надлишковості, підвищення пропускної здатності каналу тощо.

Шифрування з ключем має певні позитивні моменти.

1 Використовуючи ключ, можна застосовувати той самий алгоритм задля відправляння повідомлень різним людям. Головне – закріпити окремий ключ за кожним респондентом.

2 В разі „зламу" зашифрованого повідомлення достатньо лише змінити ключ, але переходити на новий алгоритм немає потреби.

Питаннями захисту інформації шляхом її перетворювання, яке виключає можливість прочитування інформації сторонньою особою, займається ***криптологія*** (kryptos – таємний, logos – наука). Криптологія поділяється на два напрями – *криптографію* й *криптоаналіз*. Цілі цих напрямів 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 існує кваліфікованих криптографів, котрі не володіли б методами криптоаналізу.

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

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.

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 надають таке означення: ***відкрита інформація*** – це невтаємничена (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.

Вочевидь, що термін "криптографія" далеко відійшов від свого первинного значення – "тайнопис", "таємний лист". Сьогодні це наукова дисципліна, яка поєднує методи захисту

інформаційних взаємовпливів різноманітного характеру, які спираються на перетворювання 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*:

$$M' = f(M), \text{ або } M' = f(M, K).$$

Перетворювання M_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, з-посеред яких:

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

Однак, окрім перехоплення й розкриття шифру, неправочинний користувач може намагатися здобути захищувану інформацію багатьма іншими способами, коли криптографія просто неспроможна цю інформацію захистити (приміром, 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 відвіднайти найслабшу ланку в цьому ланцюзі, аби з найменшими витратами добутися до інформації. Тому правочинні користувачі мають враховувати "засаду рівнопотужності 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 тощо.

1.1 **Шифри перестановки**

Простий метод криптографічного перетворювання, який містить правило переставляння літер у відкритому тексті. Шифри перестановки мають невелику криптостійкість, тому їх не використовують без додаткових перетворювань.

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

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 перестановкою, а число 5 – степенем перестановки.

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.

1.1.1 Прилад Сцитала

Одним з перших фізичних приладів, які зреалізовують шифр перестановки, 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 маршрутної перестановки. Зміст цього шифру полягає в такому.

Відкритий текст виписується в прямокутну таблицю з n рядків та m стовпців. Припускається, що довжина тексту t 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".

1.1.2 "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" 44 становить 880, а кількість "магічних квадратів" 55 – близько 250 000.

Уперше ці квадрати виникли в Китаї, де їм було надавано певної "магічної" сили. Наведемо приклад: у квадрат розміром 44 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

Приміром, 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 перестановки, але вважалося, що особливої стійкості йому надає чаклунство "магічного квадрата".

1.1.3 Практичне застосовування шифрів перестановки в системах зв'язку

Практичну реалізацію шифру перестановки 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.

Перестановка 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. 1.1 та 1.2).

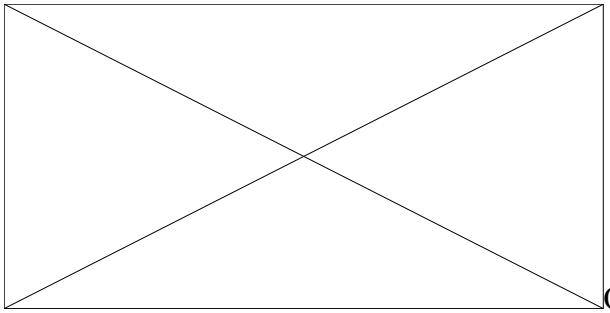 Ошибка: источник перёкрестной ссылки не найден

Рисунок 1.1 – Поділення ширини смуги

Ошибка: источник перёкрестной ссылки не найден

Рисунок 1.2 – Перестановка частотних смуг

Найпростіший скремблер обмежує захист уведенням подібних найпростіших частотних перетворювань. 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. 1.3).

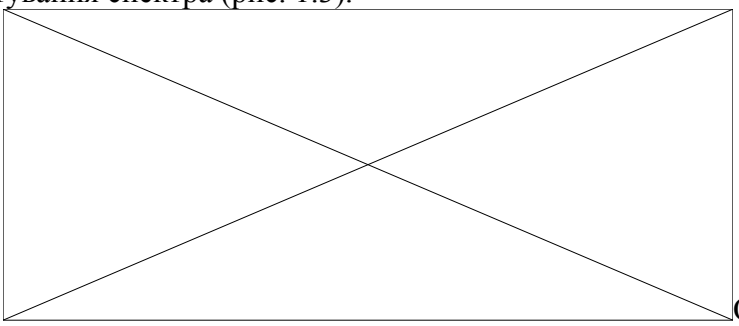 Ошибка: источник перёкрестной ссылки не найден

Рисунок 1.3 – Інвертування спектра

Частотно-часові перестановки. Ще більш складні системи розбивають сигнал на часовому інтервалі 60...500 мс і на кожнім інтервалі використовують у комбінації власні аналогові перетворювання. Змінюванням перетворювань 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 зашифровування 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 вітчизняних 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 перестановки.

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.

1.2 Шифри простої заміни

Шифри простої заміни (одноабеткові підстановки) – це простий метод перетворювань, який містить правило заміни символів вихідного тексту на інші символи тої самої абетки.

Шифр заміни є найпростішим та найбільш популярним шифром. Як випливає з самої назви, шифр заміни здійснює перетворювання (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 зашифрованого 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 такій спосіб: відкритий текст $x_1x_2\ldots x_n$ перетворюється на зашифрований текст $g(x_1)\, g(x_2)\ldots g(x_n)$.

Як відкритий текст, так і шифртекст утворюються з літер, котрі входять до скінченної множини символів, називаних *абеткою*. Прикладами абеток є скінченна множина усіх великих літер, скінченна множина усіх великих і малих літер та цифр тощо.

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, по’єднуючи по n літер, дістаємо абетку $\sum^n$, яка має m^n n-грам.

Приміром, 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 перетворювань корисно замінювати літери абетки на цілі числа – 0, 1, 2, 3, ... Це дозволяє спростити виконання необхідних алгебричних маніпуляцій. Приміром, можна встановити взаємно однозначну відповідність поміж українською абеткою

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

та множиною цілих

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

поміж російською абеткою

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

та множиною цілих

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

поміж англійською абеткою

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

та множиною цілих

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

(див. табл. 1.1, 1.2 та 1.3).

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 на числа дозволяє більш чітко сформулювати основні концепції та прийоми криптографічних перетворювань. Водночас у більшості ілюстрацій використовуватиметься абетка природної мови.

Таблиця 1.1 – 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	И	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 1.2 – 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 1.3 – 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 перетворювання E являє собою сукупність перетворювань

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

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

Перетворювання $E^{(n)}$ 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 безваріантності перетворювання $E^{(n)}$ на множину $\overline{Z}_{m,n}$.

Криптографічна система може трактуватися як сімейство криптографічних перетворювань

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

позначених параметром K, називаним *ключем*.

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

1.2.1 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 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

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 використовуваний 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 сьогодні 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 переписки Цезаря. Нагадаємо, що сам Цезар усе життя використовував один і той самий ключ (зсунення на три літери). Цим шифром він користувався, зокрема, для обміну посланнями з Ціцероном.

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.

1.2.2 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.

1.2.2.1 Диск Енея

Перший з винаходів – так званий "диск Енея". Засади його побудови й дії є вельми прості. На диску діаметром 10...15 см і товщиною 1...2 см висвердлювалися 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 у 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.

1.2.2.2 Лінійка Енея

Ідею Енея було використано при створюванні й інших оригінальних шифрів заміни. Приміром, 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 завершення зашифровування нитка витягалася й 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.

1.2.2.3 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 до сьогодні.

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 використовування книги для таємного обміну повідомленнями. Приміром, якщо адресати заздалегідь домовилися поміж собою про використовування 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.

1.2.3 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 55 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, в якому її записано. 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.

Існував і інший варіант шифрування за допомогою квадрата Полібія. 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. 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 завжди мати при собі ключ – квадрат. Виникла небезпека щодо таємного ознайомлення з цим ключем сторонніх осіб. Як компромісний розв’язок в якості ключа було запропоновано пароль. Легко запам'ятовуваний пароль вписувався без повторювання літер до квадрата; у клітинки, котрі залишилися порожніми, за абеткою вписувалися літери абетки, відсутні в паролі. Приміром, нехай паролем є слово THE TABLE.

Тоді квадрат матиме 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 розташовування літер при використовуванні лінійки Енея, а також шифру заміни Цезаря (за довільного розташовування 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 шифртекст:

13.21.11.23.42.42.14.11. (1.1)

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 (1.2)

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 (1.3)

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 Е відкритого тексту переходить у різні літери: К, Е; літера Р – у літери D, Н). Було виявлено й негативний момент. Якщо в шифрі простої заміни шифртекст буде написано з однією помилкою (наприклад у тексті (1.1) 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 (1.3) буде спотворено четверту літеру (літеру С замінено, приміром, на К), то в розшифрованому тексті буде вже два спотворення: THE HIPLE, що вже утруднює відновлення вихідного повідомлення.
Аналогічно обстоїть справа з помилками вигляду "пропускання літер". Нехай у тексті (1.3) пропущено літеру С. 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 (1.3) першої літери при розшифровуванні здобудемо ЕЕ APPLE.
Слід зауважити, що в дещо зміненому вигляді шифр Полібія добувся до наших днів і дістав своєрідної назви "тюремний шифр". Для його використовування 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. Приміром, 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 56 (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.

1.2.4 Спосіб шифрування Тритемія і 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" ґрунтовано на засаді заміни літер зашифровуваного тексту на заздалегідь обумовлені слова. З цих слів складалося зовнішньо "безневинне" повідомлення. Наведемо приклад.
Замінимо літери H, I на такі слова:

H = ЗЕЛЕНИЙ, МІЙ, БІЛЯ
I = КЛЮЧ, МОРЕ, ГАЙ

Тоді негативна секретна відповідь **HI** 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. Перший рядок цієї таблиці є водночас і рядком літер відкритого тексту. Перша літера тексту зашифровується за першим рядком, друга літера – за другим рядком і т. д.; після використовування останнього рядка – знову повертаються до першого рядка. Приміром, слово "fight" (боротьба) набуває вигляду "fjikx".
Зреалізовування таблиці Тритемія не потребувало використовування 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:

- упровадження 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.

1.2.4.1 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.

1.2.4.2 Шифр „братерства франкмасонів”

Шифр „братерства франкмасонів”, чи „вільних каменярів”, що його 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:

Фраза "We talk about" при зашифровуванні набуває вигляду

Геометричне подання може змінюватися, приміром, на

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.

1.2.5 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.

При шифруванні відшуковують у цій таблиці чергову літеру відкритого тексту й записують до шифртексту літеру, розташовану нижче за неї в тім самім стовпці. Якщо літера тексту міститься в нижньому рядку таблиці, тоді для шифртексту беруть першу верхню літеру з того ж самого стовпця.

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

1.2.6 Біграмний шифр Плейфейра

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

У цілому структура таблиці системи шифрування Плейфейра є майже

аналогічна до структури таблиці Трисемуса.

Процедура зашифровування містить 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 до одного рядка чи стовпця шифрувальної таблиці, 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;

- якщо обидві літери біграми відкритого тексту належать до одного стовпця таблиці, то за літери шифртексту вважаються літери, котрі розміщено під ними. Коли при цьому літера відкритого тексту перебуває в нижньому рядку, то для шифртексту береться відповідна літера з верхнього рядка того самого стовпця;

- якщо обидві літери біграми відкритого тексту належать до одного рядка таблиці, то за літери шифртексту вважаються літери, котрі розміщено праворуч від них. Коли при цьому літера відкритого тексту перебуває в крайньому правому стовпці, то для шифру беруть відповідну літеру з лівого стовпця в тому самому рядку.

При розшифровуванні застосовується зворотний порядок дій.

1.3 Шифри складної заміни

При шифруванні за допомогою шифрів складної заміни закон перетворювання змінюється від символу до символу. 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 у табл.1. 4.

Таблиця 1.4 – 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 використовування 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.

1.3.1 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 1466 року, являла собою першу в Європі наукову працю з криптології. Криптологи усього світу вважають Л. Альберті за засновника криптології.

Леон Альберті уперше запропонував ідею подвійного шифрування: текст, здобутий внаслідок першого зашифровування, 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 зашифрування полягав у перебуванні літери відкритого тексту на зовнішньому диску й заміні її на відповідну (яка містилася під нею) літеру шифртексту. Після зашифровування кількох 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 – шифрабеткою. Якщо в перебігу шифрування шифрабетка 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, переважно, використовуються й у наші дні. Однак засіб продукування послідовності абеток шифртексту 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 кодопозначань 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 позначань. Оскільки однознакових позначань виявляється порівняно небагато, то, аби не впадала в око їхня мала частість з’явлення в шифртексті, Ардженті рекомендував додавати однознакові позначання літер, які найчастіше зустрічаються у відкритому тексті.

Наведемо приклад шифру заміни Ардженті для італійської мови. У цій заміні поряд із шифруванням використовується шифрування-кодування певних 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 вигляду

5128066284580377 або 1772850682584780537.

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 шифртексту на улюблені ним символіко-геометричні фігури. Зрозуміло, жодного ускладнення при цьому шифр Альберті не набув, додалося лише екзотики у шифртексті.

Основна книга Порта про тайнопис – це книга "Про таємну переписку". 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 шифртексті 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. 1.4.

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 1.4 – Шифр Белазо для української мови

Шифрування здійснюється за допомогою секретного гасла. Це гасло періодично виписується над відкритим текстом, за першою літерою цього гасла відшуковується 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).

Наведемо 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 і о д и ч н и й ш и ф р …….....

Шифртекст: з ш г і 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 застосовування. Причина цього – необхідність завжди мати при собі зазначену таблицю і складність процесу шифрування. Однак було надано імпульсу для з ′явлення інших систем шифрування (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", в якій є розділи, присвячені криптографії. У ній набули відбиття нові ідеї криптографії: використовування частини найчастіш 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 перестановки.
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 виникали порожні місця, то в них вписувалися довільні літери. Потім літери квадрата виписувалися порядково, що й становило шифртекст.
Запропонований Кардано шифр-ґрати покладено в основу славнозвісного шифру Рішельє, в якому шифртекст мав вигляд "безневинного" послання. З цупкого матеріалу вирізувався прямокутник розміром, приміром, 710 клітинок; 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, використовування цього шифру спричинює утруднення й вимагає інтелекту певного рівня.
Блез де Віженер (XVI ст.), посол Франції в Римі, ознайомившись з працями Тритемія, Белазо, Кардано, Порта, Альберті, також захопився криптографією.

1585 року Блез де Віженер 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 із засновників теорії ймовірностей, а потім і Норбертом Вінером – "батьком" кібернетики. У цьому трактаті знову „взято на озброєння" ідею використовування найбільш 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 (Додаток Б).

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 відшуковують 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 ключем *r*-абеткового підставляння є *r*-рядок

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

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

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

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

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 використовування таблиці Тритемія, запропонований Віженером, полягає в застосовуванні гасла. Власне Віженер сполучив підходи Тритемія, Белазо, Порта до шифрування відкритих текстів, істотно не додавши до них нічого оригінального.
Пізніше шифр Віженера значно спростив для його практичного використовування граф Гронсфельд – керівник першого в Німеччині державного дешифрувального органа ("криптографічної лабораторії"). Його пропозиція призвела до з'яви 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 зашифровуванні літера відкритого тексту замінюється на літеру, котра відстоїть від неї праворуч (циклічно) в абетці на кількість літер, зумовлюваних відповідною цифрою гасла. Так, приміром, за зазначеного гасла слово THE TABLE перетворюється на послідовність UKJAJCOJ.
Подальша модернізація призвела нашого часу 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.

Застосуймо 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 зашифровування. 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 вельми спрощену систему Віженера як шифр, який "неможливо розкрити!".
Шифри Віженера з коротким періодичним гаслом використовуються й у наші дні в системах шифрування, які не потребують 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. 1.5. У такої таблиці є одна перевага: правила зашифровування й розшифровування за нею збігаються: літери вилучаються з верхнього ряду абетки. Це створює певні зручності при використовуванні 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 певні розроблені ним методи дешифрування. Зокрема він запропонував

використовувати перебирання можливих відкритих слів за їхньою довжиною, якщо в шифртексті залишалося розбивання на слова.

Запропонована Фальконером система шифрування поєднує два шифри: вертикальної перестановки 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 ФХЦЧШЩ Ь ЮЯ
1 3 5 6 7
2 4

	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 1.5 – Шифр Бофора для англійської абетки

1.3.2 Роторні машини

Першою спробою побудувати роторну машину була так звана машина Джефферсона, створена наприкінці XVIII сторіччя першим державним секретарем CIF Томасом Джефферсоном. Вона являла собою певну кількість дисків, які надівались на вісь, утворюючи в такій спосіб циліндр. На ободі кожного колеса рівномірно й випадково було нанесено символи абетки, з яких формувався текст криптограм. Розподілювання символів було випадковим, і на кожному колесі воно відрізнювалось від розподілення на інших колесах. Колеса можна було знімати та змінювати за місцями. Уздовж циліндра могли пересуватись та фіксуватись дві паралельні планки. Прокручуючи кожне колесо, блок відкритого тексту набирали уздовж першої планки. Текст, що складався в такий спосіб уздовж другої планки і не мав жодного смислу, являв собою відповідний блок зашифрованого тексту (криптограми). Ключем у даному разі були розподілення літер на колесах, послідовність цих коліс та відстань поміж планками (рис. 1.6).

Л	В	Б	К	А	Ш	У	І	Ф	Д
Ш	И	Ф	Р	З	А	М	І	Н	И
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
А	К	О	Ф	Ц	Ь	Л	У	Е	Г
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
В	Н	Ф	Р	Д	Я	Н	С	Ш	Х

Рисунок 1.6 – Схема Коліс Джефферсона

Рисунок 1.6 – Схема Коліс Джефферсона

Всього машина Джефферсона мала 36 дисків, на кожному з яких було нанесено по 26 літер латинської абетки. Це означає, що сумарна кількість варіантів, якими могло бути зашифроване повідомлення, дорівнювала $26! \cdot 36!$ і мала порядок 10^{60}.

На жаль, винахід Джефферсона було забуто на багато років, через те що рівень розвинення математики на той час не дозволив правильно оцінити стійкість такого способу шифрування. Сам Джефферсон та його адміністрація продовжували користуватись іншими, значно гіршими шифрами.

20-ми роками XX сторіччя було винайдено електромеханічні пристрої шифрування, котрі автоматизують процеси зашифровування й розшифровування. Робота таких машин базується на засаді 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 (рис. 1.7).

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 сполучено із 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 долучуватися до вхідних контактів ротора, який слідує за ним. Тоді, приміром, якщо на клавіатурі чотириторної 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 поверталися – і наступного разу заміна була іншою. Аби спантеличити криптоаналітиків, ротори оберталися з різною швидкістю.

Щоби роторна машина була оптимальною, мають виконуватись такі умови:

- період повторювання має бути великим;
- після зашифровування кожного знаку якомога більша частина роторів повинна змінювати своє положення.

Щодо машини ENIGMA, то другому пунктові вимог вона не відповідає, але цим забезпечується простота її технічної реалізації. Ускладнення способу обертання дисків має виконуватись в такий спосіб, щоби зберігалась однозначність шифрування, а це є надто складна річ.

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

- роторів;
- порядку розташування роторів;

- кількості місць зупинки на колесо;
- характеру руху тощо.

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 порядка 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 зашифровування.

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

1.3.3 Одноразова система шифрування

Майже всі застосовувані на практиці шифри схарактеризовуються як умовно надійні, оскільки вони можуть бути переважно 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 використовування 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 підстановки 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 відправлячем, а другий – одержувачем. Для кожного символу X_i повідомлення використовується власний 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 буде абсолютно надійний, якщо набір ключів K_i буде 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 використовування 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, приміром гарячою лінією Москва–Київ. Однак така вимога практично є нездійсненна для сучасних систем опрацьовування інформації, де потрібно зашифровувати безліч мільйонів символів.

У певних варіантах одноразового нотатника вдаються до більш простого керування ключовою послідовністю, але це призводить до певного зниження надійності шифру. Наприклад, ключ зумовлюється зазначенням місця в книзі, відомій і відправлячеві 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.

2 ЗАСАДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У першому розділі розглянуто класичні методи шифрування, які лежать у підґрунті побудови будь-якої криптографічної системи.

Перші криптосистеми виникають ще до початку нової ери. Приміром, Юлій 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 сьогодні розвинення обчислювальних засобів прискорює розробляння й удосконалювання криптографічних методів.

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

З одного боку, розширилося використовування 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 дискредитування криптографічних систем, котрі ще донедавна вважалися за стійкі.

2.1 Завдання, розв’язувані криптографічними методами

Перш ніж розпочати вивчення основних криптографічних систем та методів, що лежать у підгрунті їхньої побудови, треба визначитися із основними поняттями у сфері криптографічного захисту інформації. Тобто треба надати відповідь на запитання про те, що саме має захищатися в телекомунікаційних системах, а також від чого та від кого воно має захищатись і в який спосіб.

Відповідь на перше запитання вимагає побудови моделі інформаційного процесу. Для цього треба визначитися з тим, хто є учасниками інформаційного процесу, які завдання перед ними стоять і як вони збираються їх розв’язувати.

Відповіді на друге запитання повинні надавати критерії нормального перебігу інформаційних процесів у системі й визначати потенційно можливі обставини, які призводитимуть до відхилення їхнього перебігу від нормального. Такі обставини називають загрозами, а осіб, котрі зумисне чи то незумисне можуть їх утворювати, називають потенційними порушниками.

Розгорнута відповідь на друге запитання є моделлю порушника. Порушник – це окрема особа, сума цілей і можливостей, яка відповідає засаді: два суб’єкти, котрі мають однакові цілі й можливості, – це один суб’єкт.