	27	46
32	83	77	34	71	65	01	68	61	92	68	08	20	66	90	73	40	61	34	77	02
61	70	27	34	63	92	15	09	08	65	68	32	20	80	02	55	10	32	92	54	90

Оскільки множини $M_а$, $M_б$, $M_в$, …, $M_я$ попарно не перетинаються, то за кожним символом шифрованого повідомлення можна однозначно визначити, якій множині він належить й, отже, яку саме літеру відкритого повідомлення він замінює. Тому розшифровування є можливе й відкрите повідомлення визначається у єдиний спосіб.

2.9.2 Шифрування за допомогою квадрата Полібія

Як вже зазначалося вище, за один з перших шифрів простої заміни вважається так званий *полібіанський квадрат*. За два сторіччя до нашої ери Полібій винайшов для цілей зашифровування квадратну таблицю розміром 5×5, заповнену літерами грецької абетки у довільному порядку (рис. 2.2).

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	ς
χ	ν	-	φ	ί

Рисунок 2.2 – Полібіанський квадрат, заповнений у довільний спосіб 24-ма літерами грецької абетки й прогалиною

При зашифровуванні в цьому квадраті відшукували чергову літеру відкритого тексту й записували до шифртексту літеру, розташовану нижче за неї в тім самім стовпці. Якщо літера тексту містилася в нижньому рядку таблиці, то для шифртексту брали найверхню літеру з того самого стовпця. Наприклад, для слова

τ α υ ρ ο σ χ

виходить шифртекст

ς φ δ μ τ ξ λ .

Концепція полібіанського квадрата виявилася плідною і набула застосування в криптосистемах подальшого часу.

2.9.3 Шифрування за рахунок перетворювання числового повідомлення на літерне

Розглянемо 30-літерну абетку української мови:

АБВГДЕЄЖЗИІКЛМНОПРСТУФХЦЧШЩЬЮЯ

У цій абетці відсутні літери Ї, Й , що практично не обмежує можливостей за складання відкритих повідомлень українською мовою.

В абетці будь-якої природної мови літери слідують одна за одною у певному порядку. Це дає можливість надати кожній літері абетки її природний порядковий номер.

Занумеруємо літери української абетки відповідно до табл. 2.6.

Таблиця 2.6 – Відповідність поміж українською абеткою та множиною цілих

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	К	Л	М	Н
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Якщо у відкритому повідомленні кожну літеру замінити на її природний порядковий номер у розглядуваній абетці, то перетворення числового повідомлення на літерне дозволяє однозначно відновити вихідне відкрите повідомлення. Наприклад, числове повідомлення 1 13 22 1 3 11 20 перетвориться на літерне повідомлення: АЛФАВІТ.

2.9.4 Розшифровування повідомлення за відомою умовою шифрування

Для зашифрованого повідомлення з n літер обирається ключ K – певна послідовність з n літер абетки, наведеної в табл. 2.6. Зашифровування кожної літери повідомлення полягає в додаванні її номера в таблиці з номером відповідної літери ключової послідовності й заміні дістаної суми на літеру абетки, номер якої має ту саму остачу від ділення на 30, що й ця сума.

Необхідно прочитати шифроване повідомлення: РБЬНПТИТСРРЕЗОХ, якщо відомо, що шифрувальна послідовність не містила жодних літер, окрім А, Б та В.

Кожну літеру шифрованого повідомлення розшифруємо в трьох варіантах, припускаючи послідовно, що відповідна літера шифрувальної послідовності є літера А, Б чи В:

Таблиця 2.7 – Три варіанти розшифровування шифрованого повідомлення

Шифртекст	**Р**	**Б**	**Ь**	**Н**	**П**	**Т**	**И**	**Т**	**С**	**Р**	**Р**	**Е**	**З**	**О**	**Х**
Варіант А	П	А	Щ	М	О	С	З	С	Р	П	П	Д	Ж	Н	Ф
Варіант Б	О	Я	Ш	Л	Н	Р	Ж	Р	П	О	О	Г	Е	М	У
Варіант В	Н	Ю	Ч	К	М	П	Е	П	О	Н	Н	В	Д	Л	Т

Обираючи з кожного стовпчика таблиці 2.7 лише по одній літері, віднайдемо осмислене повідомлення НАШКОРЕСПОНДЕНТ, яке й є шуканим.

Зауваження. З дістаної таблиці можна було б віднайти не одне осмислене повідомлення. Кількість решти різноманітних варіантів вихідних повідомлень без обмежень на осмисленість дорівнює 3^{15}, або 14348907, тобто понад 14 мільйонів!

2.9.5 Подвійне шифрування

Перетворення шифру простої заміни в абетці $A = \{a_1, a_2, \ldots, a_n\}$, яка складається з n різних літер, полягає в заміні кожної літери тексту, який треба зашифрувати, літерою тієї самої абетки, причому різні літери замінюються на різні. Ключем до шифру простої заміни є таблиця 2.8, в якій зазначено, якою саме літерою треба замінити кожну літеру російської абетки A.

Таблиця 2.8 – Зашифровування літер за допомогою шифру простої заміни

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
Ч	Я	Ю	Э	Ы	Ь	Щ	Ш	Ц	Х	Ф	У	Б	Д	Т

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
З	В	Р	П	М	Л	К	А	И	О	Ж	Е	С	Г	Н

Якщо слово СРОЧНО зашифрувати простою заміною за допомогою ключа таблиці 2.8, то вийде слово ВЗДАБД. Зашифрувавши здобуте слово за допомогою того самого ключа вдруге, здобудемо слово ЮШЫЧЯЫ.

Слід визначити, скільки всього всіляких слів можна здобути, якщо зазначений процес зашифровування продовжувати необмежено. Оскільки розглядуваний шифр має таку властивість, що різні літери замінюються на різні, то при зашифровуванні різних слів виходять різні слова. З іншого боку, однакові літери замінюються на однакові незалежно від циклу зашифровування, тому що використовується один і той самий ключ. Отже, при зашифровуванні однакових слів виходять однакові слова, тобто, кількість різних слів, які можна здобути в зазначеному процесі зашифровування з початковим словом СРОЧНО, збігається з найменшим номером циклу зашифровування, котрий дає це початкове слово.

Оскільки літера С повторюється в кожнім циклі зашифровування, номер якого дорівнює 5, а літери Р, О, Ч, Н – у кожнім циклі, номери яких є кратні до 13, 7, 2 та 3 відповідно, то слово СРОЧНО з'явиться вперше в циклі з номером, дорівнюваним

$$НСК\,(2,3,5,7,13) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730,$$

де НСК – найменше спільне кратне.

2.9.6 Шифрування за допомогою афінної системи

У системі шифрування Цезаря використовувалися лише адитивні властивості цілих $\overline{Z}_m$. Однак символи множини $\overline{Z}_m$ можна також перемножувати за модулем m. Застосовуючи водночас операції додавання та множення за модулем m над елементами множини $\overline{Z}_m$, можна здобути систему підставляння, що її називають афінною системою підставляння Цезаря.

Визначимо перетворювання в такій системі:

$$E_{a,b}: \overline{Z}_m \rightarrow \overline{Z}_m;$$
$$E_{a,b}: t \rightarrow E_{a,b}(t);$$
$$E_{a,b}(t) = at + b \pmod m,$$

де a, b – цілі числа, $0 \le a, \ b < m$; НСД (найбільший спільний дільник) $(a, m) = 1$.

У даному перетворюванні літера, котра відповідає числу t, замінюється на літеру, котра відповідає числовому значенню $at + b$ за модулем m.

Слід зауважити, що перетворення $E_{a,b}(t)$ є взаємно однозначним відбиттям на множину $\overline{Z}_m$ лише в тому разі, якщо найбільший спільний дільник чисел

a та *m* дорівнює одиниці, тобто *a* та *m* повинні бути взаємно простими числами. Наприклад, нехай *m* = 26, *a* = 3, *b* = 5. НСД (3,26) = 1 і можна здобути подану в табл. 2.9. відповідність поміж числовими кодами літер,

Таблиця 2.9 – Відповідність поміж числовими кодами літер

t	0	1	2	3	4	5	6	7	8	9	10	11	12
3*t* + 5	5	8	11	14	17	20	23	0	3	6	9	12	15

t	13	14	15	16	17	18	19	20	21	22	23	24	25
3*t* + 5	18	21	24	1	4	7	10	13	16	19	22	25	2

Якщо перетворити числа на літери англійської мови, дістанемо подану в табл. 2.10. відповідність для літер відкритого тексту та шифртексту,

Таблиця 2.10 – Відповідність для літер англійської мови відкритого тексту та шифртексту

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
F	I	L	O	R	U	X	A	D	G	J	M	P	S	V

P	Q	R	S	T	U	V	W	X	Y	Z
Y	B	E	H	K	N	Q	T	W	Z	C

Вихідне повідомлення HOPE перетвориться на шифртекст AVYR.

Достоїнством афінної системи є зручне керування ключами: ключі зашифровування й розшифровування подаються в компактній формі у вигляді пари чисел (*a, b)*. Недоліки афінної системи є аналогічні до недоліків системи шифрування Цезаря.

2.9.7 Шифрування за допомогою системи Цезаря з ключовим словом

Система шифрування Цезаря з ключовим словом є одноабетковою системою підставляння. Особливістю цієї системи є використання ключового слова для зсунення та змінювання порядку символів в абетці підставляння.

Оберемо певне число *k*, $0 \le k < 25$, і слово чи коротку фразу як ключове слово. Бажано, щоб усі літери ключового слова були різні. Оберемо слово DIPLOMAT за ключове й число *k* = 5.

Ключове слово записується під літерами абетки, розпочинаючи з літери, числовий код якої збігається з обраним числом *k*:

0 1 2 3 4 5 10 15 20 25
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D I P L O M A T

Решта літер абетки підставляння записуються після ключового слова за абеткою:

5
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V W X Y Z D I P L O M A T B C E F G H J K N Q R S U

Тепер ми маємо підставляння для кожної літери довільного повідомлення.

Вихідне повідомлення

SEND MORE MONEY

шифрується як

HZBY TCGZ TCBZS

Слід зазначити, що вимога щодо розходження всіх літер ключового слова не є обов'язковою. Можна просто записати ключове слово (чи фразу) без повторення однакових літер. Наприклад, ключова фраза

КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН

і число $k = 3$ породжують таку таблицю підставляння:

Таблиця 2.11 – Зашифровування літер за допомогою ключової фрази у шифрі простої заміни

0			З												
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Ъ	Э	Ю	К	А	Д	Ы	М	О	Т	Е	Ч	С	В	Н	Л

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
И	П	Р	Я	Б	Г	Ж	З	Й	У	Ф	Х	Ц	Ш	Щ	Ь

Безперечним достоїнством системи Цезаря з ключовим словом є те, що кількість можливих ключових слів є практично невичерпна. Недоліком цієї системи є можливість зламу шифртексту на підставі аналізу частості з'явлення літер.

2.9.8 Шифрування за допомогою таблиці Трисемуса

Для здобуття шифру заміни Трисемуса зазвичай використовувалися таблиці для записування літер абетки й ключове слово. У таблицю спочатку вписувалося по рядках ключове слово, причому повторювані літери відкидалися. Потім ця таблиця доповнювалася літерами абетки, які не увійшли до неї одна за одною.

Для української абетки таблиця Трисемуса може мати розмір 4×8. Оберемо за ключ слово БАНДЕРОЛЬ. Розглянемо шифрувальну таблицю з ключем, поданим у табл. 2.12

Таблиця 2.12 – Шифрувальна таблиця з ключовим словом

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Є	Ж	З	И	І
Ї	Й	К	М	П	С	Т	У
Ф	Х	Ц	Ч	Ш	Щ	Ю	Я

Як і в разі полібіанського квадрата, при шифруванні відшукують у цій таблиці чергову літеру відкритого тексту і записують у шифртекст літеру, розташовану нижче за неї в тім самім стовпці. Якщо літера тексту міститься в ни-

жньому рядку таблиці, тоді для шифртексту беруть першу верхню літеру з того ж самого стовпця.

Наприклад, при шифруванні за допомогою цієї таблиці повідомлення

ДІЛОМАЙСТРАВЕЛИЧАЄ

дістаємо шифртекст

ЄУІИЧВХЩЮЗВЙЖІТДВМ

Такі табличні шифри називаються ***монограмними***, тому що шифрування виконується за однією літерою.

2.9.9 Шифрування за допомогою біграмного шифру Плейфейра

Основою шифру Плейфейра є шифрувальна таблиця з випадково розташованими літерами абетки вихідних повідомлень.

У цілому структура таблиці системи шифрування Плейфейра є цілком аналогічна до структури таблиці Трисемуса. Тому для пояснення процедур зашифровування й розшифровування в системі Плейфейра скористаємося таблицею 2.12.

Процедура зашифровування включає такі вимоги:

Відкритий текст вихідного повідомлення розбивається на пари літер (біграми). Текст повинен мати парну кількість літер і в ньому не повинно бути біграм, котрі містили б дві однакові літери. Якщо цих вимог не додержано, то текст змодифіковується навіть через незначні орфографічні помилки.

Послідовність біграм відкритого тексту перетворюється за допомогою шифрувальної таблиці на послідовність біграм шифртексту за такими правилами:

♦ якщо дві літери відкритого тексту не потрапляють в один рядок чи стовпець (як, наприклад, літери А та И у табл. 2.12), тоді відшукують літери в кутах прямокутника, визначуваного даною парою літер. (У нашому прикладі це літери АИОВ. Пара літер АИ відбивається в пару ОВ.) Послідовність літер у біграмі шифртексту має бути дзеркально розташована стосовно послідовності літер у біграмі відкритого тексту;

♦ якщо обидві літери біграми відкритого тексту належать до одного стовпця таблиці, то за літери шифртексту вважаються літери, котрі розміщено під ними (наприклад, біграма НК дає біграму шифртексту ГЦ). Якщо при цьому літера відкритого тексту перебуває в нижньому рядку, то для шифртексту береться відповідна літера з верхнього рядка того самого стовпця (наприклад, біграма ВХ дає біграму шифртексту ЙА);

♦ якщо обидві літери біграми відкритого тексту належать до одного рядка таблиці, то за літери шифртексту вважаються літери, котрі розміщено праворуч від них (наприклад, біграма НО дає біграму шифртексту ДЛ). Якщо при цьому літера відкритого тексту перебуває в крайньому правому стовпці, то для шифру беруть відповідну літеру з лівого стовпця в тому самому рядку (наприклад, біграма ХЯ дає біграму шифртексту ЦФ).

Зашифруємо текст:

ВСЯКИЙ СВОГО ЩАСТЯ КОВАЛЬ

Розбиття цього тексту на біграми дає

ВС ЯК ИЙ СВ ОГ ОЩ АС ТЯ КО ВА Л Ь

Дана послідовність біграм відкритого тексту перетворюється за допомогою шифрувальної таблиці (див. табл. 2.12) на таку послідовність біграм шифртексту:

ГЖ ЦУ ВТ ЖГ НИ РЮ ДВ УЮ ТН ЙВ БІ

При розшифровуванні застосовується зворотний порядок дій.

2.9.10. Шифрування за допомогою криптосистеми Хілла

Нехай простори вихідних повідомлень та криптотекстів збігаються й дорівнюють ∑, де ∑ – англійська абетка. Надамо літерам номери, відповідно до порядку їхнього слідування в абетці:

Таблиця 2.13 – Відповідність поміж англійською абеткою та множиною цілих

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

15	16	17	18	19	20	21	22	23	24	25
P	Q	R	S	T	U	V	W	X	Y	Z

Всі арифметичні операції виконуються за модулем 26 (кількість літер в абетці).

Оберемо розмірність використовуваних матриць. У процедурі зашифровування набори з d літер вихідного повідомлення шифруються разом. Візьмемо $d = 2$.

Тоді A – квадратна 2×2 матриця. Елементами A є цілі числа від 0 до 25. Потребуватимемо далі, аби матриця A була невиродженою, тобто існувала матриця A^{-1}.

Розглянемо алгоритм зашифровування в криптосистемі Хілла.

Дано квадратну матрицю виду $\begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$

$$A = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}.$$

1 Обчислюється визначник D матриці A:

$$D = a_{11}a_{22} - a_{12}a_{21} = 3 \cdot 5 - 2 \cdot 3 = 15 - 6 = 9.$$

2 Визначається долучена матриця алгебричних доповнень A^*, складена з алгебричних доповнень до елементів матриці A, причому алгебричне доповнення до елемента a_{ij} перебуває на перетинанні j-того рядка й i-того стовпця.

$$A^* = \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix}.$$

Під алгебричним доповненням A_{ij} елемента a_{ij} розуміють мінор M_{ij}, домножений на $(-1)^{i+j}$:

$$A_{ij} = (-1)^{i+j} M_{ij},$$

тобто

$$A_{11} = (-1)^{1+1} \cdot M_{11} = (-1)^2 \cdot a_{22} = 1 \cdot 5 = 5;$$
$$A_{12} = (-1)^{2+1} \cdot M_{12} = (-1)^3 \cdot a_{12} = -1 \cdot 2 = -2;$$
$$A_{21} = (-1)^{1+2} \cdot M_{21} = (-1)^3 \cdot a_{21} = -1 \cdot 3 = -3;$$
$$A_{22} = (-1)^{2+2} \cdot M_{22} = (-1)^4 \cdot a_{11} = 1 \cdot 3 = 3.$$

Отже, можна записати здобуту матрицю алгебричних доповнень:

$$A^* = \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}.$$

3 Визначається обернена матриця A^{-1}.

За обернену матрицю для A слугуватиме матриця, котра виходить із долученої матриці A^* діленням усіх її елементів на D.

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{D} & \frac{A_{21}}{D} \\ \frac{A_{12}}{D} & \frac{A_{22}}{D} \end{pmatrix} = \begin{pmatrix} \frac{5}{9} & \frac{-3}{9} \\ \frac{-2}{9} & \frac{3}{9} \end{pmatrix}.$$

Перевіримо, чи виконується умова $A \cdot A^{-1} = E$, де E – квадратна одинична матриця.

За правилом перемножування матриць, елемент, який розміщено в i-тому рядку й j-тому стовпці матриці добутку, дорівнює сумі добутків відповідних елементів i-того рядка матриці A та j-того стовпця матриці A^{-1}.

$$A \cdot A^{-1} = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} \frac{5}{9} & \frac{-3}{9} \\ \frac{-2}{9} & \frac{3}{9} \end{pmatrix} = \begin{pmatrix} 3\frac{5}{9} - 3\frac{2}{9} & 3\left(\frac{-3}{9}\right) + 3\frac{3}{9} \\ 2\frac{5}{9} - 5\frac{2}{9} & 2\left(\frac{-3}{9}\right) + 5\frac{3}{9} \end{pmatrix} = \begin{pmatrix} \frac{15-6}{9} & \frac{9-9}{9} \\ \frac{10-10}{9} & \frac{15-6}{9} \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Отже, можна дійти висновку, що обернену матрицю знайдено правильно.

4 Зведення оберненої матриці за модулем 26.

$$A^{-1} \bmod 26 = \begin{pmatrix} \frac{5}{9} & \frac{-3}{9} \\ \frac{-2}{9} & \frac{3}{9} \end{pmatrix} \bmod 26 = \begin{pmatrix} \frac{135}{9} & \frac{153}{9} \\ \frac{180}{9} & \frac{81}{9} \end{pmatrix} \bmod 26 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}.$$

5 Зашифровування відкритого повідомлення.

Зашифровування здійснюється за допомогою рівняння $A \cdot P = C$, де A – матриця перетворення; P – вектор, компонентами якого є номери літер відкритого повідомлення відповідно до табл. 2.13; C – вектор, компонентами якого є номери літер закритого повідомлення відповідно до табл. 2.13.

Зашифруємо слово HELP.

Спочатку розіб'ємо n-граму відкритого тексту на біграми. Потім у кожній біграмі відкритого тексту замінимо кожну літеру на її числовий еквівалент відповідно до табл. 2.13.

Вихідне повідомлення HELP визначає два вектори:

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad \text{та} \quad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix};$$

$$C_1 = A \cdot P_1 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \cdot 7 + 3 \cdot 4 \\ 2 \cdot 7 + 5 \cdot 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} 33 \\ 34 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 8 \end{pmatrix};$$

$$C_2 = A \cdot P_2 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 3 \cdot 11 + 3 \cdot 15 \\ 2 \cdot 11 + 5 \cdot 15 \end{pmatrix} \bmod 26 = \begin{pmatrix} 78 \\ 97 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 19 \end{pmatrix}.$$

Отже, здобули послідовність чисел 7, 8, 0, 19.

З табл. 2.13 дістаємо криптотекст HIAT.

Процес розшифровування йде за зворотним алгоритмом.

$$P_1 = A^{-1} \cdot C_1 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 15 \cdot 7 + 17 \cdot 8 \\ 20 \cdot 7 + 9 \cdot 8 \end{pmatrix} \bmod 26 = \begin{pmatrix} 241 \\ 212 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix};$$

$$P_2 = A^{-1} \cdot C_2 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 15 \cdot 0 + 17 \cdot 19 \\ 20 \cdot 0 + 9 \cdot 19 \end{pmatrix} \bmod 26 = \begin{pmatrix} 323 \\ 171 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

Здобута цифрова послідовність 7, 4, 11, 15 відповідно до табл. 2.13 надає можливість відновити вихідний текст: HELP.

2.10 Завдання для самоперевірки

Завдання 2.1 Використовуючи шифр Цезаря, зашифрувати свої іменні дані (прізвище, ім'я, по батькові).

Завдання 2.2 Зашифрувати свої іменні дані, якщо ключем є таблиця, наведена в прикладі розд. 2.9.1.

Завдання 2.3 Зашифрувати слово ЖУК простою заміною за допомогою ключа, наведеного у таблиці 2.8 прикладу розд. 2.9.5.

Якщо процес шифрування продовжувати необмежено, то в якому циклі вперше з'явиться вихідне слово?

Завдання 2.4 За допомогою афінної системи підставляння Цезаря для української абетки перетворити відкрите повідомлення КЛЮЧ на шифртекст.

$E_{a, b}(t) = at + b \pmod m$, де $m = 31$, $a = 3$, $b = 5$.

Завдання 2.5 Зашифрувати за допомогою таблиці Трисемуса свої іменні дані.

За ключ взяти слово ДОКУМЕНТ.

Завдання 2.6 Зашифрувати за допомогою шифра Плейфейра свої іменні дані.

За ключ взяти слово ДОКУМЕНТ.

Завдання 2.7 Зашифрувати за допомогою криптосистеми Хілла своє прізвище, якщо коефіцієнти квадратної матриці є такі:

$a_{11} = 9$; $a_{12} = 2$; $a_{21} = 4$; $a_{22} = 7$.

Абетка – українська + 5 розділових знаки (mod 38).

3 ШИФРИ СКЛАДНОЇ ЗАМІНИ (БАГАТОАБЕТКОВІ ШИФРИ)

Шифри складної заміни називають багатоабетковими шифрами, тому що для шифрування кожного символу вихідного повідомлення застосовують власний шифр простої заміни. Багатоабеткове підставляння послідовно й циклічно змінює використовувані абетки.

При r-абетковому підставлянні символ x_0 вихідного повідомлення замінюється на символ y_0 з абетки B_0, символ x_1 – на символ y_1 з абетки B_1 і т. д., символ x_{r-1} замінюється на символ y_{r-1} з абетки B_{r-1}, символ x_r замінюється на символ y_r знову з абетки B_0 і т. д.

Загальна схема багатоабеткового підставляння для випадку $r = 4$ наведена в табл. 3.1.

Таблиця 3.1 – Схема r-абеткового підставляння для випадку $r = 4$

Вхідний символ	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
Абетка підставляння	B_0	B_1	B_2	B_3	B_0	B_1	B_2	B_3	B_0	B_1

Ефект використання багатоабеткового підставляння полягає в тім, що забезпечується маскування природної статистики вихідної мови, тому що конкретний символ з вихідної абетки A може бути перетворено на кілька різних символів шифрувальних абеток B_j.

3.1 Історія розвинення шифрів складної заміни

Багатоабеткові шифри заміни запропонував і запровадив у практику криптології Леон Батист Альберті, котрий був також відомим архітектором і теоретиком мистецтва. Його книга "Трактат про шифр", написана 1566 року, являла собою першу в Європі наукову працю з криптології. Криптологи усього світу вважають Л. Альберті за основоположника криптології.

Леон Альберті уперше запропонував ідею подвійного шифрування – текст, здобутий внаслідок першого шифрування, піддавався повторному зашифровуванню. У трактаті Альберті було наведено і його власний шифр, який він назвав "шифром, вартим королів". Він стверджував, що цей шифр є недешифровний. Реалізація шифру здійснювалася за допомогою шифрувального диска, який поклав початок цілої серії багатоабеткових шифрів. Пристрій являв собою пару дисків – зовнішній, нерухомий (на ньому було нанесено літери в природному порядку й цифри від 1 до 4) і внутрішній – рухомий (на ньому літери було переставлено). Процес шифрування полягав у перебуванні літери відкритого тексту на зовнішньому диску й заміні її на відповідну (яка містилася під нею) літеру шифрованого тексту. Після зашифровування декількох слів внутрішній диск зсувався на один крок. Ключем даного шифру є порядок розташування літер на внутрішньому диску і його початкове положення щодо зовнішнього диска.

Шифр, зреалізовуваний диском Альберті, нашого часу дістав назви багатоабеткового. Зміст цієї назви полягає в такому.

Повернімося до дворядкового запису шифру заміни Ю. Цезаря. Назвемо верхній рядок абеткою відкритого тексту, а нижній – абеткою шифрованого тексту (шифрабеткою). Якщо в перебігу шифрування абетка шифрованого тексту не змінюється, то шифр є одноабетковим (чи шифром простої заміни); якщо ж ця абетка змінюється, то шифр є багатоабетковим. Отже, шифр Цезаря – це шифр простої заміни, а в багатоабетковому шифрі Альберті кількість абеток дорівнює кількості літер в абетках відкритого тексту плюс чотири. Альберті – винахідник багатоабеткових шифрів, які, в основному, використовуються й у наші дні. Однак засіб продукування послідовності абеток шифрованого тексту та їхній вибір є надто ускладнений; в Альберті він визначався циклічним зсуненням на одиницю через заздалегідь обумовлену кількість літер, які треба зашифрувати, тобто процес шифрування став "динамічним".

Другий винахід Альберті – літерно-цифровий код (щоправда, малого обсягу). Цифри на диску Альберті (1, 2, 3, 4) шифруються так само, як і літери. Альберті запропонував використовувати упорядковані дво-, три- й чотирицифрові комбінації в якості кодопозначень для літер, слів і цілих фраз (кількість таких комбінацій дорівнює 336). Не виключено, що такі коди використовувалися й раніше, але в історичних документах їх позв’язують з ім’ям Альберті. Особливо відзначимо, що кодовані повідомлення потім повторно шифрувались, тобто використовувався код з перешифровуванням. Ця ідея використовується і в сучасному шифруванні.

У XVI сторіччі вагомий внесок до розвинення криптографії вклав криптограф папи римського Маттео Ардженті, котрий успадкував мистецтво тайнопису від свого дядька. Саме Ардженті запропонував використовувати слово-пароль для надання абетці легко запам’ятовуваного змішаного вигляду. Про це вже йшлося при розгляданні ускладненого шифру Полібія.

Ардженті рекомендував не відокремлювати слова, застосовувати омофонні заміни, вставляти в шифртекст велику кількість "пустишок", усувати пунктуацію, не вставляти в шифртекст відкриті слова ("клер") і т. д. Для утруднення дешифрування шифрів заміни він запропонував таке: замінювати літери чи на цифри (від 0 до 9), чи на числа (від 00 до 99), причому, аби уникнути плутанини при розшифровуванні, цифри, використовувані як самостійні шифропозначення, не повинні входити до двознакових позначень. Оскільки однознакових позначень виявляється порівняно небагато, то, аби не впадала в око їхня мала частість з’явлення в шифртексті, Ардженті рекомендував додавати однознакові позначення літер, які найчастіше зустрічаються у відкритому тексті.

Наведемо приклад шифру заміни Ардженті для італійської мови. У цій заміні поряд із шифруванням використовується шифрування-кодування деяких дво- й трилітерних часто вживаних сполучень.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**L**	**M**	**N**	**O**
1	**86**	**02**	**20**	**62, 82**	**22**	**06**	**60**	**3**	**24**	**26**	**84**	**9**

P	**Q**	**R**	**S**	**T**	**U**	**Z**
66	**68**	**28**	**42**	**80**	**46**	**88**

ET	**CON**	**NON**	**CHE**	**ПУСТИШКИ**
08	**64**	**00**	**44**	**5, 7**

Слово **ARGENTI** могло набути при зашифровуванні такого вигляду:

5128066284580377 або такого: **17728506825847805З7**.

Це було насправді серйозне ускладнення шифру заміни. Частісний аналіз дешифрувальника істотно ускладнювався.

Ардженті займався також ускладненням кодів (номенклаторів). Зокрема, він уперше розробив літерний код, у якому 1200 літер, складів, слів і цілих фраз замінювалися на групу з літер.

Порта видозмінив шифрувальний диск Альберті, перетворивши абетку шифрованого тексту на улюблені ним символіко-геометричні фігури. Зрозуміло, жодного ускладнення при цьому шифр Альберті не набув, додалося лише екзотики у шифрованому тексті.

Основна книга Порта про тайнопис – це книга "Про таємне переписування". Вона написана в жанрі підручника. У ній Порта висвітлив слабкості широко розповсюджених того часу шифрів, у тому числі й шифрів масонів, котрі він іронічно назвав шифрами "сільських жителів, жінок та дітей", і запропонував так званий біграмний шифр.

Цей шифр є шифр біграмної (дволітерної) заміни, в якому кожному дволітерному сполученню відкритого тексту в шифрованому тексті відповідав спеціально вигаданий знак. Знаки шифртексту мали форму символіко-геометричних фігур. Власне це був той самий шифр простої заміни, але на рівні дволітерних сполучень. Криптографічна стійкість за такої заміни порівняно з політерним шифруванням помітно ставала потужнішою.

Порта також запропонував змеханізовувати процес шифрування за його таблицею. Він навів опис механічного дискового пристрою, який зреалізовує біграмну заміну.

Порта рекомендував не використовувати в переписуванні стандартних слів та виразів; більш того, він пропонував записувати відкритий текст з помилками, аби утруднити роботу дешифрувальника. Він писав: "... коли тема переписування є відома, аналітик може робити проникливі припущення щодо слів ...", що може істотно полегшити роботу дешифрувальника.

Порта запропонував певну модифікацію шифру Белазо. У застосуванні до української мови він являє собою прямокутну таблицю з літер абетки в порядку, наведеному на рис. 3.1.

1	А Б	а н	б о	в п	г р	д с	е т	є у	ж ф	з х	и ц	і ч	ї ш	й щ	к ь	л ю	м я
2	В Г	а о	б п	в р	г с	д т	е у	є ф	ж х	з ц	и ч	і ш	ї щ	й ь	к ю	л я	м н
3	Д Е	а п	б р	в с	г т	д у	е ф	є х	ж ц	з ч	и ш	і щ	ї ь	й ю	к я	л н	м о
4	Є Ж	а р	б с	в т	г у	д ф	е х	є ц	ж ч	з ш	и щ	і ь	ї ю	й я	к н	л о	м п
5	З И	а с	б т	в у	г ф	д х	е ц	є ч	ж ш	з щ	и ь	і ю	ї я	й н	к о	л п	м р
6	І Ї	а т	б у	в ф	г х	д ц	е ч	є ш	ж щ	з ь	и ю	і я	ї н	й о	к п	л р	м с
7	Й К	а у	б ф	в х	г ц	д ч	е ш	є щ	ж ь	з ю	и я	і н	ї о	й п	к р	л с	м т
8	Л М	а ф	б х	в ц	г ч	д ш	е щ	є ь	ж ю	з я	и н	і о	ї п	й р	к с	л т	м у
9	Н О	а х	б ц	в ч	г ш	д щ	е ь	є ю	ж я	з н	и о	і п	ї р	й с	к т	л у	м ф
10	П Р	а ц	б ч	в ш	г щ	д ь	е ю	є я	ж н	з о	и п	і р	ї с	й т	к у	л ф	м х
11	С Т	а ч	б ш	в щ	г ь	д ю	е я	є н	ж о	з п	и р	і с	ї т	й у	к ф	л х	м ц
12	У Ф	а ш	б щ	в ь	г ю	д я	е н	є о	ж п	з р	и с	і т	ї у	й ф	к х	л ц	м ч
13	Х Ц	а щ	б ь	в ю	г я	д н	е о	є п	ж р	з с	и т	і у	ї ф	й х	к ц	л ч	м ш
14	Ч Ш	а ь	б ю	в я	г н	д о	е п	є р	ж с	з т	и у	і ф	ї х	й ц	к ч	л ш	м щ
15	Щ Ь	а ю	б я	в н	г о	д п	е р	є с	ж т	з у	и ф	і х	ї ц	й ч	к ш	л щ	м ь
16	Ю Я	а я	б н	в о	г п	д р	е с	є т	ж у	з ф	и х	і ц	ї ч	й ш	к щ	л ь	м ю

Рисунок 3.1 – Шифр Белазо для української мови

Шифрування здійснюється за допомогою секретного гасла. Це гасло періодично виписується над відкритим текстом, за першою літерою цього гасла відшукується абетка (великі літери на початку рядків), у верхній чи нижній напівабетці відшукується перша літера відкритого тексту і замінюється на відповідну їй літеру з верхнього чи нижнього рядка. Аналогічно шифруються й інші літери (інтервали поміж словами не враховуються). Навеведемо приклад:

Гасло: **с к а р б н и ц я с к а р б н и ц я …….....**

Відкритий текст: **п е р и о д и ч н и й ш и ф р …….....**

Шифртекст: **з ш г п б щ ь л б р п ї п ж ї .....**

За цей шифр Порта пізніше назвали батьком сучасної криптографії, але свого часу цей шифр не набув широкого застосування. Причина цього – необхідність постійно мати при собі зазначену таблицю і складність процесу шифрування. Однак було надано імпульсу для з′явлення інших систем шифру (наприклад шифру Віженера).

У середині XVI сторіччя в Італії з'являється книга математика, лікаря й філософа Дж. Кардано "Про тонкощі" з доповненням "Про різні речі", у якій є розділи, присвячені криптографії. У ній знайшли відбиття нові ідеї криптографії: використання частини самого передаваного відкритого тексту як ключа до шифру і новий спосіб шифрування, котрий увійшов до історії як ґрати Кардано. Для виготовлення ґрат брався лист із твердого матеріалу (картон, пергамент, метал), котрий являв собою квадрат, в якому вирізано "вікна". При шифруванні ґрати накладалися на аркуш паперу і літери відкритого тексту вписувалися у "вікна". По заповненні всіх "вікон" ґрати поверталися на 90° – знову літери відкритого тексту вписувалися у "вікна" повернених ґрат. Потім знову здійснювалось повертання на 90° і т. д. За один "захід" ґрати працювали чотири рази. Якщо текст було зашифровано не цілковито, то ґрати ставилися у вихідне положення – і вся процедура повторювалася. Це є не що інше, як шифр переставляння.

Головна вимога до ґрат Кардано: за всіх повертань "вікна" не повинні потрапляти на одне й те саме місце в квадраті, в якому утворюється шифртекст.

Якщо в квадраті після зняття ґрат утворилися порожні місця, то в них вписувалися довільні літери. Потім літери квадрата виписувалися порядково, що й становило шифрований текст.

Запропонований Кардано шифр-ґрати покладено в основу славнозвісного шифру Рішельє, в якому шифрований текст мав вигляд "безневинного" послання. З цупкого матеріалу вирізувався прямокутник розміром, приміром, 7×10; у ньому робилися "вікна". Секретний текст вписувався в ці „вікна", потім ґрати знімалися – і клітинки, що вони залишилися, заповнювалися у такий спосіб, аби вийшло "безневинне" повідомлення. Зрозуміло, використання цього шифру спричинює утруднення й вимагає відповідного інтелекту.

Блез де Віженер (XVI ст.), посол Франції в Римі, ознайомившись з працями Тритемія, Белазо, Кардано, Порта, Альберті, також захопився криптографією. 1585 року він написав "Трактат про шифри", в якому викладено основи криптографії. У цій праці він зауважує: "Усі речі в світі являють собою шифр. Уся природа є просто шифром і секретним посланням". Цю думку було пізніше повторено Блезом Паскалем – одним з основоположників теорії ймовірностей, а потім і Норбертом Вінером – "батьком" кібернетики. У цьому трактаті знову „взято на озброєння" ідею використання самого відкритого тексту як ключа. Заздалегідь обумовлюється одна ключова літера абетки, й перша літера повідомлення шифрується таблицею Тритемія за рядком, що він відповідає першій літері шифрованого повідомлення, і т. д. Отже, було зреалізовано ідею, раніше запропоновану Кардано.

Система Віженера є подібна до такої системи шифрування Цезаря, в якій ключ підставляння змінюється від літери до літери. Цей шифр багатоабеткової

заміни можна описати таблицею шифрування, яку називають таблицею (квадратом) Віженера. У додатку Б подано таблицю Віженера для української абетки.

Таблиця Віженера використовується для зашифровування й розшифровування. Таблиця має два входи:

- верхній рядок підкреслених символів, який використовується для зчитування чергової літери вихідного відкритого тексту;
- крайній лівий стовпець ключа.

Послідовність ключів зазвичай здобувають з числових значень літер ключового слова.

При шифруванні вихідного повідомлення його виписують у рядок, а під ним записують ключове слово (чи фразу). Якщо ключ виявився коротше за повідомлення, то його циклічно повторюють. У перебігу шифрування відшукують у верхньому рядку таблиці чергову літеру вихідного тексту й у лівому стовпці – чергове значення ключа. Чергова літера шифртексту перебуває на перетинанні стовпця, визначуваного зашифровуваною літерою, і рядка, визначуваного числовим значенням ключа. Нехай ключова послідовність має довжину r, тоді ключ r-абеткового підставляння є r-рядок

$$\bar{\pi} = (\pi\ \pi_0, \pi_1, ..., \pi_{r-1}).$$

Система шифрування Віженера перетворює відкритий текст $\bar{x} = (x_0, x_1, ..., x_{n-1})$ на шифртекст $\bar{y} = (y_0, y_1, ..., y_{n-1})$ за допомогою ключа $\bar{\pi} = (\pi_0, \pi_1, ..., \pi_{n-1})$ згідно з правилом

$$T_\pi\ \bar{x} = (x_0, x_1, ..., x_{n-1}) \rightarrow \bar{y} = (y_0, y_1, ..., y_{n-1});$$

$$(y_0, y_1, ..., y_{n-1}) = (\pi_0(x_0), \pi_1(x_1), ..., \pi_{n-1}(x_{n-1})),$$

де $\pi_i = \pi_{(i \bmod r)}$.

Недолік цього шифру – його слабка стійкість: якщо використовувана таблиця Тритемія є відома, то для дешифрування досить опробувати першу (ключову) літеру – і шифр "розколюється".

Другий варіант використання таблиці Тритемія, запропонований Віженером, полягає в застосуванні гасла. Власне Віженер сполучив підходи Тритемія, Белазо, Порта до шифрування відкритих текстів, істотно не внісши до них нічого оригінального.

Пізніше шифр Віженера значно спростив для його практичного використання граф Гронсфельд – керівник першого в Німеччині державного дешифрувального органа ("криптографічної лабораторії"). Його пропозиція призвела до появи так званого шифру гаммування – одного з найпоширеніших шифрів у сучасній криптографії. Суть цієї пропозиції полягає в такому.

Випишемо латинську абетку:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

За ключ-гасло обирається число, котре легко запам’ятовується, наприклад 13579. Це гасло періодично виписується над літерами відкритого тексту (одна

цифра над літерою). При шифруванні літера відкритого тексту замінюється на літеру, котра відстоїть від неї праворуч (циклічно) в абетці на кількість літер, зумовлюваних відповідною цифрою гасла. Так, наприклад, за зазначеного гасла слово **THE TABLE** перетворюється на шифровану послідовність **UKJAJCOJ**.

Подальша модернізація призвела в наш час до шифру модульного гаммування.

Пронумеруємо літери абетки: A = 01, B = 02, C = 03, …, Z = 26.

Слово **THE TABLE** набуває вигляду:

20.08.05.20.01.02.12.05.

Застосуємо операцію циклічного (модульного) додавання. Від звичайного додавання ця операція відрізнюється тим, що, якщо сума перевищує 26, від неї віднімається 26; обернена операція – віднімання схарактеризовується тим, що, якщо в результаті виходить від'ємне число, до нього додається 26.

Зашифровування провадиться за операцією модульного додавання. Випишемо гасло 13579 періодично під відкритим текстом і складемо відповідні числа. Здобудемо шифртекст: 21.11.10.01.10.13.15.10., що відповідає сполученню літер **UKJAJCOJ**. При розшифровуванні гасло віднімається з літер шифртексту.

Астрологічні захоплення Віженера навернули його до шифру, в якому шифрзнаками є положення небесних тіл у момент шифрування. Він намагався перевести свої послання на "мову неба".

Історія іноді "забувається" на сторіччя. Нашого часу шифр Віженера, який полягає в періодичному продовженні ключового слова за таблицею Тритемія, витіснив імена попередників. При цьому цей шифр часто зпримітизовується до елементарності, завдаючи образи його авторові. На початку XX сторіччя один з популярних американських журналів подав дуже спрощену систему Віженера як шифр, який "неможливо розкрити!".

Шифри Віженера з коротким періодичним гаслом використовуються й у наші дні в системах шифрування, від яких не вимагається високої криптографічної стійкості. Приміром, ці шифри використовуються в програмі-архіваторі "ARJ", у програмі "Word for Windows" (версія 2.6) тощо.

Шифр Віженера надалі модернізувався. Так, у XIX сторіччі англійський адмірал Бофор запропонував використовувати таблицю, подану на рис. 3.2. У такої таблиці є одна перевага: правила зашифровування й розшифровування за нею збігаються: і в тім, і в тім разі літери вилучаються з верхнього ряду абетки. Це створює певні зручності при використанні шифрів: не треба запам'ятовувати два різні правила (зашифровування й розшифровування).

Зауважимо, що з розвиненням математики зникла потреба у таблицях Віженера й Бофора при зашифровуванні й розшифровуванні.

У XVII сторіччі Дж. Фальконер (Англія) видав книгу "Розкриття секретних повідомлень". У ній викладено деякі розроблені ним методи дешифрування. Зокрема він запропонував використовувати перебирання можливих відкритих слів за їхньою довжиною, якщо в шифрованому тексті залишалося розбивання на слова.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z

Рисунок 3.2 – Шифр Бофора для англійської абетки

Запропонована Фальконером система шифрування поєднує два шифри: вертикального переставляння й гаммування. Наведемо приклад. Оберемо гасло ЛІЛІПУТ. За цим гаслом будується так званий номерний ряд за таким правилом: літери гасла нумеруються за абеткою, при цьому однакові літери набувають послідовних номерів. Зазначеному гаслові відповідає такий номерний ряд: 3 1 4 2 5 7 6

АБВГДЕЄ ЖЗИ І Ї Й К Л М Н О П РС Т У ФХЦЧШЩЬЮЯ
1 3 5 6 7
2 4

Зашифруємо фразу ШИФР ВЕРТИКАЛЬНОГО ПЕРЕСТАВЛЯННЯ. При шифруванні фраза виписується в прямокутник розміром 5×6 без прогалин поміж словами. Стовпці позначаються цифрами номерного ряду.

3	1	4	2	5	6
ш	и	ф	р	в	е
р	т	и	к	а	л
ь	н	о	г	о	п
е	р	е	с	т	а
в	л	я	н	н	я

Первинний шифртекст утворюється шляхом виписування літер по стовпцях, а самі стовпці слідують один за одним у порядку, визначуваному номерним рядом. Здобудемо

ИТНРЛРКГСНШРЬЕВФИОЕЯВАОТНЕЛПАЯ

Потім цей первинний шифртекст удруге шифрується шифром модульного гаммування.

Окремим випадком системи шифрування Віженера є система шифрування Вернама. Конкретна версія цього шифру, запропонована 1926 року Гілбертом Вернамом, співробітником фірми AT&T США, використовує двійкове подання символів вихідного тексту (модуль $m = 2$).

Кожен символ вихідного відкритого тексту з англійської абетки {A, B, C, D, ..., Z}, розширеного шістьма допоміжними символами (прогалина, повернення каретки й т. п.), передусім кодувався в п'ятибітовий блок (b_0, b_1, …, b_4) телеграфного коду Бодо. Випадкова послідовність двійкових ключів k_0, k_1, k_2, ... заздалегідь записувалася на паперовій стрічці. Шифрування вихідного тексту, попередньо перетвореного на послідовність двійкових символів x, здійснювалося шляхом додавання за модулем 2 символів x з послідовністю двійкових ключів k. Символи шифртексту

$$y = x \oplus k.$$

Розшифровування полягає в додаванні за модулем 2 символів y шифртексту з тією самою послідовністю ключів k:

$$x = y \oplus k = x \oplus k \oplus k.$$

При цьому послідовності ключів, використовувані при шифруванні й розшифровуванні, компенсують одна одну (при додаванні за модулем 2) – і як наслідок відновлюються символи *x* вхідного тексту.

При розроблянні своєї системи Вернам перевіряв її за допомогою закільцьованих стрічок, установлених на передавачі й приймачі для того, аби використовувалась одна й та сама послідовність ключів.

Слід зазначити, що метод Вернама не залежить від довжини послідовності ключів і, окрім того, дозволяє використовувати випадкову послідовність ключів. Однак при реалізації методу Вернама виникають серйозні проблеми, пов'язані з необхідністю доставляння одержувачеві такої самої послідовності ключів, як і у відправника, або з необхідністю безпечного зберігання ідентичних послідовностей ключів у відправника й одержувача. Ці недоліки системи шифрування Вернама подолано при шифруванні методом гаммування.

3.2 Роторні машини

У 20-х роках XX сторіччя було винайдено електромеханічні пристрої шифрування, котрі автоматизують процеси шифрування й дешифрування. Робота таких машин базується на принципі багатоабеткової заміни символів вихідного тексту за довгим ключем відповідно до версії шифру Віженера. Більшість з них – американська машина SIGABA (M-134), англійська TYPEX, німецька ENIGMA, японська PURPLE - були роторними машинами.

Головною деталлю роторної машини є ротор (чи колесо) із дротовими перемичками всередині. Ротор має форму диска (розміром з хокейну шайбу). На кожному боці диска розташовано рівномірно за колом *m*-електричні контакти, де *m* – кількість знаків абетки (в разі латинської абетки *m* = 26, української – 33). Кожен контакт на передньому боці диска з'єднано з одним з контактів на задньому боці. Як наслідок електричний сигнал, котрий являє собою знак, буде переставлено відповідно до того, як він проходить через ротор від переднього боку до заднього.

Приміром, ротор можна закомутувати дротовими перемичками для підставляння А замість Ф, Б – замість У, С – замість Л і т. п. При цьому вихідні контакти одного ротора мають приєднуватися до вхідних контактів ротора, який слідує за ним. Тоді, наприклад, якщо на клавіатурі чотирироторної машини натискалася клавіша А, то перший ротор міг перетворити її на літеру Ф, яка, пройшовши через другий ротор, могла стати літерою Т, яку третій ротор міг замінити на літеру К, котра могла бути перетворена четвертим ротором на літеру Е шифртексту. Після цього ротори повертались – і наступного разу заміна була іншою. Аби спантеличити криптоаналітиків, ротори оберталися з різною швидкістю.

Роторна машина може бути налаштована за ключем зміною будь-яких її змінних:

- роторів;
- порядку розташування роторів;
- кількості місць зупинки на колесо;
- характеру руху і т. д.

Оскільки перекомутовувати ротори складно, то зазвичай на практиці машини забезпечували комплектом роторів, у якому перебувало більше роторів, аніж можна водночас розмістити в машині. Первинне налаштовування за ключем здійснювалося вибором роторів, які складають комплект. Вторинне налаштовування за ключем здійснювалося вибором порядку розташування роторів у машині й установленням параметрів, керуючих рухом машини. З метою утруднення розшифровування шифртекстів неправочинним користувачем ротори щодня переставляли місцями чи замінювали. Більша частина ключа визначала початкові положення роторів і конкретні переставляння на комутаційній дошці, за допомогою якої здійснювалося початкове переставляння вихідного тексту до його шифрування.

Роторні машини були найважливішими криптографічними пристроями під час другої світової війни й домінували, принаймні, до кінця 50–х років минулого сторіччя.

3.3 Одноразова система шифрування

Майже всі застосовувані на практиці шифри схарактеризовуються як умовно надійні, оскільки вони можуть бути в принципі розкриті за наявності необмежених обчислювальних можливостей. Абсолютно надійні шифри не можна зруйнувати навіть за використання необмежених обчислювальних можливостей. Існує єдиний такий шифр, застосовуваний на практиці, – одноразова система шифрування. Характерною рисою одноразової системи шифрування є одноразове використання ключової послідовності.

Одноразова система шифрує вихідний відкритий текст

$$\overline{X} = (X_0, X_1, ..., X_{n-1})$$

на шифртекст

$$\overline{Y} = (Y_0, Y_1, ..., Y_{n-1})$$

за допомогою підставляння Цезаря

$$Y_i = (X_i + K_i) \bmod m, \ 0 < i < n,$$

де K_i – i-й елемент випадкової ключової послідовності.

Ключовий простір $\overline{K}$ одноразової системи являє собою набір дискретних випадкових величин з $\overline{Z}_m$ і містить m^n значень.

Процедура розшифровування описується співвідношенням

$$X_i = (Y_i - K_i) \bmod m,$$

де K_i – i-й елемент тієї ж самої випадкової ключової послідовності.

Одноразову систему винайдено 1917 року американцями Дж. Моборном та Г. Вернамом. Для реалізації цієї системи підставляння іноді використовують одноразовий нотатник. Цей нотатник складено з відривних листків, на кожному з яких надруковано таблицю з випадковими числами (ключами) K_i. Нотатник

виконується у двох екземплярах: один використовується відправником, а другий – одержувачем. Для кожного символу X_i повідомлення використовується свій ключ K_i з таблиці лише одноразово. Після того як таблицю використано, її має бути вилучено з нотатника і знищено. Шифрування нового повідомлення розпочинається з нового листка.

Цей шифр є абсолютно надійний, якщо набір ключів K_i є насправді випадковий і непередбачуваний. Якщо криптоаналітик спробує використовувати для заданого шифртексту всі можливі набори ключів і відновити всі можливі варіанти вихідного тексту, то вони усі виявляться рівноймовірними. Не існує жодного способу обрати вихідний текст, що його було насправді надіслано. Теоретично доведено, що одноразові системи є нерозкривними системами, оскільки їхній шифртекст не містить достатньої інформації для відновлення відкритого тексту.

Здавалося б, що завдяки даному достоїнству одноразові системи варто застосовувати завжди, коли є вкрай потрібна абсолютна інформаційна безпека. Однак можливості застосовування одноразової системи є обмежені чисто практичними аспектами. Істотним моментом є вимога одноразового використання випадкової ключової послідовності. Ключова послідовність з довжиною, не меншою за довжину повідомлення, повинна передаватися одержувачеві повідомлення заздалегідь чи окремо певним секретним каналом. Ця вимога не буде надто обтяжливою для передавання насправді важливих одноразових повідомлень, наприклад гарячою лінією Москва – Київ. Однак така вимога практично є нездійсненна для сучасних систем опрацьовування інформації, де потрібно зашифровувати безліч мільйонів символів.

У деяких варіантах одноразового нотатника вдаються до більш простого керування ключовою послідовністю, але це призводить до певного зниження надійності шифру. Наприклад, ключ обумовлюється зазначенням місця в книзі, відомій і відправникові й одержувачеві повідомлення. Ключова послідовність розпочинається з певного місця цієї книги й використовується в такий самий спосіб, як і в системі Віженера. Іноді такий шифр називають шифром з рухомим ключем.

3.4 Приклади розв'язування криптографічних завдань за допомогою багатоабеткових шифрів

3.4.1 Шифрування за допомогою таблиці Віженера

Нехай за ключове обране слово *АМБРОЗІЯ*. Необхідно зашифрувати повідомлення *ПРИЛІТАЮ СЬОМОГО*.

Випишемо відкрите повідомлення в рядок і запишемо під ним ключове слово з повторенням. В третій рядок будемо виписувати літери шифртексту, визначувані з таблиці Віженера (додаток Б).

Повідомлення	П	Р	И	Л	І	Т	А	Ю
Ключ	А	М	Б	Р	О	З	І	Я
Шифртекст	П	В	І	Б	Ш	Ь	І	Ь

С	Ь	О	М	О	Г	О
А	М	Б	Р	О	З	І
С	Й	П	В	В	Ї	Ш

3.4.2 Шифрування за допомогою шифру Гронсфельда

Шифр складної заміни, називаний *шифром Гронсфельда*, являє собою модифікування шифру Цезаря з числовим ключем. Для цього під літерами відкритого повідомлення записують цифри числового ключа. Якщо ключ є коротший за повідомлення, то його запис циклічно повторюють. Шифртекст здобувають приблизно так само, як в шифрі Цезаря, але відлічують за абеткою не третю літеру (як це чинять в шифрі Цезаря), а обирають ту літеру, котру зміщено за абеткою на відповідну цифру ключа. Приміром, застосовуючи як ключ групу з чотирьох початкових цифр числа *e* (основу натурального логарифму), а саме 2718, здобуваємо для відкритого повідомлення *БЕЗ ОХОТИ НЕМА РОБОТИ* такий шифртекст:

Повідомлення	**Б**	**Е**	**З**	**О**	**Х**	**О**	**Т**	**И**	**Н**	**Е**	**М**	**А**	**Р**	**О**	**Б**	**О**	**Т**	**И**
Ключ	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**
Шифртекст	**Г**	**Й**	**И**	**Ц**	**Ч**	**Х**	**У**	**О**	**П**	**Й**	**Н**	**З**	**Т**	**Х**	**В**	**Ц**	**Ф**	**Н**

Слід зазначити, що шифр Гронсфельда розкривається відносно легко, якщо врахувати, що в числовому ключі кожна цифра має лише десять значень, а отже, є лише десять варіантів прочитання кожної літери шифртексту. З іншого боку, шифр Гронсфельда припускає подальші модифікування, що вони поліпшують його стійкість, зокрема подвійне шифрування різними числовими ключами.

Шифр Гронсфельда являє собою, власне кажучи, окремий випадок системи шифрування Віженера.

3.4.3 Шифрування за допомогою подвійного квадрата

1854 року англієць Чарльз Уїтстон розробив новий метод шифрування біграмами, котрий називають подвійним квадратом. Своєї назви цей шифр дістав за аналогією з полібіанським квадратом. Шифр Уїтстона відкрив новий етап в історії розвинення криптографії. На відміну від полібіанського, шифр "подвійний квадрат" використовує одразу дві таблиці (рис. 3.3), розміщувані на одній горизонталі, а шифрування здійснюється біграмами, як у шифрі Плейфейра. Ці не надто складні модифікації призвели до з′явлення на світ якісно нової криптографічної системи ручного шифрування. Шифр "подвійний квадрат" виявився вельми надійним та зручним і застосовувався в Німеччині навіть у роки другої світової війни.

Пояснімо процедуру шифрування цим шифром на прикладі. Нехай є дві таблиці з довільно розташованими в них українськими абетками. Перед зашифровуванням повідомлення розбивають на біграми. Кожна біграма шифрується окремо. Першу літеру біграми відшукують у лівій таблиці, а другу літеру – у правій таблиці. Потім подумки будують прямокутник у такий спосіб, аби літери біграми містилися в його протилежних вершинах. Інші дві вершини цього прямокутника надають літери біграми шифртексту.

Ж	**Щ**	**Н**	**Ю**	**Р**
И	**Т**	**Ь**	**Ц**	**Б**
Я	**М**	**Е**	**Л**	**С**
В	**І**	**П**	**Ч**	**А**
Х	**Д**	**У**	**О**	**К**
З	**Є**	**Ф**	**Г**	**Ш**

И	**Ч**	**Г**	**Я**	**Т**
Ф	**Ж**	**Ь**	**М**	**О**
З	**Ю**	**Р**	**В**	**Щ**
Ц	**У**	**П**	**Е**	**Л**
Є	**А**	**Н**	**Б**	**Х**
І	**К**	**С**	**Ш**	**Д**

Рисунок 3.3 – Дві таблиці з довільно розташованими символами української абетки для шифру "подвійний квадрат"

Припустімо, що шифрується біграма вихідного тексту ИЛ. Літера И міститься в стовпці 1 і рядку 2 лівої таблиці. Літера Л міститься в стовпці 5 і рядку 4 правої таблиці. Це означає, що прямокутник утворено рядками 2 й 4, а також стовпцями 1 лівої таблиці й 5 правої таблиці. Отже, до біграми шифртексту входять літера О, розміщена в стовпці 5 і рядку 2 правої таблиці, і літера В, розташована в стовпці 1 і рядку 4 лівої таблиці, тобто здобуваємо біграму шифртексту ОВ.

Якщо обидві літери біграми повідомлення містяться в одному рядку, то й літери шифртексту беруть з того самого рядка. Першу літеру біграми шифртексту беруть з лівої таблиці в стовпці, який відповідає другій літері біграми повідомлення. Друга ж літера біграми шифртексту береться з правої таблиці в стовпці, який відповідає першій літері біграми повідомлення. Тому біграма повідомлення ТО перетворюється на біграму шифртексту ЖБ. В аналогічний спосіб шифруються всі біграми повідомлення:

Повідомлення	**ПО**		**ВТ**		**ОР**		**НА**		**ПЕ**		**РЕ**		**ДА**		**ЧА**
Шифртекст	**ЛЬ**		**ЛЖ**		**НЛ**		**ЧУ**		**ЧП**		**ЯА**		**ДА**		**УО**

Шифрування методом подвійного квадрата надає вельми стійкий до розкриття і простий у застосуванні шифр. Зламування шифртексту "подвійний квадрат" потребує потужних зусиль, при цьому довжина повідомлення має бути не менш ніж тридцять рядків.

3.5 Завдання для самоперевірки

Завдання 3.1 Зашифрувати за допомогою таблиці Віженера свої іменні дані (П.І.Б.). Ключове слово – ДОКУМЕНТАЦІЯ.

Завдання 3.2 Зашифрувати методом "подвійного квадрата" свої іменні дані.

Завдання 3.3 Зашифрувати шифром Гронсфельда свої іменні дані. Як ключ застосувати дату свого народження (наприклад, 25 березня 1987 року буде подано такою послідовністю чисел: 25031987).

4 ШИФРУВАННЯ МЕТОДОМ ГАММУВАННЯ

4.1 Накладання гамми шифру на відкритий текст

Під гаммуванням розуміють процес накладання за певним законом гамми шифру на відкриті дані. ***Гамма шифру*** – це псевдовипадкова послідовність, створена за заданим алгоритмом для зашифровування відкритих даних і розшифровування зашифрованих даних.

Процес зашифровування полягає в генеруванні гамми шифру і накладенні здобутої гамми на вихідний відкритий текст у зворотний спосіб, наприклад з використанням операції додавання за модулем 2.

Слід зазначити, що перед зашифровуванням відкриті дані розбивають на блоки $T_0^{(i)}$ однакової довжини, зазвичай по 64 біти. Гамма шифру створюється у вигляді послідовності блоків $Г_{ш}^{(i)}$ аналогічної довжини.

Рівняння зашифровування можна записати у вигляді

$$T_{ш}^{(i)} = Г_{ш}^{(i)} \oplus T_0^{(i)}, \quad i = 1 \ldots M,$$

де $T_{ш}^{(i)}$ – i-й блок шифртексту; $Г_{ш}^{(i)}$ – i-й блок гамми шифру; $T_0^{(i)}$ – i-й блок відкритого тексту; M – кількість блоків відкритого тексту.

Процес розшифровування зводиться до повторного генерування гамми шифру і накладення цієї гамми на зашифровані дані. Рівняння розшифровування має вигляд

$$T_0^{(i)} = Г_{ш}^{(i)} \oplus T_{ш}^{(i)}.$$

Здобуваний цим методом шифртекст є вельми складний для розкриття, оскільки тепер ключ є змінним. По суті, гамма шифру повинна змінюватися у випадковий спосіб для кожного зашифровуваного блока. Якщо період гамми перевищує довжину всього зашифровуваного тексту і зловмисникові невідома жодна з частин відкритого тексту, то такий шифр можна розкрити лише безпосереднім перебиранням усіх варіантів ключа. У цьому разі криптостійкість шифру визначається довжиною ключа.

4.2 Методи генерування псевдовипадкових послідовностей чисел

При шифруванні методом гаммування як ключ використовується випадковий рядок бітів, котрий поєднується з відкритим текстом, також поданим у двійковому вигляді (наприклад А = 00000, У = 00001, З = 00010 і т. д.), за допомогою побітового додавання за модулем 2 – і в результаті виходить шифрований текст.

Генерування непередбачуваних двійкових послідовностей великої довжини є однією з важливих проблем класичної криптографії. Для розв’язання цієї проблеми широко використовуються генератори двійкових псевдовипадкових послідовностей.

Генеровані псевдовипадкові ряди чисел часто називають гаммою шифру, чи просто ***гаммою*** (за назвою літери γ грецької абетки, часто використовуваної в математичних формулах для позначання випадкових величин).

Зазвичай для генерування послідовності псевдовипадкових чисел застосовують комп'ютерні програми, котрі, хоча й називаються генераторами випадкових чисел, насправді видають детерміновані числові послідовності, котрі за своїми властивостями є надто схожі на випадкові.

До криптографічно стійкого генератора псевдовипадкової послідовності чисел (гамми шифру) пред'являються три основних вимоги:

- період гамми повинен бути доволі великим для шифрування повідомлень різної довжини;
- гамма має бути практично непередбачуваною, що означає неможливість завбачати наступний біт гамми, навіть якщо відомі є тип генератора і попередній фрагмент гамми;
- генерування гамми не повинно спричинятись до великих технічних складностей.

Довжина періоду гамми є найважливішою характеристикою генератора псевдовипадкових чисел. По закінченні періоду числа розпочнуть повторюватися – і їх можна буде завбачати. Необхідна довжина періоду гамми визначається ступенем закритості даних. Чим довше є ключ, тим складніше його добрати. Довжина періоду гамми залежить від обраного алгоритму здобування псевдовипадкових чисел.

Друга вимога позв'язана з такою проблемою: у який спосіб можна вірогідно переконатися, що псевдовипадкова гамма конкретного генератора є насправді незавбачуваною? Поки що не існує таких універсальних і практично перевірних критеріїв та методик. Щоби гамма вважалася за незавбачувану, тобто істинно випадкову, необхідно, аби її період був доволі великим, а різноманітні комбінації бітів певної довжини було рівномірно розподілено по всій її довжині.

Третя вимога зумовлює можливість практичної реалізації генератора програмним чи апаратним шляхом із забезпеченням потрібної швидкодії.

Один з перших способів генерування псевдовипадкових чисел на ЕОМ запропонував 1946 року Джон фон Нейман. Суть цього способу полягає в тому, що кожне наступне випадкове число утворюється піднесенням до квадрата попереднього числа з відкиданням цифр молодших і старших розрядів. Однак цей спосіб виявився ненадійним – і від нього невдовзі відмовились.

З відомих процедур генерування послідовності псевдовипадкових цілих чисел найчастіше застосовується так званий лінійний конгруентний генератор. Цей генератор продукує послідовність псевдовипадкових чисел Y_1, Y_2, ..., Y_{i-1}, Y_i, ..., використовуючи співвідношення

$$Y_i = (a \cdot Y_{i-1} + b) \bmod m,$$

де Y_i – i-те (поточне) число послідовності; Y_{i-1} – попереднє число послідовності; a, b та m – константи; m – модуль; a – множник (коефіцієнт); b – приріст. Поточне псевдовипадкове число Y_i дістають з попереднього числа Y_{i-1} множенням його на коефіцієнт a, додаванням з приростом b та обчисленням ос-

тачі від ділення на модуль m. Дане рівняння генерує псевдовипадкові числа з періодом повторювання, котрий залежить від обираних значень параметрів a, b та m і може сягати значення m. Значення модуля m обирається дорівнюваним 2^n або простому числу, наприклад $m = 2^{31} - 1$. Приріст b має бути взаємно простим з m, коефіцієнт a має бути непарним числом.

Конгруентні генератори, що працюють за алгоритмом, запропонованим Національним бюро стандартів США, використовуються, зокрема, в системах програмування. Ці генератори мають довжину періоду 2^{24} і добрі статистичні властивості. Однак така довжина періоду є замала для криптографічних застосовувань. Окрім того, доведено, що послідовності, генеровані конгруентними генераторами, не є криптографічно стійкі.

Існує спосіб генерування послідовностей псевдовипадкових чисел на підставі лінійних рекурентних співвідношень.

Розглянемо рекурентні співвідношення та їхні різницеві рівняння:

$$\sum_{j=0}^{k} h_j a_{i+j} = 0;$$

$$a_{i+k} = -\sum_{j=0}^{k-1} h_j a_{i+j}, \qquad (4.1)$$

де $h_0 \neq 0$, $h_k = 1$ і кожне h_i належить до поля $GF(q)$.

Розв'язком цих рівнянь є послідовність елементів a_0, a_1, a_2, ... поля $GF(q)$. Співвідношення (4.1) визначає правило обчислення a_k за відомими значеннями величин a_0, a_1, a_2, ..., a_{k-1}. Потім за відомими значеннями a_0, a_1, a_2, ..., a_k визначають a_{k+1} і т. д. Як наслідок за початковими значеннями a_0, a_1, a_2, ..., a_{k-1} можна побудувати нескінченну послідовність, причому кожен її наступний член визначається з k попередніх. Послідовності такого виду легко зреалізовуються на комп'ютері; при цьому реалізація виходить особливо простою, якщо всі h_i та a_i набувають значень 0 та 1 з поля $GF(2)$.

На рис. 4.1 подано лінійну послідовну перемикальну схему, яку може бути використано для обчислення суми (4.1) і, отже, для обчислення значення a_k за значеннями k попередніх членів послідовності. Вихідні величини a_0, a_1, a_2, ..., a_{k-1} вміщують в розряди зсувового регістру, послідовні зсунення вмісту якого відповідають обчисленню послідовних символів; при цьому вихід i-го зсунення дорівнює a_i. Даний пристрій називають генератором послідовності чисел, побудованим на базі зсувового регістру з лінійним зворотним зв'язком.

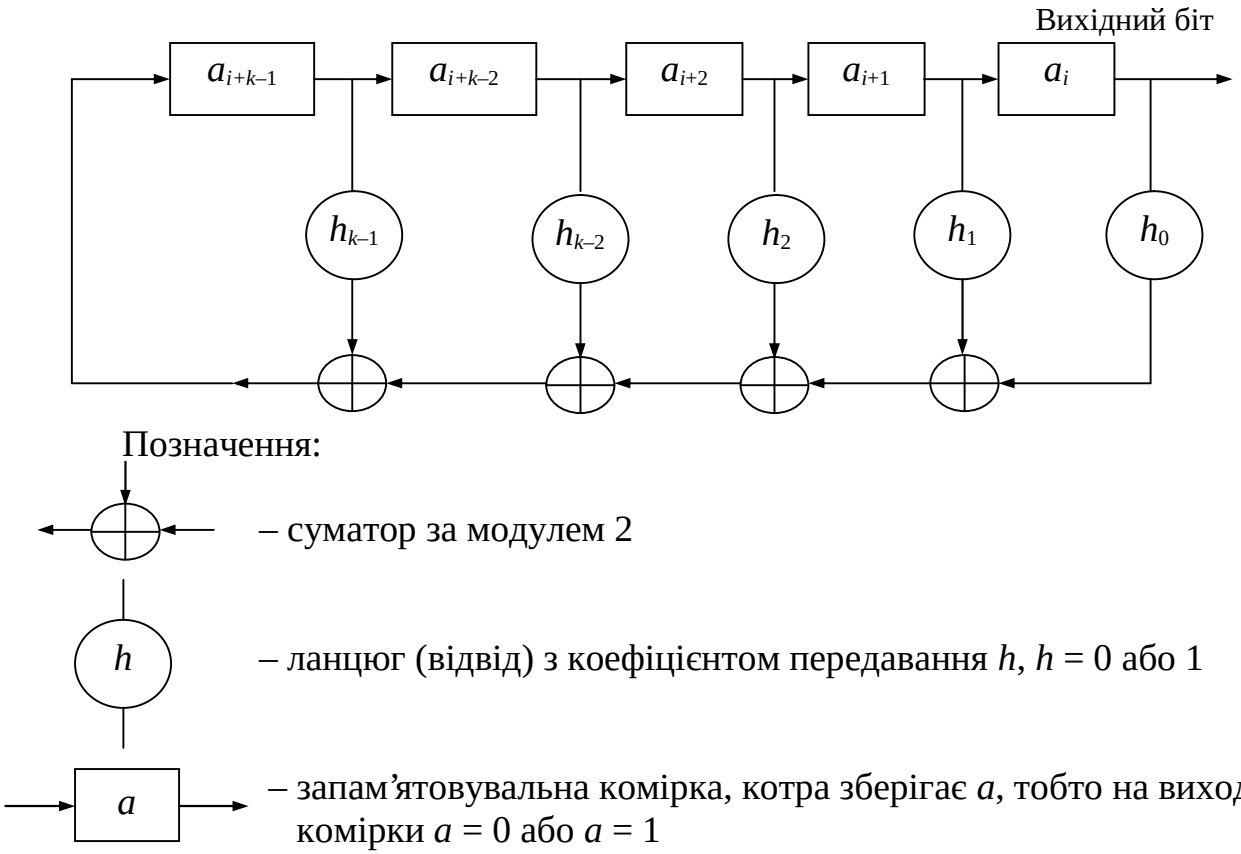


Рисунок 4.1 – Генератор з регістром зсування

Розв'язки лінійних рекурентних співвідношень, зреалізовувані генератором з регістром зсунення, описуються такою теоремою. Нехай багаточлен

$$h\,(X) = \sum_{j=0}^{k} h_j\ X^j,$$

де X – формальна змінна; h^j – коефіцієнт при X^j, який набуває значення 0 чи 1; $h_0 \neq 0$, $h_k = 1$, і нехай n – найменше ціле додатне число, для якого багаточлен $X^n - 1$ ділиться на $h(X)$. Окрім того, багаточлен

$$g(X) = (X^n - 1) / h\,(X).$$

Тоді розв'язки рекурентних співвідношень

$$\sum_{j=0}^{k} h_j\ a_{i+J} = 0$$

у вигляді послідовності елементів $a_0, a_1, a_i, \ldots, a_{n-1}$ є періодичні з періодом n і сукупність, складена з перших періодів усіх можливих розв'язків, розглядуваних як багаточлени за модулем $(X^n - 1)$, тобто

$$a\,(X) = a_0\ X^{n-1} + a_1\ X^{n-2} + \ldots + a_{n-2}\ X + a_{n-1},$$

збігається з ідеалом, породженим багаточленом $g(X)$ в алгебрі багаточленів за модулем $(X^n - 1)$.

Зауважимо, що якщо за такого визначення багаточлена $a(X)$ елементи a_0, a_1, a_2, … обчислюються в порядку зростання номерів, то коефіцієнти багато-

члена $a(X)$ обчислюються, розпочинаючи з коефіцієнтів при ступенях вищих порядків. Слід також зазначити, що вигляд багаточлена

$$h(X) = \sum_{j=0}^{k} h_j X^j$$

визначає конфігурацію зворотних зв'язків (відводів) h_j в генераторі зі зсувовим регістром. Інакше кажучи, якщо в багаточлена $h(X)$ коефіцієнт $h_j = 1$, це означає, що відвід h_j у схемі генератора наявний, якщо ж у багаточлена $h(X)$ коефіцієнт $h_j = 0$, то відвід h_j в схемі генератора є відсутній. У якості $h(X)$ необхідно обирати незвідний примітивний багаточлен. За такого обрання багаточлена $h(X)$ зі старшим ступенем m генератор забезпечує видавання псевдовипадкової послідовності двійкових чисел з максимально можливим періодом $2^m - 1$.

Розглянемо за приклад трирозрядний зсувовий регістр з лінійним зворотним зв'язком (рис. 4.2), побудований відповідно до незвідного примітивного багаточлена

$$h(X) = X^3 + X^2 + 1,$$

де коефіцієнти $h_3 = 1$, $h_2 = 1$, $h_1 = 0$, $h_0 = 1$.

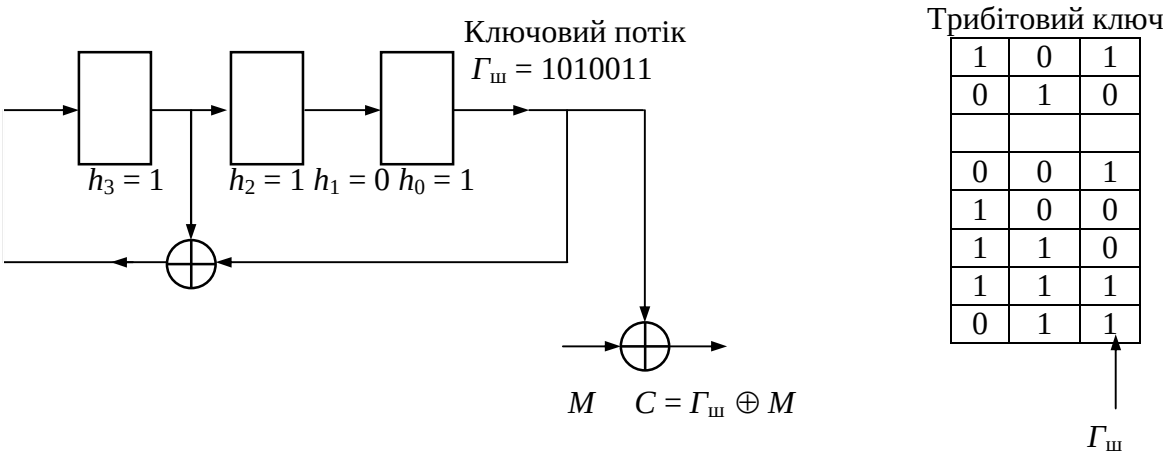


Рисунок 4.2 – Трирозрядний регістр зсування зі зворотними зв'язками

Нехай ключем є 101. Регістр розпочинає працювати з цього стану; послідовність станів регістру наведено на рисунку 4.2. Регістр проходить через усі сім ненульових станів – і знову повертається до свого вихідного стану 101. Це є найдовший період даного регістру з лінійним зворотним зв'язком. Така послідовність називається *послідовністю максимальної довжини* для зсувового регістра (Maximal Length Shift Register Sequence – MLSRS). За будь-якого цілого m існує m-бітова послідовність MLSRS з періодом $2^m - 1$. Зокрема за $m = 100$ послідовність матиме період $2^{100} - 1$ і не повторюватиметься 10^{16} років при передаванні лініями зв'язку зі швидкістю 1 Мбіт/с.

У нашому прикладі вихідною послідовністю (гаммою шифру) $Г_ш$ зсувового регістру зі зворотним зв'язком є послідовність 1010011, котра циклічно повторюється. У цій послідовності є чотири одиниці й три нулі і їхній розподіл є настільки близький до рівномірного, наскільки це є можливе в послідовності,

котра має довжину 7. Якщо розглянути пари послідовних бітів, то пари 10 та 01 з'являються двічі, а пари 00 та 11 – одноразово, що знову стає настільки близьким до рівномірного розподілу, наскільки це є можливо. У разі послідовності максимальної довжини для m-розрядного регістру ця властивість рівнорозподілюваності поширюється на трійки, четвірки й т. д. бітів, аж до m-бітових груп. Внаслідок такої близькості до рівномірного розподілу послідовності максимальної довжини часто використовуються в якості псевдовипадкових послідовностей у криптографічних системах, котрі імітують роботу криптостійкої системи одноразового шифрування.

Хоча така криптографічна система здійснює імітацію завбачувано криптостійкої системи одноразового шифрування, сама вона не відрізняється стійкістю і може бути розкрита за кілька секунд роботи комп'ютера за умови наявності відомого відкритого тексту.

Якщо відводи регістру зі зворотним зв'язком зафіксовано, то для віднайдення початкового стану регістру доволі знати m бітів відкритого тексту. Щоб віднайти m бітів ключового потоку, m бітів відомого відкритого тексту складають за модулем 2 з відповідними m бітами шифртексту. Здобуті m бітів дають стан зсувного регістру зі зворотним зв'язком у зворотному напрямку на певний момент часу. Потім, моделюючи роботу регістру у зворотному напрямку, можна визначити його вихідний стан.

Якщо відводи регістру зі зворотним зв'язком не є фіксовані, а є частиною ключа, то досить $2m$ бітів відомого відкритого тексту, аби порівняно швидко визначити розташування відводів регістру та його початковий стан.

Нехай $S(i)$ – вектор-стовпець, який складається з m символів 0 та 1 й визначає стан регістру в i-й момент часу. Тоді

$$S(i + 1) = A \cdot S(i) \bmod 2,$$

де A – матриця розміром $m \times m$, котра визначає положення відводів регістру зі зворотним зв'язком.

Для трирозрядного регістру (див. рис. 4.2)

$$A = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix}.$$

Матриця A завжди має таку структуру: у її першому рядку відбито послідовність відводів у регістрі, безпосередньо під головною діагоналлю розташовуються одиниці, а в решті позицій – нулі.

$2m$ бітів відомого відкритого тексту дозволяють обчислити $2m$ послідовних бітів ключового потоку. Для спрощення позначень припустімо, що це – перші $2m$ бітів ключового потоку. Отже,

S (1) – перша група m відомих бітів ключового потоку;

S (2) – наступна група (розпочинаючи з номера 2) з m відомих бітів ключового потоку;

S (m + 1) – остання група з m відомих бітів ключового потоку.

Далі можна утворити дві матриці розміром $m \times m$:

$$X(1) = [S(1), S(2), \ldots, S(m)];$$

$$X(2) = [S(2), S(3), \ldots, S(m + 1)],$$

пов'язані співвідношенням

$$X(2) = \mathrm{A} \cdot X(1) \bmod 2.$$

Можна довести, що для будь-якої послідовності максимальної довжини матриця $X(1)$ завжди є несингулярна, тому матрицю A можна обчислити як

$$A = X(2)\,[X(1)]^{-1} \bmod 2.$$

Обертання матриці $X(1)$ потребує (щонайбільш) біля m^3 операцій, тому легко виконується за будь-якого поміркованого значення m.

Для криптографії послідовності максимальної довжини MLSRS можна зробити більш криптостійкими, використовуючи нелінійну логіку. Зокрема, як ключовий потік використовується нелінійно "фільтрований" вміст зсувового регістру, а для здобуття послідовності максимальної довжини – лінійний зворотний зв'язок, як це подано на рис. 4.3.

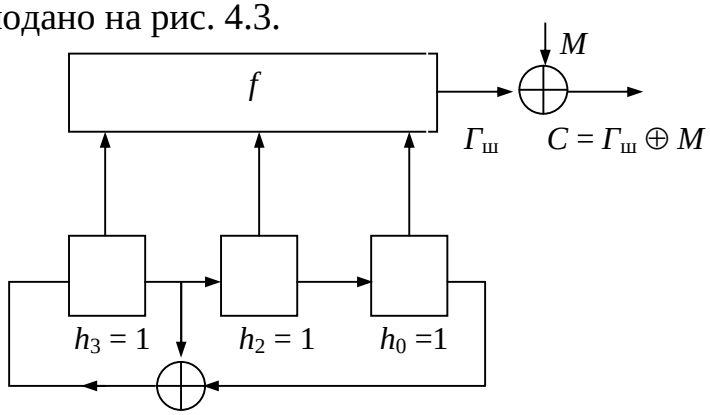


Рисунок 4.3 – Лінійний зсувовий регістр
з нелінійними логічними ланцюгами на виході

Функція f має обиратися у такий спосіб, аби забезпечити оптимальний баланс поміж нулями й одиницями, а „фільтрована" послідовність має розподіл, близький до рівномірного. Необхідно також, аби „фільтрована" послідовність мала великий період. Якщо $(2^m - 1)$ є простим числом (як у прикладі: за $m = 3$ маємо $2^3 - 1 = 7$), то „фільтрована" послідовність може мати період $(2^m - 1)$ (при обранні структури зсувового регістру відповідно до незвідного примітивного багаточлена $h(X)$ ступеня m). До згаданих значень m належать, зокрема, такі: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, а здобуті в такий спосіб прості числа називаються *простими числами Мерсена*.

Незважаючи на те, що „фільтровану" вихідну послідовність зазвичай не можна здобути за допомогою m-розрядного зсувового регістру з лінійним зворотним зв'язком, її завжди можна здобути за допомогою зсувового регістру більшої довжини з лінійним зворотним зв'язком. Регістр довжиною $(2^m - 1)$ завжди дозволить це зробити, а іноді для цього придатен і більш короткий регістр.

5 ДЕШИФРУВАННЯ КЛАСИЧНИХ ШИФРІВ

5.1 Дешифрування шифру простої заміни

Уведемо математичні моделі відкритих текстів, використовувані при криптографічному аналізуванні шифрів, а також окреслимо певні частісні властивості відкритих текстів. Далі використаємо деякі з цих властивостей і акцентуємо увагу на ймовірнісно-статистичних закономірностях, які мають місце у відкритому тексті й використовуються при дешифруванні шифрів простої заміни й переставляння.

Існують стійкі закономірності відкритого тексту, які слід враховувати при дешифруванні шифрів простої заміни й переставляння. Можливість дешифрування певного шифру значною мірою залежить від того, наскільки криптографічні перетворення руйнують ймовірнісно-статистичні закономірності, наявні у відкритому тексті. До найбільш стійких закономірностей відкритого повідомлення належать такі:

1) в осмислених текстах кожної природної мови різні літери зустрічаються з різною частістю, при цьому відносні частості вживання літер у різних текстах однієї мови є близькі поміж собою. Те ж саме можна стверджувати й про частості вживаності пар, трійок літер відкритого тексту;

2) будь-яка природна мова має так звану надлишковість, що дозволяє з великою ймовірністю "вгадувати" зміст повідомлення, навіть якщо частина літер у повідомленні є невідома.

У таблиці 5.1 зазначено відносну частість вживаності літер абетки російської мови.

Таблиця 5.1 – Частість вживаності літер абетки російської мови

1	а - 0,062	11	к - 0,028	21	ф - 0,002
2	б - 0,014	12	л - 0,035	22	х - 0,009
3	в - 0,038	13	м - 0,026	23	ц - 0,004
4	г - 0,013	14	н - 0,053	24	ч - 0,012
5	д - 0,025	15	о - 0,090	25	ш - 0,006
6	е - 0,072	16	п - 0,023	26	щ - 0,003
7	ж - 0,007	17	р - 0,040	27	ы - 0,016
8	з - 0,016	18	с - 0,045	28	ъ,ь - 0,014
9	и - 0,062	19	т - 0,053	29	э - 0,003
10	й - 0,010	20	у - 0,021	30	ю - 0,006
				31	я - 0,018

Подібні таблиці наводяться в багатьох джерелах. Їх здобуто на підставі підрахунків частостей вживаності певних літер на великих обсягах відкритого

тексту. З огляду на те, що для експериментів залучається різний вихідний матеріал, значення ймовірностей дещо відрізнюються поміж собою.

Якщо упорядкувати літери за спаданням імовірностей, то дістанемо варіаційний ряд

О,Е,А,И,Н,Т,С,Р,В,Л,К,М,Д,П,У,Я,З,Ы,Б,Ь,Г,Ч,Й,Х,Ж,Ю,Ш,Ц,Щ,Э,Ф.

Як запам’ятати перші 10 найчастіш вживаних літер російської абетки? Пригадуєте, як запам’ятовують основні кольори у фізиці? Треба запам’ятати фразу: *Каждый охотник желает знать, где сидит фазан.* Перші літери слів фрази вказують на основні кольори. У криптографії треба запам’ятати слово СЕНОВАЛИТР — у ньому наявні всі 10 найбільш вживаних літер.

Частісна діаграма вживаності літер, зрозуміло, залежить від мови. У таблиці 5.2 подано у відсотках відносні частості найбільш уживаних літер деяких мов.

Таблиця 5.2 – Відносні частості найбільш уживаних літер деяких мов

Мова	Частість вживаності літер, %					
Англійська	e – 12,75	t – 9,25	r – 8,50	i – 7,75	h – 7,75	o – 7,50
Французька	e – 17,75	a – 8,25	s – 8,25	i – 7,25	n – 7,25	r – 7,25
Німецька	e – 18,50	n –11,50	I – 8,00	r – 7,50	s – 7,00	a – 5,00
Арабська	a – 17,75					
Грецька	a – 14,25					
Японська	p – 15,75					
Латина	a – 11,00					
Малайська	a – 20,25					
Санскрит	a – 31,25					

Частості вживаності знаків абетки залежать не лише від мови, але й від характеру тексту. Приміром, у тексті з криптографії буде підвищено ймовірність використання літер Ф, Ш (через часто вживані слова "шифр", "криптографія"). У математичному тексті ймовірніше буде завищено частість використання літери Ф (через слова "функція", "функціонал" і т. п.).

У стандартних текстових файлах найчастіше вживано символ "прогалина"; в *exe*-файлах найчастіше вживано символ 0; в текстах, написаних у текстовому процесорі ChiWriter, зручному для оформлення математичних текстів, перше місце посів символ "\" – backslash.

Частісна діаграма є стійкою характеристикою тексту. З теорії ймовірностей випливає, що за вельми слабких обмежень на ймовірнісні властивості випадкового процесу є справедливий закон великих чисел, тобто відносні частості V_k знаків збігаються за ймовірністю зі значеннями їхніх імовірностей P_k:

$$P\left\{\left|\frac{\vartheta_k}{N} - p_k\right| > \varepsilon\right\} \xrightarrow[N\to\infty]{} 0.$$

Це є слушно для послідовності незалежних випробувань, для кінцевого регулярного однорідного ланцюга Маркова. Експерименти засвідчують, що це є слушно й для відкритих текстів.

З позицій сучасної криптографії, шифри переставляння і простої заміни мають істотний недолік: вони не цілковито руйнують ймовірнісно-статистичні властивості, наявні у відкритому повідомленні.

При дешифруванні тексту, зашифрованого шифром простої заміни, використовують частісні характеристики відкритого тексту. Власне, якщо підраховувати частості вживаності знаків у шифрованому тексті, упорядкувати їх за спаданням та порівняти з варіаційним рядом імовірностей відкритого тексту, то ці дві послідовності будуть близькі. Найімовірніше перше місце посяде прогалина, далі слідуватимуть літери О, Е, А, И.

Зрозуміло, якщо текст не є надто довгий, то не є неодмінним повний збіг. Може опинитися на другому місці О, а на третьому – Е, але в кожному разі в перших і других рядах однакові літери розташовуватимуться неподалік одна від одної, й щоближче до початку (щобільше ймовірність вживання знаків), тим менше буде відстань поміж знаками.

Аналогічна картина спостерігається і для пар сусідніх літер (біграм) відкритого тексту (найчастіше зустрічається біграма російського відкритого тексту – СТ). Однак для здобуття стійкої картини довжина послідовності має бути істотно більше. На порівняно невеликих відрізках відкритого тексту ця картина є трохи розмита. Більш стійкою характеристикою біграм є відсутність в осмисленому тексті, як говорять, певних біграм; наявність заборонних біграм, котрі мають імовірність, дорівнювану практично нулю.

Чи бачили ви коли-небудь у відкритому тексті біграми ЪЬ, "голосна" Ь, "прогалина" Ь? Знання й використовування зазначених особливостей відкритого тексту значно полегшує дешифрування шифрів переставляння й заміни.

Розглянемо приклад дешифрування шифру простої заміни.

Нехай маємо такий шифртекст:

ДОЧАЛЬ ИЬЦИО ЛИОЙО ВНЫИЮШ ХЕМВЛНХЕИ ДОСОЛЬ ЧСО ИА’fy1" ТЬЖАТСР ЬАС АКЕИОЙО ДОКЩОКЗЖАЙО КПЗ РТАЩ ТПЬЧНАР ТДОТОУН ХЕМВОРНИЕЗ ЕИМОВЛНЯЕЕ РЮУОВ БВЕД СОЙВНМЕЧАТБОГ ’ ТЕТСАЛЮ ЫНРЕТЕС ОС ОТОУ АИИОТСАГ ЕИМОВЛНЯЕЕ АА ЯАИИОТСЕ Е РОЫЛОЦИОТСАГ РПНКАПШЯАР ДО ЫНЖУСА ТРОАГ ЕИМОВЛНЯЕЕ ДВАЦКА РТАЙО ДОКЧАВБИАЛУОПШХОА ВНЫИООУ ВНЫЕА РЕКОР ЫНЖЕЖНАЛОГ ЕИМОВЛНЯАА КОБЬЛАИСНПШИНЗ САПАМОИИНЗ САПАРЕЫЕОИИНЗ БОЛДШЭСАВИНЗ БНЦКЮГ РЕК ЕИМОВЛНЯЕЕ УЛААС ТРОЕ ТДАЯЕМЕЧАТБЕА ОТОУАИИОТСЕ Е ФСК ОТОЧАИИОТСЕ ТЕПШИО РПЕЗЭС ИН РЮУОВ ЛАСОКОР ХЕМВОРЙЙВЗ ЕИМОВЛНЯЕЕ УОПШХОА ЫИНЧАИЕА ЕЛАЭС ОУЪАЛЮ Е СВАУЬАЛНЗ ТБОВОТСШ ДАВАКНЧЕ ХЕМВОРНИИОГ

Роботу слід розпочати з підрахунку частості вживаності символів у шифрованому тексті. Після того як здійснено підрахунок, упорядкуємо символи за спаданням частостей:

$$b_1\ b_2\ b_3\ b_4\ b_5\ \ldots$$

Під цим рядом слід підписати варіаційний ряд імовірностей знаків у відкритому тексті:

О Е А И Н Т С Р В Л К М Д П У Я З Ы Б Ь Г Ч Й Х Ж Ю Ш Ц Щ Э Ф

За вельми великої довжини шифртексту, для того аби з шифрованого здобути відкритого тексту, стане замінити b_1 на 0, b_2 – на Е, b_3 – на А й т. д. Принаймні саме така ситуація матиме місце для найбільш імовірних літер. У нас матеріалу недостатньо. Переглянувши шифртекст після такої заміни, бачимо, що він не читається, – отже, матеріалу насправді є замало.

Що нам залишається? Вгадувати заміну. При цьому маємо все ж враховувати статистичні особливості відкритого тексту. У шифртексті через прогалину найімовірніше позначено прогалину; через літеру О – О чи А; через Е – О чи Е, чи А; через А – Е чи А, чи И й т. д.

Можна рекомендувати виписати шифртекст, а під ним у стовпець – найбільш імовірні заміни для цих літер. У нашому прикладі заміну добрано у такий спосіб, що літеру абетки замінено саме на найбільш імовірне для неї позначення. Тому сам шифртекст у даному прикладі виписувати немає потреби. Він збігається із середнім рядком послідовності стовпців найбільш імовірних замін.

Що рідше зустрічається літера, тим більшої глибини треба брати стовпець, аби була впевненість, що в стовпці міститься знак відкритого тексту. У нашому випадку стовпці взято однаковою глибиною в п’ять символів, але виписано їх лише для найчастіше вживаних літер.

При дешифруванні без використання засобів автоматизації далі треба вгадувати заміну. Якщо пильно придивитися до тексту, то зробити це не є вельми складно. В тексті є слово АА з двох часто вживаних літер. Що це може бути за слово? У російській мові немає слів ОО, ИИ, НН тощо. Так, перебираючи можливі слова, ми віднайдемо одне слово ЕЕ і дійдемо висновку, що літеру Е було замінено на А. Надто часто в шифртексті слова закінчуються біграмами ЕЕ. В російській мові типовими закінченнями є сполучення ЕЕ, ИИ. З огляду на те, що заміну для літери Е ми вже вгадали, дійдемо висновку, що в шифртексті літери И замінено на Е. Тоді усюди в шифртексті можна провести зворотну заміну. Тепер ми вже можемо вгадувати окремі слова. У такий спосіб, добряче поламавши голову, ми, як у грі "Поле чудес", зрештою відновимо увесь текст.

У стовпцях найбільш імовірних замін літери, котрі відповідають слушним зворотним замінам, має бути позначено як великі. Прочитавши відкритий текст, ви переконаєтесь, що він являє собою одну з кількох пропозицій з книги С.А. Дориченка та В.В. Ященка «25 этюдов о шифрах», М., 1994.

Для дешифрування в автоматизованому режимі насамперед слід завести до пам’яті комп’ютера словник відповідної мови.

Програма дешифрування повинна, переглядаючи шифртекст, здійснювати спробні зворотні заміни, у припущенні, що на даному фіксованому місці у відкритому тексті перебувало перевірюване слово. Після кожної заміни програма частково відновлює ключове підставляння, частково розшифровує текст і відкидає варіант підставляння, якщо в певному місці відновленого тексту виникає літеросполучення, якого не може бути у відкритому тексті розглядуваної мови. Після відновлення певної кількості замін у тексті виникають ділянки, в яких віднайдено значну кількість літер. Решта літер добираються шляхом перебирання словника і підставляння до тексту слів, які не суперечать відновленим попередньо замінам.

Слід зазначити, що практичних навичок з дешифрування шифру простої заміни можна набути лише після проведення самостійних дослідів з дешифрування.

5.2 Дешифрування шифру переставляння

Для відновлення відкритого тексту шифру переставляння слід переставити стовпці у такий спосіб, аби в рядках з'явився осмислений текст.

Розглянемо приклад дешифрування шифру переставляння восьми стовпців.

Нехай шифртекст має вигляд, наведений в таблиці 5.3.

Таблиця 5.3 – Шифртекст російською мовою

1	2	3	4	5	6	7	8
п	а	я		в		и	м
0	ч	ш	г		У		е
е	б	ж	л		е		0
м		ч	–	0	т	0	я
	е	г	е		У	с	Щ
	а	к	ь	З	а	т	т
я	Р	е		е	п		ь
	ю	З	в	а	н	в	
0	и	а	в	е	ш	л	
	е	е	я	м		п	н
ь	Р	Р	н	З	е	е	е
З	а	м	а	н		а	к
ч	с	т	а		ь	а	н
0	я	л	м		а	л	
0	ь	ч	х	т	а	т	
в		е	0	а	я	е	я
0	е	Р	м	т	ь	е	
д	с	г	ы		0	а	т
е	б	в	н		ы		
	а	у	и	н	З	н	л
	г	и	а	0	к	к	д
	а	0	б	д	г	н	
	ж	а	У	е	д	я	д
х	л	и		е	м	0	а
к	Р	т	д		ь	0	е
	ь	х	в	т	0	н	
р	л	е		е	д	а	ю
р		З	е	в		е	д
ш		в	а	е	н	е	н
т	и	и	е	в			д
		в		с	д		

Зіставимо переставлянню стовпців таблицю 8×8; при цьому поставимо на перетинанні *i*-того рядка й *j*-того стовпця одиницю, якщо *j*-тий стовпець після зворотного переставляння має слідувати за *i*-тим. Наше завдання – відновити таблицю, відповідну слушному переставлянню стовпців.

Далі попарно прилаштовуватимемо один стовпець до одного. Якщо при цьому в певних рядках виникатимуть заборонні біграми, то стовпці не зможуть у відкритому тексті слідувати один за одним, – й відповідна клітинка закреслюється. В нашому прикладі шостий стовпець не може слідувати за четвертим, тому що інакше в тексті в першому рядку йтимуть дві прогалини поспіль. Переглянемо, наприклад, шостий рядок. Якби четвертий стовпець слідував за першим, то в тексті були б слова, які розпочинаються з Ь. Після переглядання всіх рядків ми здобудемо таблицю 5.4.

Таблиця 5.4 – Дешифрування шифру переставляння

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	**X**	**X**		**X**	**X**	**X**		**X**
2		**X**		**X**		**X**		
3			**X**					**X**
4	**X**	**X**		**X**		**X**	**X**	**X**
5	**X**				**X**	**X**	**X**	**X**
6	**X**	**X**		**X**		**X**	**X**	
7	**X**			**X**	**X**	**X**	**X**	**X**
8	**X**	**X**			**X**	**X**	**X**	**X**

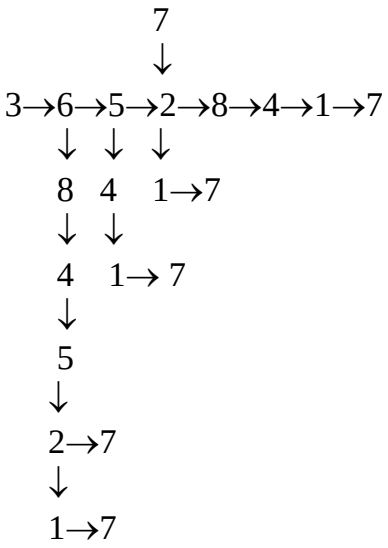
Якби текст був довшим і мав більше рядків, то в кожнім рядку й у кожнім стовпці залишилося б лише по одній незакресленій клітинці – і переставляння було б відновлено. Стосовно нашої таблиці ми можемо лише стверджувати, що шостий стовпець слідує за третім (позначимо цю подію як $3 \to 6$), якщо шостий стовпець не є останнім. Для шостого стовпця можливі два варіанти продовження:

$$\begin{array}{c} 8 \\ \downarrow \\ 3 \to 6 \to 5 \end{array}$$

Нам треба розглянути обидва варіанти й спробувати відкинути хибний. Якщо це не вдасться, то слід продовжувати обидва варіанти:

$$\begin{array}{ccc} 8 \to 4 & & 1 \\ \uparrow & & \uparrow \\ 3 \to 6 & \to 5 \to & 2 \to 7 \end{array}$$

У підсумку здобуваємо певне дерево можливого слідування стовпців у відкритому тексті:



Кожній гілці дерева відповідає певне переставляння стовпців.

Далі перевіряємо кожен варіант на осмисленість і дістаємо слушний варіант:

$$3\to6\to5\to2\to8\to4\to1\to7$$

Зауважимо, що не обов'язково було будувати дерево до кінця. Наприклад, гілку $3\to6\to8\to4\to5$ можна було відкинути одразу. Хіба можна визнати за осмислений фрагмент тексту

З	6	8	4	5
я		м		в
ш	У	е	г	
ж	е	0	л	
ч	т	я		0
г	У	Щ	е	З
к	а	т	ь	е
е	а	т		а

Така процедура відкидання гілок була б необхідна, якби рядків було дещо менше й дерево було, відповідно, набагато більш розгалуженим. Запропоновану процедуру легко автоматизувати і зробити придатною для зреалізовування на ЕОМ.

Алгоритм дешифрування має складатися з таких етапів.

1 Попередня робота. Аналізуючи вельми потужний обсяг відкритих текстів, побудувати множину заборонних біграм.

2 Попередня робота. Скласти словник усіляких v-грам для $v = 2, 3, ..., d$, які можуть зустрітися у відкритому тексті. Число d обирається виходячи з можливостей обчислювальної техніки. Побудувати таблицю 8×8. При цьому перебираються послідовно всі помітні біграми і для кожної опробуваної біграми – послідовно всі рядки. Якщо хоча б в одному рядку перший символ біграми зустрічається в i-тому стовпці, а другий – у j-тому, то клітинка $i\times j$ таблиці закреслюється.

3 Обрати певний стовпець за вихідний.

4 Розпочати процедуру побудови дерева шляхом прилаштовування до вихідного стовпця усіх варіантів стовпців.

5 Для кожного здобутого варіанта додати ще один з решти стовпців. Якщо хоча б в одному з рядків таблиці зустрінеться триграма, відсутня у словнику розміщених триграм, – то варіант відкидається.

6 Для кожного з невідкинутих варіантів додаємо ще одного стовпця і провадимо відкидання хибних варіантів за словником дозволених чотириграм.

Якщо словник побудовано лише для $d \leq 3$, то відкидання провадиться шляхом перевірки на припустимість триграм, які зустрілися в останніх трьох стовпцях кожного рядка. Продовжуємо цей процес до здійснення цілковитого переставляння. Нижче наведено відновлений для нашого прикладу текст.

Таблиця 5.5 – Відновлений текст

	1	2	3	4	5	6	7	8
1	я		в	а	м		п	и
2	ш	у		ч	е	г	0	
3	ж	е		б	0	л	е	
4	ч	т	0	1	я		М	0
5	г	У		е	Щ	е		с
6	к	а	З	а	т	ь		т
7	е	п	е	Р	ь		я	
8	З	н	а	ю		в		в
9	а	ш	е	и		в	0	л
10	е		м	е	н	я		п
11	Р	е	З	Р	е	н	ь	е
12	м		н	а	к	а	З	а
13	т	ь		с	н	а	ч	а
14	л	а		я		м	0	л
15	ч	а	т	ь		х	0	т
16	е	л	а		п	0	в	е
17	Р	ь	т	е		м	0	е
18	г	0		с	т	ы	д	а
19	в	ы		б		н	е	
20	у	З	н	а	л	и		н
21	е	к	0	г	д	а		к
22	0	г	Д	а		б		н
23	а	д	е	ж	д	У		я
24	и	м	е	л	а		х	0
25	т	ь		Р	е	д	к	0
26	х	0	т	ь		в		н
27	е	д	е	л	ю		Р	а
28	З		в		д	е	Р	е
29	в	н	е		н	а	ш	е
30	и		в	и	д	е	т	ь
31	в	а	с					

Зауваження стосовно ступеня неоднозначності відновлення відкритого тексту. В обох прикладах нам вдалося, хоча й за певних зусиль, відновити відкриті тексти. Робота з дешифрування значно полегшується зі збільшенням довжини шифртексту (чи, як говорять, обсягу наявного в розпорядженні матеріалу перехоплення). Якби обсяг матеріалу було збільшено кількаразово, то в другому прикладі в таблиці 8×8 з великою ймовірністю було б закреслено всі клітинки, окрім відповідних справжньому порядку слідування один за одним стовпців у відкритому тексті. У першому прикладі варіаційний ряд частості вживаності літер відкритого тексту майже цілковито збігався б з варіаційним рядом імовірностей знаків відкритого тексту і нам залишалося підписати один варіаційний ряд під іншим і здійснити зворотну заміну. Окремі помилки легко усувалися б при першому ж прочитуванні дешифрованого варіанта тексту. З іншого боку, при зменшенні обсягу матеріалу завдання дешифрування істотно ускладнюється. Насправді, уявіть собі, що вам запропоновано дешифрувати зашифрований за допомогою простої заміни шифртекст, складений з одного першого слова нашого першого прикладу – ДОЧАЛЬ. Для кожного слова з шести різних літер віднайдеться проста заміна, застосовуючи яку ми здобудемо даний шифртекст. Проблема полягає не в тім, аби віднайти ключове підставляння, а в тім, як обрати з численної кількості варіантів відновлених відкритих текстів саме той, котрий було зашифровано.

Отже, важливою характеристикою ефективності криптографічного захисту є ступінь неоднозначності відновлення відкритого тексту за шифрованим. Подамо якісне означення цього поняття. Під ступенем неоднозначності природно розуміти математичне сподівання кількості варіантів відкритих текстів, які може бути здобуто за застосовування алгоритму дешифрування. Якщо припустити, що за випадкового вибору хибного ключа (ключа, розбіжного зі справжнім ключем, із застосуванням якого було здобуто шифртекст, відновлений при розшифровуванні) і розшифровування на цьому випадковому хибному ключі розшифрований текст не відрізняється від випадкового тексту, то ймовірність того, що здобутий текст довжини N буде осмисленим (за класичним означенням імовірностей), дорівнює відношенню кількості сприятливих завершень – кількості $A(N)$ осмислених відкритих текстів довжини N до загальної кількості текстів довжини N, котра дорівнює, вочевидь, n^N, де n – кількість літер в абетці відкритих текстів. Для того аби дістати ступінь неоднозначності, слід помножити здобуте відношення на кількість K варіантів ключів, звідки дістаємо формулу

$$r = r(N) = KA(N)n^{-N} \qquad (5.1)$$

для обчислення ступеня неоднозначності L відновлення відкритого тексту. Отже, шифрування забезпечує надійний захист повідомлення, якщо неоднозначність відновлення відкритого тексту за шифрованим є надто велика.

Ступінь неоднозначності дозволяє класифікувати шифри за ступенем їхньої криптографічної стійкості. Якісні міркування тут є такі. Якщо неоднозначність дешифрування (можлива кількість здобуваних відкритих текстів) є $r(N)$, а

мета дешифрування визначена здобуттям відкритого справжнього тексту, то ймовірність здобуття саме його оцінюється величиною $l/r(N)$. Шифри, для яких $r(N) = A(N)$, називаються ***абсолютно (теоретично) стійкими*** (для абсолютно стійкого шифру застосування будь-якого алгоритму дешифрування не надає жодної інформації про відкритий текст). До формули (5.1), її висновку та її трактувань слід ставитися надто обережно. Насправді для здобуття абсолютної стійкості шифру досить мати n^N ключів.

Шифри, що вони теоретично не є стійкими, для яких надійність криптографічного захисту забезпечується надто великою складністю зреалізовування відомих алгоритмів дешифрування, називають ***практично стійкими***.

Шифри, котрі не належать до класів теоретично стійких чи практично стійких шифрів, називають ***шифрами тимчасової стійкості***.

Кількість осмислених відкритих текстів довжини N для великих значень N зазвичай вважається за дорівнювану 2^{HN}, де H – ентропія (в бітах) на знак відкритого тексту. Для літературного тексту, як засвідчують експериментальні розрахунки, величина H є наближена до одиниці. Для більш формалізованих текстів (організаційно-розпорядчих листів, документів тощо) величина H перебуває в межах від 0,5 до 0,8.

Повертаючи до аналізу шифру простої заміни, зауважимо, що ступінь неоднозначності відновлення відкритого тексту для цього шифру має вигляд

$$r(N) = \frac{n!2^{HN}}{n^N},$$

де H – ентропія на літеру відкритого тексту.

Шифр простої заміни є теоретично стійким при шифруванні літературного тексту (n = 32) довжиною в одне-два слова і забезпечує лише тимчасову стійкість за великого обсягу матеріалу.

Експерименти засвідчують, що практичне дешифрування шифру простої заміни для літературного тексту є можливе в разі, якщо довжина шифртексту вдвічі-втричі перевищує розмір абетки відкритого тексту, тобто дорівнює 60...100 літерам.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1 **Введение** в криптографию / Под общ. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.: ил.

2 **Барабаш А.В**., **Шанкин Г.П.** Криптография: Науч.-попул. изд. Серия «Аспекты защиты». – М.: Солон-Р, 2002. – 511 с.

3 **Романец Ю.В**., **Тимофеев П.А., Шаньгин В.Ф.** Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – М.: Радио и связь. – 328 с.

4 **Анин Б.Ю**. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.: ил.

5 **Саломаа А**. Классическая криптография: Пер. с англ. – М.: Мир, 1996. – 304 с.

6 **Петров А.А**. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.: ил.

7 **Жельников В**. Криптография от папируса до компьютера. – М.: ABF, 1997. – 336 с.

8 **Тайны** планеты Земля: Универс. ил. справочник для всей семьи: Заря. – 2002. – № 1.

ДОДАТОК А

Таблиця шифрування Тритемія

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

ДОДАТОК Б

Таблиця Віженера для української абетки

Ключ	**а**	**б**	**в**	**г**	**д**	**е**	**є**	**ж**	**з**	**и**	**і**	**ї**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ь**	**ю**	**я**
0	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
1	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
2	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
3	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
4	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
5	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д
6	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е
7	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є
8	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж
9	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з
10	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и
11	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і
12	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї
13	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й
14	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к
15	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л
16	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
17	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н
18	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
19	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
20	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
21	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
22	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
23	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
24	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
25	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
26	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
27	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
28	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
29	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
30	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
31	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

НАВЧАЛЬНЕ ВИДАННЯ

ЗАХАРЧЕНКО Микола Васильович
ЙОНА Лариса Григорівна
ЩЕРБИНА Юрій Володимирович
ОНАЦЬКИЙ Олексій Віталійович

РОЗВИНЕННЯ КРИПТОЛОГІЇ ТА ЇЇ МІСЦЕ В СУЧАСНОМУ СУСПІЛЬСТВІ

Частина І

КЛАСИЧНІ МЕТОДИ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ

Навчальний посібник

За редакцією **М.В. Захарченка**

Редактор *І. В. Ращупкіна*
Комп’ютерне верстання *Ж.А. Гардиман*