Міністерство транспорту та зв'язку України

Державний департамент з питань зв`язку та інформатизації

Одеська національна академія зв`язку ім. О. С. Попова

Кафедра документального електрозв`язку

С. М. ГОРОХОВ, Л. Г. ЙОНА, О. В. ОНАЦЬКИЙ

Під редакцією проф. М.В. Захарченка

СУЧАСНІ КРИПТОГРАФІЧНІ СИСТЕМИ

Навчальний посібник
з дисципліни
«Захист інформації в телекомунікаційних системах і мережах»

для освітньо-професійної підготовки бакалаврів
з напряму галузі 0509 Радіотехніка, радіоелектронні апарати та зв'язок
за напрямом підготовки 6.050903 – Телекомунікації

Одеса
2007

УДК 003.26

План НМВ 2006 р.

Навчальний посібник розробили С. М. Горохов,
Л. Г. Йона,
О. В. Онацький

Сучасні криптографічні системи: Навч. посібник. – Одеса: ВЦ ОНАЗ ім. О.С. Попова, 2007. – 152 стор.

Під редакцією проф. М. В. Захарченка

Навчальний посібник призначено для студентів, котрі вивчають дисципліну "Захист інформації в телекомунікаційних системах і мережах". Містить систематичне викладення наукових основ від найпростіших прикладів та основних понять до сучасних криптографічних концепцій. Спрямовано на вивчення симетричних криптосистем. Розглянуто криптосистеми з відкритим ключем, а також питання убезпечення від несанкціонованого втручання в електронних системах.

Навчальний посібник розглянуто й ухвалено до видання на засіданні кафедри ДЕЗ.
Протокол № 12 від 12 грудня 2006 р.

Зав. кафедрою ДЕЗ, проф. М. В. Захарченко

Навчальний посібник розглянуто й ухвалено до видання методичною радою факультету ТКС
Протокол № 12 від 24 грудня 2006 р.

Декан факультета ТКС, доц. О. В.Онацький

ЗМІСТ

ПЕРЕДМОВА

Дисципліна Н3.16 — “Захист інформації в телекомунікаційних системах і мережах ” впроваджено до учбового плану освітньо-професійної програми підготовки бакалаврів з напряму галузі 0509 Радіотехніка, радіоелектронні апарати та зв’язок за напрямом підготовки 6.050903 – Телекомунікації.

Метою навчальної дисципліни є формування у студентів знань та вмінь з питань криптографічного захисту інформації, яка зберігається й передається телекомунікаційними системами та мережами.

Курс базується переважно на дисциплінах: Н2.01 — Вища математика; Н3.4 – „Обчислювальна техніка та мікропроцесори”; Н3.14 – „Системи документального електрозв’язку”; ВД3.1 – „Мережні технології”, – з яких студенти повинні знати види первинних сигналів електрозв’язку, основні характеристики ліній передавання, характеристики й загальні принципи функціювання систем комутації та систем передавання електрозв’язку.

Дисципліна складається з двох модулів:

модуль 1 – Основи законодавчої та нормативно-правової бази України, архітектура системи безпеки інформації та класичні методи шифрування (лекцій – 16 год.; практичних занять – 8 год.; лабораторних робіт – 8 год.; самостійна робота – 33 год.; всього – 65 год.);

модуль 2 – Сучасні криптосистеми (лекцій – 16 год.; практичних занять – 10 год.; лабораторних робіт – 6 год.; самостійна робота (індивідуальне завдання) – 38 год.; всього – 70 год.).

Для засвоєння змісту дисципліни “Захист інформації в телекомунікаційних системах і мережах” треба набути таких знань та вмінь:

– вміти розкласти функцію в степеневі ряди й ряди Фур`є («Вища математика», модуль 4);

– знати основні характеристики електричних фільтрів («Теорія електричних кіл та сигналів», модуль 6);

– знати основні відомості з теорії інформації («Теорія електричного зв`язку», модуль 2);

– знати випадкові електричні сигнали та їхній математичний опис («Теорія електричного зв’язку», модуль 2);

– знати основні параметри та правила побудови деяких найчастіш уживаних двійкових коригувальних кодів («Системи документального електрозв`язку», модуль 2).

Структура дисципліни

№ тижня	Тематика та зміст двогодинних лекцій, додатковий матеріал для самостійного вивчання	Література з теми
1	Актуальність проблеми захисту інформації в сучасних системах телекомунікації. Системний підхід до вирішення проблеми захисту інформації	Л3
2	Аналіз погроз інформації в системах телекомунікації. Основні шляхи витоку інформації	Л3
3	Політика інформаційної безпеки. Інформаційні обєкти захисту	Л3

	та принципи розподілу доступу до них. Рівні захищеності інформаційних обєктів та рівні гарантій щодо їхньої захищеності	
4	Секретна система звязку. Завдання, розв'язувані криптографічними методами. Стійкість криптосистем	Л4
5	Принципи побудови класичних шифрів. Шифри, які використовують операції перестановки	Л1, Л4
6	Шифри, які використовують операції простої заміни	Л1, Л4
7	Шифри, які використовують операції складної заміни	Л1, Л4
8	Загальні принципи побудови симетричних криптосистем. Математични операції, використовувані в симетричних криптосистемах	Л4
9	Основи архітектури сучасних симетричних криптосистем. Блочні алгоритми шифрування. Шифри на базі мережі Фейстеля	Л4
10	Криптосистема DES. Схема алгоритму шифрування DES. Режими роботи алгоритму шифрування DES	Л4
11	Стандарт шифрування IDEA	Л4
12	Вітчизняний стандарт шифрування ГОСТ 28147–89. Схема алгоритму шифрування ГОСТ 28147–89. Режими роботи вітчизняного стандарту шифрування ГОСТ 28147–89	Л4
13	Криптосистеми з незасекреченим ключем. Процедури розшифровування та розшифровування в криптосистемі RSA	Л4
14	Проблема автентифікації даних. Однонапрямні ГЕШ–функції. Електронний цифровий підпис. Алгоритм цифрового підпису RSA	Л4
15	Алгоритм цифрового підпису Ель Гамаля. Вітчизняний стандарт щодо цифрового підпису	Л4
16	Принципи керування ключовою системою. Генерування, зберігання та розподілювання ключів. Метод Диффі–Хеллмана	Л4

Література

1 Захарченко М. В., Йона Л. Г., Щербина Ю. В., Онацький О. В. Розвинення криптології та її місце в сучасному суспільстві. Частина 1. Класичні методи шифрування та дешифрування.: Навч. посібник.– Одеса: ОНАЗ ім. О.С. Попова, 2004. –80стор.

2 Кисель В.А., Захарченко Н.В. Основы криптографии: Учеб. пособие. ⁄ – Одеса: УДАЗ ім. О.С.Попова, 1997.

3 Защита информации в системах телекоммуникации: Учеб. пособие ⁄ Под ред. В.Л. Банкета – Одесса: УДАЗ ім. О.С. Попова, 1997.

4 Даний навчальний посібник.

ПЕРЕЛІК ПРАКТИЧНИХ ЗАНЯТЬ

Теми занять	№
МОДУЛЬ 1	
Модулярна арифметика. Розв'язування типових задач	2
Шифри перестановки. Розв'язування типових задач	2
Шифри простої заміни. Розв'язування типових задач	2
Шифри складної заміни. Розв'язування типових задач	2
МОДУЛЬ 2	
Законодавча база України. Основні положення законів "Про інформацію", "Про захист інформації в автоматизованих системах"	2

щодо захисту інформації в телекомунікаційних системах та мережах звязку	
Нормативно-правова база України. Основні положення нормативно-правової бази України щодо захисту інформації в телекомунікаційних системах та мережах звязку, “Концепція захисту інформації в системах звязку України”	2
Вивчення алгоритму функціювання криптосистеми DES. Режими роботи криптосистеми DES	2
Вивчення алгоритму криптосистеми ГОСТ 28147–89. Режими роботи криптосистеми ГОСТ 28147–89	2
Дослідження асиметричного алгоритму RSA	2

ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ

Найменування лабораторної роботи	Кіль-кість годин
МОДУЛЬ 1	
Дослідження шифру „Гомоморфна підстановка”	2
Дослідження шифру подвійної перестановки	2
Дослідження шифрів моноабеткової заміни	2
Дослідження шифру „подвійний квадрат”	2
МОДУЛЬ 2	
Дослідження шифрів Віженера та Гронсфельда	2
Дослідження асиметричного алгоритму цифрового підпису RSA	2
Дослідження алгоритму розподілювання ключів методом Диффі–Хеллмана	2

Перелік знань та вмінь, яких має набути студент

в процесі вивчання матеріалу

1 Надавати за потреби захист інформації в телекомунікаційних системах та мережах за допомогою програмних чи апаратних засобів, використовуючи нормативну базу України щодо захисту інформації, наявну апаратуру та знання сучасного технічного захисту інформації.

2 Під керівництвом провідного фахівця виконувати обчислювання необхідних параметрів систем технічного захисту інформації в системах та мережах звязку.

КОНТРОЛЬНІ ЗАПИТАННЯ ДЛЯ ПЕРЕВІРКИ ЗНАНЬ ТА ВМІНЬ ОБОВ`ЯЗКОВОЇ ЧАСТИНИ ПРОГРАМИ МОДУЛЯ

1 Що означає поняття “документ” в інформаційних системах?

2 Що означає поняття “секретна інформація” в інформаційних системах?

3 Що означає поняття “відкрита інформація” в інформаційних системах?

4 Навести схему секретної системи звязку.

5 Що означає поняття “закрита інформація” в інформаційних системах?

6 В чому полягає суть понять “перемішування” та “розсіювання” за К. Шенноном?

7 Які існують канали несанкціонованого витікання інформації в системах телекомунікації?

8 Які питання вивчає криптоаналіз?

9 Які існують класи криптоалгоритмів?

10 Що називають атаками на інформаційні обєкти?

11 Пояснити поняття “пасивна атака”.

12 Пояснити поняття “активна атака”.

13 Принцип рівнопотужного захисту в інформаційних системах.

14 Що називають загрозами для інформаційних обєктів?

15 У яких трьох аспектах має розв’язуватись проблема захисту інформації в телекомунікаціях?

16 Які алгоритми називають блочними?

17 Які види інформаційних злочинів існують в телекомунікаційних мережах?

18 Принципи побудови шифрів на базі мережі Фейстеля.

19 Що означає поняття “ключ” в інформаційних системах?

20 Пояснити суть методів шифрування: заміни, перестановки та гаммування.

21 Пояснити суть понять: інформаційні ресурси, інформаційні процеси, інформаційні системи.

22 Принципи поділу загроз інформаційним обєктам на потенційно можливі та зумисні.

23 Поясніть вміст використовування засобів забезпечування безпеки: фізичних, апаратних, програмних, організаційних, законодавчих.

24 Що означає поняття “відкрита інформація” в інформаційних системах?

25 Які алгоритми називають несиметричними?

26 Які алгоритми називають симетричними?

27 Що означає поняття “інформаційна взаємодія” в інформаційних системах?

28 Принципи шифрування за допомогою операції переставляння. Основні шифри перестановки.

29 Складові криптології? У чому полягає їхня сутність?

30 Чим відрізнюються процеси розшифровування та дешифрування інформації?

31 Які запитання слід задати, перш ніж вдаватися до захисту інформації?

32 Які питання вивчає криптографія?

33 Що означає поняття „криптостійкість”?

34 Який шифр є стійким за К. Шенноном?

35 Властивості захищуваної інформації.

ТЕСТИ ДЛЯ РЕКТОРСЬКОЇ ТА ГАЛУЗЕВОЇ ПЕРЕВІРОК

1 Які властивості інформації підлягають захисту в автоматизованих системах та системах телекомунікації?

- конфіденційність, цілісність, доступність, спостережуваність;
- конфіденційність, цілісність, доступність;
- цілісність, доступність, спостережуваність, таємність.

2 Що означає поняття "документ" згідно з нормативною базою України?

- інформація, зафіксована на будь-якому матеріальному носії;
- інформація, зафіксована на будь-якому матеріальному носії у визначеному законом порядку;
- інформація, зафіксована на будь-якому матеріальному носії й зареєстрована у державному органі.

3 У які способи розв'язується проблема передавання юридичнозначущих документів каналами зв'язку?

- шифрування та застосовування цифрового підпису;
- використовування криптографічних протоколів автентифікації;
- застосовування цифрового підпису.

4 У яких трьох аспектах має розв'язуватись проблема захисту інформації в системах телекомунікації?

- удосконалювання відповідної нормативної бази, організаційних заходів та програмно-апаратних засобів;
- удосконалювання відповідної нормативної бази, розробляння сучасних захищуваних інформаційних технологій, удосконалювання сучасних розподілювальних обчислювальних мереж.

5 Складові організаційних заходів щодо побудови систем захисту інформації

- організація секретного виробництва, облік електронного та паперового документообігу, контроль за поводженням персоналу;

- керування доступом, контроль загроз, контроль коректності роботи апаратно-програмних засобів, ідентифікація та автентифікація користувачів.

6 Що називають загрозами інформаційним об'єктам?

- потенційно можливі події, котрі призводять до порушень політики безпеки;
- потенційно можливі події, котрі призводять до втрат конфіденційності, цілісності та доступності інформації;
- потенційно можливі події, котрі призводять до втрат електронних документів.

7 Які види інформаційних злочинів існують в телекомунікаційних мережах?

- порушення конфіденційності, цілісності та доступності інформації, яка передається та опрацьовується у системах телекомунікації;
- відмова від авторства електронного документа, відмова від факту отримання документа, підробка електронного документа.

8 Що називають несанкціонованим доступом до інформації?

- доступ до об'єкта, який підлягає захистові, в обхід монітора доступу;
- доступ до об'єкта, який підлягає захистові з боку користувача, котрий не має відповідних повноважень;
- доступ до об'єкта, який підлягає захистові, в обхід встановлених правил розподілу доступу.

9 З яких частин складається секретна схема зв'язку, визначена К. Шенноном?

- відкритий та закритий канали зв'язку, джерела повідомлень та ключів, а також криптографічний алгоритм;
- алгоритми зашифровування та розшифровування, алгоритм формування ключів та

система зв’язку з окремим закритим каналом.

10 Які умови побудови абсолютно стійкого шифру було окреслено К. Шенноном?

- алгоритм шифрування має зберігатись у секреті, ключі мають містити інформації не менше за зашифровуваний текст та передаватись через допоміжний секретний канал;
- ключі до алгоритму шифрування мають обиратись випадково, використовуватись лише одноразово й містити інформації не менше за зашифровуваний текст;
- довжина ключа має дорівнювати довжині повідомлення, яке підлягає шифруванню; алгоритм шифрування має містити операції заміни, перестановки та функційних перетворювань, а ключі мають обиратись незалежно один від одного.

11 Які алгоритми називають симетричними?

- блочні, поточні та змішаної структури;
- алгоритми, в яких операції зашифровування й розшифровування виконуються одним ключем;
- зворотні алгоритми, які дозволяють виконувати операції зашифровування й розшифровування.

12 Які алгоритми називають поточними?

- симетричні алгоритми, виконувані в режимі гаммування без розподілу відкритого тексту на блоки;
- симетричні алгоритми, виконувані без розподілу відкритого тексту на блоки;
- симетричні алгоритми, виконувані без розподілу на блоки з ключем, довжина якого дорівнює довжині повідомлення.

13 Що входить до складу криптографічної системи?

- алгоритм шифрування, множина повідомлень, множина ключів та множина криптограм;
- алгоритм шифрування, множина повідомлень, множина ключів, множина криптограм та відповідна документація;
- алгоритм шифрування, множина повідомлень, множина ключів, множина криптограм й відповідна документація та допоміжний секретний канал зв’язку.

14 Які криптографічні перетворювання використовуються за побудови симетричних криптографічних алгоритмів?

- гаммування, перестановки та заміни;
- функційні перетворювання, перестановки та заміни;
- параметричні перетворювання, перестановки та заміни, гаммування.

15 Що називають зворотним криптографічним алгоритмом?

- криптографічний алгоритм, який використовує один ключ як для зашифровування, так і для розшифровування;
- криптографічний алгоритм, який дозволяє зашифровувати й розшифровувати повідомлення без його перебудови.

16 Які криптографічні перетворювання використовуються в криптосистемі DES?

- зворотні табличні перестановки, табличні заміни, перестановки із розширюванням блоків, перестановки зі стискуванням блоків, циклічні перестановки;
- зворотні табличні перестановки, табличні заміни, перестановки із розширюванням блоків, заміни зі стискуванням блоків, циклічні перестановки;
- табличні перестановки, табличні заміни, функційні перетворювання.

17 Які криптографічні перетворювання використовуються у вітчизняному шифрувальному стандарті ГОСТ 28147–89?

- зворотні табличні перестановки, табличні заміни, перестановки із розширюванням блоків, перестановки зі стискуванням блоків, циклічні перестановки;

- табличні перестановки, табличні заміни, функційні перетворювання;

- зворотні табличні перестановки, табличні заміни, перестановки із розширюванням блоків, заміни зі стискуванням блоків, циклічні перестановки.

18 Які алгоритми називають асиметричними?

- алгоритми, які будуються із використовуванням однонапрямлених функцій;

- алгоритми, які передбачають наявність окремих ключів для зашифровування та розшифровування повідомлень;

- алгоритми, які використовують окремі алгоритми для зашифровування та розшифровування повідомлень.

19 Які функції називають однонапрямленими?

- функції, до яких не існує відповідних обернених функцій;

- функції, котрі мають відповідні обернені функції, але їхнє обчислювання є завданням, яке неможливо розв'язати через його складність;

- функції, котрі мають відповідні обернені функції, але способу їхнього обчислювання поки що не віднайдено.

20 Які функції називають однонапрямленими функціями з секретом?

- функції, обернене значення яких може бути дістано лише за умови наявності їхнього секретного параметра;

- функції, обернене значення яких може бути дістано лише за умови наявності секретного алгоритму.

21 Що таке є процедура автентифікації?

- процедура перевірки правильності паролю користувача системи;

- процедура перевірки повноважень користувача системи;

- ідентифікація користувача системи та підтвердження його повноважень.

22 Що називають "головним ключем" у системі розподілювання ключової інформації?

- ключ, за допомогою якого шифруються сеансові ключі користувачів;

- первинний ключ, з якого утворюються сеансові ключі із використовуванням відповідного алгоритму;

- ключ до алгоритму утворювання сеансових ключів.

23 Для чого застосовується зашифровування повідомлення?

- задля перетворювання відкритого тексту на незрозумілий текст;

- задля передавання каналами зв'язку;

- задля подавання відкритих повідомлень у вигляді бітового потоку.

24 Криптографія – це:

- наука, яка поєднує криптоаналіз та криптологію;

- наука про захист інформації, до якої може здійснюватися небажаний доступ;

- наука про зламування шифрів.

25 Ключ шифрування – це:

- спосіб кодування повідомлень;
- правило перетворювання відкритого повідомлення на закрите;
- пароль, внаслідок володіння яким закрите повідомлення стає доступним любому користувачеві.

26 Атака – це:
- можливість зламування криптосистеми без ключа;
- пароль, внаслідок володіння яким закрите повідомлення стає доступним любому користувачеві;
- порушення доступності повідомлення.

27 Загроза – це:
- можливість зміни процесу опрацьовування повідомлення;
- порушення доступності повідомлення;
- впливи на систему, котрі можуть завдати шкоди її безпеці.

28 Документ в інформаційних системах – це:
- матеріальна форма одержування, зберігання, поширювання й використовування інформації шляхом фіксації її на будь-якому носієві;
- основний об'єкт захисту в автоматизованих системах;
- відомості, котрі зберігаються в автоматизованих системах.

29 Доступність інформації – це:
- доступність вмісту для обмеженого кола користувачів;
- відсутність зумисного перекручування інформації;
- можливість доступу до інформаційних ресурсів автоматизованої системи в межах чинних повноважень.

30 Служба захисту інформації створюється задля:
- реалізації правових, організаційних та технічних заходів щодо захисту інформації;
- виявляння діяльності розвідувальних служб;
- виявляння діяльності окремих користувачів та організацій, спрямованої на приховування правопорушень.

31 Несанкціонованим доступом до інформації називають:
- перехоплене зашифроване повідомлення;
- ознайомлення з конфіденційною інформацією;
- несанкціоновану зміну, підміну чи знищування інформації.

32 Пасивним проникненням називають:
- підмикання до мережі зв'язку спеціального термінала;
- підмикання до лінії зв'язку чи збирання електромагнітних випромінювань ліній особою, котра не є користувачем ЕОМ;
- використовування інформації з файлів, створюваних на базі розподілюваних обчислювальних мереж.

33 Повідомлення складається з відкритого тексту?
- так;
- ні.

34 Кодування й шифрування – це є одне й те саме?
- так;
- ні.

35 Розшифровування – це процес перетворювання закритих повідомлень на відкриті?
- так;
- ні.

36 Криптоаналіз – це наука про розкриття шифрів?
- так;
- ні.

37 Криптологія – це наука, яка поєднує криптографію й криптоаналіз?
- так;
- ні.

38 Атака – це спроба реалізації погроз?

- так;
- ні.

39 Погрози – це впливи на систему, котрі можуть завдати шкоди її безпеці?

- так;
- ні.

40 Погрози можуть мати чи об'єктивну природу, чи суб'єктивну?

- так;
- ні.

41 Погрози, котрі мають суб'єктивну природу, можуть бути лише випадковими?

- так;
- ні.

42 Конфіденційність, цілісність та доступність є властивостями інформації?

- так;
- ні

43 Цілісність – це відсутність зумисного перекручування інформації?

- так;
- ні.

44 Доступність – це допуск до вмісту обмеженої кількості користувачів?

- так;
- ні.

45 Конфіденційність – це можливість доступу до інформаційних ресурсів автоматизованої системи?

- так;
- ні.

46 Несанкціонованим доступом до інформації називається перехоплювання зашифрованого повідомлення?

- так;
- ні.

47 Пасивне проникнення – це підміна чи знищення інформації?

- так;
- ні.

48 Суб'єктами інформаційних відносин є:

- лише громадяни України, юридичні особи й держава;
- лише інші держави, їхні громадяни та юридичні особи, міжнародні організації й особи без громадянства;
- усе вище перелічене.

49 Автоматизована система – це:

- система, яка здійснює автоматизоване опрацьовування даних, до складу якої входять технічні засоби їхнього опрацьовування (засоби обчислювальної техніки та зв'язку), а також методи і процедури, програмне забезпечення;
- система, за допомогою якої забезпечується зв'язок поміж користувачами;
- система, котра здійснює спостерігання за проходженням інформації.

50 Умова абсолютної стійкості для шифрів:

- довжина ключа й довжина відкритого повідомлення повинні бути однакові;
- непевність алгоритму шифрування є менше за непевність зашифровуваного повідомлення ;
- ключ має бути криптостійким.

51 До поточних алгоритмів належать:

- алгоритм, який використовує різні ключі зашифровування і розшифровування;
- алгоритм, в якому кожен символ відкритого тексту зашифровується незалежно від інших і розшифровується в такий самий спосіб.

52 Перемішування — це :

- властивість шифру приховувати залежність поміж символами вихідного тексту й шифрованого тексту;
- властивість шифру, за якої один символ (біт) вихідного тексту впливає на шифрування кількох символів (бітів) шифртексту.

53 Функційне перетворювання $F(R_{i-1}, K_i)$ (алг. DES) використовує таку операцію:

- порозрядне підсумовування з 48-бітовим ключем за модулем 32;
- лінійна перестановка з розширенням довжини блока;
- поділ вхідної послідовності на дві рівні частини – ліву та праву –, по 32 біти кожна;
- заміна зі стискуванням до 32-х бітів.

54 У режимі гаммування (ГОСТ 28147–89), зашифровування відбувається шляхом:

- побітового додавання за модулем 32 блока відкритого тексту та блока гамми довжиною 32 біти;
- побітового додавання за модулем 2 блока відкритого тексту та блока гамми довжиною 64 біти;
- підсумовування за модулем 32 блоків відкритого тексту з блоками гамми.

55 Імітовставка – це:

- блок фіксованої довжини, утворюваний з відкритих даних з використовуванням синхронадсилання задля забезпечення імітозахисту;
- блок фіксованої довжини, утворюваний з відкритих даних з використовуванням ключа;
- блок фіксованої довжини, утворюваний з відповідного ключа перших 16 розрядів, і додаваний до зашифровуваних даних для забезпечення імітозахисту.

56 Синхронадсилання S застосовується в режимах:

- простої заміни;
- гаммування зі зворотним зв'язком по виходу.

57 Кількість циклів в алгоритмі шифрування DES:

- 16;
- 32;
- 256.

58 Довжина блока в алгоритмі шифрування ГОСТ 28147–89:
- 32;
- 64;
- 256.

59 Розмір ключа в алгоритмі шифрування IDEA:
- 64;
- 128;
- 256.

60 Розмір ключа алгоритму шифрування ГОСТ 28147–89:
- 64;
- 128;
- 256.

61 Розмір ключа алгоритму шифрування DES:
- 48;
- 56;
- 64.

62 Шифр IDEA припускає:
- попередній поділ передаваної послідовності на 128-розрядні блоки, які шифруються за допомогою 128-бітового ключа;
- попередній поділ передаваної послідовності на 64-розрядні блоки, які шифруються за допомогою 128-бітового ключа;
- попередній поділ передаваної послідовності на 64-х розрядні блоки, які шифруються за допомогою 64-бітового ключа.

63 Шифр IDEA виконується за:
- 8 циклів;
- 16 циклів;
- 32 цикли.

64 У першому циклі шифр IDEA використовує:
- 2 ключі;
- 4 ключі;
- 6 ключів;
- 16 ключів.

65 Кількість циклів в алгоритмі ГОСТ 28147–89:
- 16;
- 32;
- 64;
- 256.

ВСТУП

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, допоки 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 хочуть ознайомитися з його змістом всупереч волі відправляча й одержувача, виникає набагато більше шансів це зробити. 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. Що жвавіше провадилося листування в суспільстві, тим більше відчувалася потреба в засобах його засекречування. Відповідно виникали все більш складні й хитромудрі шифри. Спочатку при зацікавлених особах з'явилися окремі 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.

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

Сучасна криптографія містить чотири великих розділи:

1Симетричні криптосистеми.

2 Криптосистеми з відкритим ключем.

3 Системи електронного підпису.

4 Керування ключами.

1 Класичні методи шифрування

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 відправляч хоче надіслати повідомлення одержувачеві. Більш того, відправляч прагне засекретити це повідомлення, аби ніхто, окрім одержувача, не зміг його прочитати. Для цього він має 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 розроблянням 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 відростало, 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 у 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 освітляння променями, зазвичай ультрафіолетом, певної частини спектра.

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

Процес перетворювання відкритого тексту з метою зробити незрозумілим його зміст для сторонніх називається ***шифруванням***. Вибір конкретного типу перетворювання визначається ключем зашифровування. Інакше кажучи, зашифровування – це процес перетворювання відкритого повідомлення на закрите. Зашифроване повідомлення називається шифртекстом.

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

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

Ключ – це правило, згідно з яким здійснюються зашифровування та розшифровування текстів. Надійність алгоритму шифрування залежить від довжини (кількісті бітів) ключа.

Зауважимо, що шифрування й кодування – це різні речі.

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

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.

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 – одноліток 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".

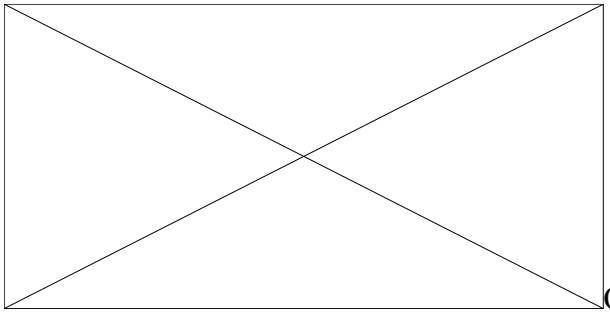
1.1.3 Практичне застосовування шифрів перестановки в системах зв'язку

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).



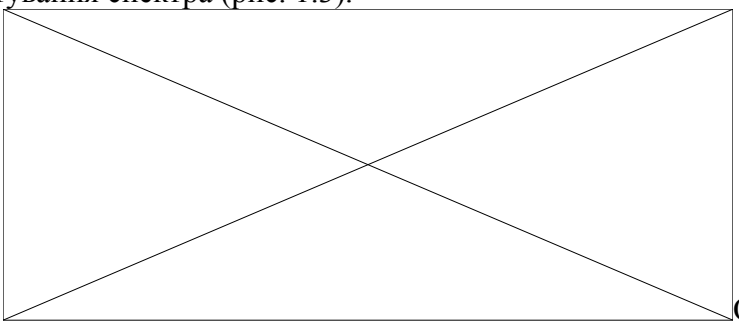
Ошибка: источник перёкрестной ссылки не найден Ошибка: источник перёкрестной ссылки не найден

Рисунок 1.1 – Поділення ширини смуги 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

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

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 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 (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 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 вигляду "пропускання літер". Нехай у тексті (1.3) 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 (1.3) 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 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.

Існує доволі велика численна кількість методів захисту інформації. Щодо криптографічних, то до їхнього складу відносять методи, у підґрунті яких лежать секретні алгоритми. Термін секретний алгоритм має широке тлумачення, але насамперед, мається на увазі алгоритм, цілковито або якийсь параметр чи частина його параметрів є відомі лише учасникам інформаційного процесу.

Надалі під *інформаційним процесом* матимемо на увазі процес взаємодії кількох суб'єктів, що передбачає обмін інформацією поміж ними. Таких суб'єктів може бути щонайменш два. Що стосується відхилення у перебігу інформаційного процесу від норми, то жодного об'єктивного критерію такої норми не існує. Тому загрозами ми й будемо називати будь-які можливі обставини, які призводять до такого відхилення. Порушники, котрі здійснюють загрози, можуть бути або законними учасниками інформаційного процесу, або особами, котрі просто мають доступ до інформації, яка опрацьовується чи передається в перебігу інформаційного процесу й, отже, можуть впливати на його перебіг.

Якщо учасники інформаційного процесу не мають змоги впливати на його перебіг, то такий процес називають *взаємодією в умовах довіри один до одного*. У противному разі процес називають *взаємодією недовіри один до одного*. Процеси останнього типу в сучасних системах є найбільш розповсюдженими. Слід зауважити, що тут йдеться не про особисту недовіру учасників процесу один до одного, а про дещо більше. Мають враховуватись всі чинники, як у внутрішньому, так і у зовнішньому середовищі функціювання системи, які можуть впливати на перебіг інформаційних взаємин.

Отже, завдання, розв'язувані криптографічними методами, можна поділити за такими критеріями:

- згідно з характером взаємин, котрі мають захищатись;
- згідно з цілями, які ставить перед собою злочинник;
- згідно з можливостями злочинників.

Найпростішим випадком інформаційних взаємодій є передавання даних від одного суб'єкта до другого. Відповідно, найрозповсюдженим завданням, розв'язуваним криптографічними методами, є захист конфіденційності інформації, котра зберігається й передається каналами зв'язку. Водночас це завдання є й найважливішим, незважаючи на те, що втілення інформаційних технологій в різноманітні сфери людської діяльності значно розширило їхнє коло.

2.2 Секретна система зв'язку

Завдання, яке полягає у захисті інформації під час передавання каналами зв'язку, вперше було сформульовано К. Шенноном у вересні 1945 року, а опубліковано у 1949 року в технічному журналі Bell System Technical Journal. Він запропонував секретну систему зв'язку, наведену на рис. 2.1.

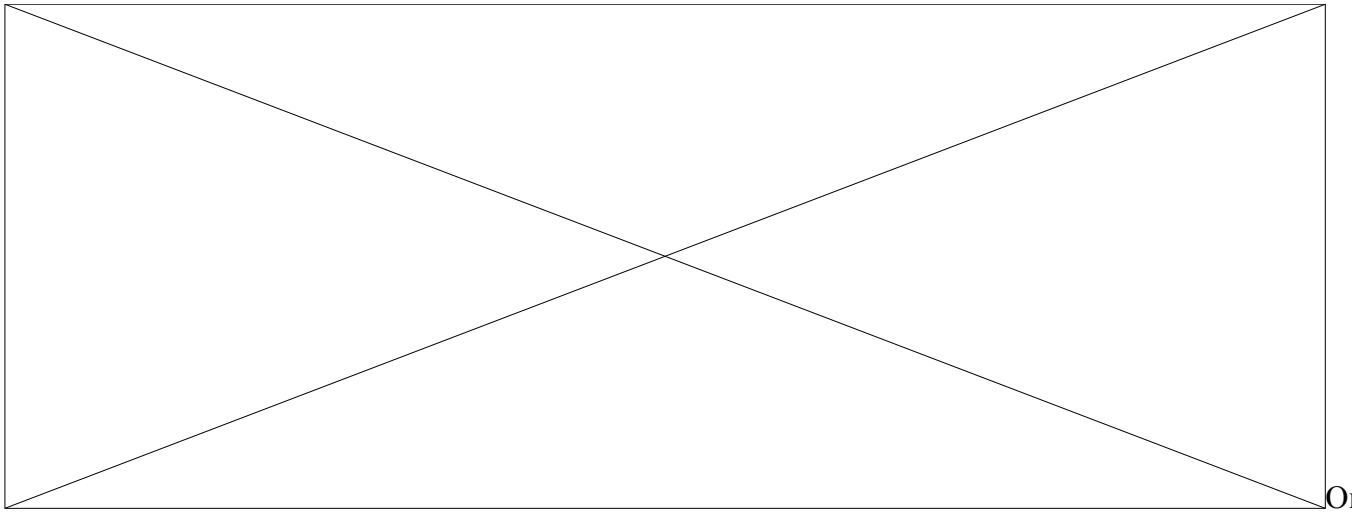
 Ошибка: источник перёкрестной ссылки не найден

Рисунок 2.1 – Схема секретної системи зв’язку

Згідно із запропонованою системою, на боці, де передається повідомлення M_i , розміщено джерело повідомлень і джерело ключів K_j. При цьому на обох множинах M і K задано розподілення $P(M)$ та $P(K)$. Це означає, що для будь-якого $M_i \in M$ певна ймовірність $p(M_i) \in P(M)$, а для будь-якого $K_j \in K$ певна ймовірність $p(K_j) \in P(K)$ і виконуються правила

$$\sum_{M_i \in M} p(M_i) = 1 \quad \text{та} \quad \sum_{K_i \in K} p(K_i) = 1 .$$

Ключ, сформований з боку, звідки подається повідомлення з імовірністю $p(K_j)$, передається на протилежний бік через окремий закритий канал зв’язку, до якого злочинник не повинен мати доступу. Необхідність такого каналу є вельми серйозним недоліком секретних систем, оскільки в мережах з великою кількістю користувачів їхня реалізація вимагає надто потужних ресурсів.

2.3 Вимоги щодо реалізації сучасних криптоалгоритмів

Сучасні криптографічні системи може бути зреалізовувано програмним, програмно-апаратним чи апаратним шляхом.

Існують такі загальні вимоги щодо реалізації криптографічних алгоритмів:

- криптографічні алгоритми має бути адаптовано до новітньої програмно-апаратної бази (приміром, алгоритми блочного шифрування в програмній реалізації має бути адаптовано до операцій з 64-розрядними числами);
- обсяг ключа має відповідати сучасним методам та засобам розшифровування зашифрованих повідомлень;

- операції шифрування й розшифровування мають за можливістю бути простими, щоби задовольняти сучасним вимогам швидкісних характеристик;

- обсяг повідомлення в перебігу виконання операцій шифрування має зводитися до мінімуму;

- має бути виключено явище розмножування помилок.

До недавнього часу алгоритми шифрування зреалізовувалися у вигляді окремих пристроїв, що зумовлювалося використовуванням криптографії задля засекречування різних методів передавання інформації (телеграф, телефон, радіозв'язок). Сьогодні апаратна реалізація також набула широкого застосовування. Це зумовлено такими причинами.

По-перше, апаратна реалізація має кращі швидкісні характеристики, аніж програмно зреалізовувані алгоритми шифрування. Використовування спеціальних чипів, адаптованих до реалізації процедур зашифровування й розшифровування, призводить до того, що, на відміну від процесорів загального призначення, вони дозволяють оптимізовувати багато математичних операцій, застосовуваних алгоритмами шифрування.

По-друге, апаратні засоби захисту інформації мають незрівнянно більшу захищеність як від побічних електромагнітних випромінювань, що виникають у перебігу роботи апаратури, так і від безпосереднього фізичного впливу на пристрої, де здійснюються операції шифрування і зберігання ключової інформації. Ці пристрої виконують в такий спосіб, що, в разі виявлення несанкціонованого доступу до них, вони саморуйнуються.

По-третє, апаратні засоби є більш зручні в експлуатації, тому що дозволяють здійснювати операції зашифровування й розшифровування для користувача в прозорому режимі; окрім того, їх легко інсталювати.

По-четверте, з огляду на різноманіття варіантів застосовування засобів криптографічного захисту інформації, апаратні засоби повсюдно використовуються для захисту телефонних перемовин, відправляння факсимільних повідомлень та інших видів передавання інформації, де неможливо використовувати програмні засоби.

До переваг програмної реалізації можна віднести те, що програма, написана під одну операційну систему, може бути змодифікована під будь-який тип ОС.

Окрім того, поновити програмне забезпечення можна з меншими часовими й фінансовими витратами. До того ж багато сучасних досягнень в області криптографічних протоколів є недоступні для реалізації у вигляді апаратних засобів.

До недоліків програмних засобів криптографічного захисту слід віднести можливість небажаного втручання в дію алгоритмів шифрування й одержання доступу до ключової інформації, що зберігається в загальнодоступній пам'яті.

Отже, слабка фізична захищеність програмних засобів є одним з головних недоліків подібних методів реалізації алгоритмів шифрування. Окрім того, програмна реалізація засобів криптографічного захисту не в змозі забезпечити виконання певних характеристик, необхідних для надійного використовування алгоритмів шифрування. Приміром, генерування ключової інформації не повинно здійснюватися програмними давачами випадкових чисел; для цього треба використовувати спеціальні апаратні пристрої.

Програмно-апаратна реалізація дозволяє користувачам усувати певні недоліки програмних засобів захисту інформації і при цьому зберігати їхні переваги (за винятком цінового критерію).

Головними функціями, покладеними на апаратну частину програмно-апаратного комплексу криптографічного захисту інформації, зазвичай є генерування ключової інформації і зберігання ключової інформації в пристроях, захищених від несанкціонованого доступу з боку

злочинника. Окрім того, за допомогою методик такого типу можна здійснювати автентифікацію користувачів за допомогою паролів (статичних чи динамічно змінюваних, котрі можуть зберігатися на різних носіях ключової інформації – смарт-карти, touch-memory і т.д.) або на підставі унікальних для кожного користувача біометричних характеристик.

2.3.1 Параметри сучасних шифрів

В реальних умовах за побудови криптографічних систем використовуються шифри, які не є досконалими. Це відбувається через те, що надто важко зреалізувати систему, яка формувала б велику кількість випадкових ключів, котрі відповідали б умовам Шеннона, та забезпечувала їхнє вчасне секретне розподілювання у мережах зв'язку з великою кількістю користувачів. Окрім того, недосконаліть шифру зовсім не означає, що він обов'язково буде зламаний. Насправді все залежить від інтелектуальних та обчислювальних ресурсів криптоаналітика. Якщо криптографічне перетворювання передбачає виконання досить великої кількості складних операцій, у потенційного злочинника не вистачить можливостей для того, щоби дешифрувати перехоплене повідомлення за розумний термін.

Таким, чином сучасні криптографічні системи мають будуватись з урахуванням можливостей імовірного злочинника, від якого захищається інформація, і, в такому разі, зрозуміло, виникає запитання про те, в який спосіб ці можливості мають враховуватись.

В якості критерію, за яким оцінюється складність обчислювального процесу за дешифрування повідомлень, найчастіш використовують кількість елементарних операцій w певного типу, які виконуються впродовж часу дешифрування одного повідомлення або визначання одного ключа. В кожному окремому випадку обговорюється, що саме містить термін *елементарна операція*. Це може бути чи сукупність операцій, виконуваних на конкретній апаратурі за один етап шифрування, чи то сукупність операцій, виконуваних упродовж часу однієї спроби підбирання ключа, чи щось інше. Головне – щоби вибір „одиниці" цього виміру було обґрунтовано.

Складність процедур дешифрування залежить від кількості апріорної інформації, яка є в розпорядженні у криптоаналітика. За найскладнішу вважається ситуація, коли, окрім перехопленої криптограми довжиною в N символів, у нього нічого немає. Такий спосіб атаки на шифр називають *аналізом на підставі перехоплених криптограм.*

В цій ситуації єдиним способом дешифрування криптограми є перевірка усіх можливих значень ключа. Якщо його довжина дорівнює довжині повідомлення, сумарна кількість ключів, які треба буде перебрати, становитиме величину 2^N. Цю величину називають *потужністю ключового простору.* Підвищення потужності ключового простору, зрозуміло, збільшує криптографічну стійкість шифру, але не завжди й не неодмінно. Приміром, для шифру простої заміни потужність ключового простору дорівнює величині $m!$, де m – кількість символів у абетці. Хоча за доволі великої довжини тексту потужність ключового простору буде надто великою, а, як відомо, шифри простої заміни ламаються статистичними методами досить легко.

На жаль, не існує універсальних методів, що їх можна було б застосовувати задля криптографічного аналізу будь-яких шифрів. Кожен з відомих шифрів потребує розробляння індивідуального способу аналізу й дешифрування. Надалі під методом аналізу шифру розумітимемо сукупність правил та дій, сформульованих на підставі дослідження конкретного шифру й використання яких дає змогу виконувати дешифрування криптограми з імовірністю, котра відрізнюється від нуля.

Дешифрування з імовірністю, яка відрізнюється від нуля, означає, що, в разі, якщо ми обиратимемо ключ не з усієї з множини K, а

лише з певної її частини K_l K, яка сформована випадковим вибором з K, ймовірність дешифрування збігається з імовірністю потрапляння ключа, за допомогою якого зашифровано повідомлення, до множини K_l.

Для подальшого вивчання засад побудови шифрів, які відповідають заданим умовам щодо їхньої криптографічної стійкості, впровадимо необхідні означення.

Мінімальна ймовірність практичного дешифрування – обґрунтована числова величина, що схарактеризовує практичну значимість алгоритму дешифрування. Ця величина залежить від багатьох параметрів і, першою чергою, від вимог щодо безпеки. Один і той самий шифр за різних умов матиме різні величини цього параметра.

Алгоритм дешифрування – обчислювальний алгоритм, побудований на підставі конкретного методу аналізу шифру, який надає змогу виконувати дешифрування.

Обчислювач – пристрій, який зреалізовує алгоритм дешифрування і має фіксовану кількість команд, кожна з яких називається *елементарною операцією* й виконується за один такт роботи.

Потужність обчислювача – кількість тактів, виконуваних за одну секунду.

Пам'ять обчислювача – доступна пам'ять, використовувана в перебігу обчислювання та зберігання даних.

Надійність алгоритму дешифрування – ймовірність дешифрування, визначувана обраним методом дешифрування та алгоритмом його реалізації.

Складність алгоритму дешифрування – кількість операцій, необхідних задля реалізації алгоритму дешифрування на даному обчислювачі, поділена на надійність даного алгоритму (якщо обчислювач припускає його реалізацію).

Максимально припустима пам'ять – числова величина, яка схарактеризовує практичну значимість алгоритму дешифрування.

Нехай M – множина всіх можливих методів аналізу шифру F з імовірністю дешифрування більше чи дорівнюваною (мінімальна ймовірність практичного дешифрування). Через S визначимо множину всіх алгоритмів дешифрування, котрі потребують пам'яті не більш за величину RAM і відповідають множині M. Окрім того, нехай C – множина всіх обчислювачів. Тоді визначимо через $Q(c, s)$ складність дешифрування алгоритму S по відношенню до обчислювача Q для всіх s S та c C.

З урахуванням розглянутого, можна зробити такий висновок. Стійкістю шифру F, за заданої мінімальної надійності та максимального обсягу пам'яті RAM, називається величина

$$\min_{Q(F) = c \in C, s \in S} Q(c, s)$$

Інакше кажучи, *стійкість шифру* – це кількість операцій, які має бути виконано за умови використовування найбільш ефективного алгоритму та найбільш потужного обчислювача.

Окрім терміну *стійкість*, часто використовують термін *практична стійкість*, який означає складність реалізації найшвидшого з відомих алгоритмів, що відповідає найбільш ефективному з відомих методів на найшвидшому з доступних обчислювачів.

Отже, при створюванні того чи іншого шифру треба враховувати можливості, які має криптоаналітик злочинника. Побудова шифрів, стійкість яких значно перевершує необхідну, не є виправдана, оскільки вона досягається збільшенням часу, витрачуваного на виконання процедур зашифровування та розшифровування, а також використовуванням надто великих обчислювальних ресурсів.

2.3.2 Елементарні криптографічні перетворювання

У статті, опублікованій Шенноном 1949 року, було запропоновано будувати шифри, які задовольняють певним умовам щодо їхньої стійкості, шляхом використовування послідовності операцій заміни, перестановок та функційних перетворювань. Такі операції називають елементарними криптографічними перетворюваннями (рис. 2.2). Щоби перетворювання можна було називати елементарним, воно повинно досить легко зреалізовуватися програмними чи апаратними засобами.

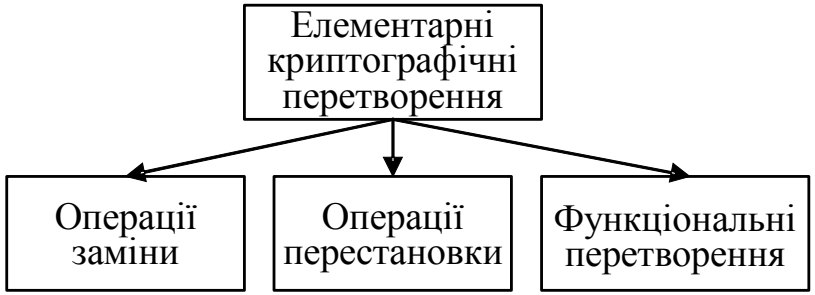


Рисунок 2.2 – Елементарні криптографічні перетворювання

Історично так склалося, що на початку розвинення криптографії утворювались та використовувались шифри, які містили одне просте перетворення. Сьогодні такі перетворювання входять до складу сучасних шифрів у якості елементарних. Здебільшого це були заміни одних символів на інші або їхні переставляння місцями в межах повідомлення, котре мало бути зашифрованим. Причому найбільшу й найрізноманітнішу групу становлять саме *шифри заміни*, тому розглядання елементарних криптографічних перетворювань розпочнемо саме з них.

У загальному випадку шифр заміни можна описати алгебричною моделлю вигляду

$$\Sigma_K = (M, K, C, E, D).$$

Вважатимемо також, що слова відкритого тексту складаються з символів абетки A_n, а слова криптограм – з символів абетки B_m. У загальному випадку у відкритому тексті групи символів, які складаються з абетки A_n, замінюються на групи символів, що складаються з абетки B_m. При цьому довжина шифровеличин та відповідних до них шифроперетворювань може не збігатися. Окрім того, кожній з шифровеличин може бути поставлено у відповідність понад одне шифроперетворювання. Тобто під час зашифровування повідомлення заміна може бути не безваріантною. Щодо розшифровування, то воно залишається однозначним, незалежно від способу зашифровування.

З урахуванням наведеного, множину шифровеличин U можна розглядати як множину слів U_i абетки A^*:

$$U = \{U_1, U_2, \ldots, U_n\},$$

а множину шифроперетворювань V – як множину слів V_i абетки B^*:

$$V = \{V_1, V_2, \ldots, V_n\}.$$

Тоді $M \subset A^*$, а $C \subset B^*$. Якщо кількість символів у абетках A та B відповідно дорівнює n та m, сумарна кількість шифровеличин U_i має становити N n, а сумарна кількість шифроперетворювань V_i – M m.

За такого способу задавання шифру заміни потужність ключового простору r, яка визначає стійкість шифру, буде надто великою.

Множину V можна подати як сімейство з r варіантів такого її розподілення:

$$V = \bigcup_{i=1}^{N} V_\alpha^{(i)}, \quad \alpha = 1,\ldots,r.$$

Для того щоби шифрування було однозначним, всі підмножини $V_\alpha^{(i)}$ не повинні перетинатись, тобто

$$V_\alpha^i \bigcap V_\alpha^{(j)} = \varnothing,$$

і кожна з підмножин $V_\alpha^{(i)}$ не повинна бути порожньою:

$$V_\alpha^i \neq \varnothing, \quad i = 1,...,N, \quad \alpha = 1,...,r.$$

Отже, з урахуванням вищенаведеного, можна надати таке означення: *шифром заміни* є шифр, котрий передбачає заміну шифровеличин відкритого тексту на відповідні до них фіксовані шифроперетворювання або групи шифроперетворювань закритого тексту.

У найпростішому випадку шифровеличини збігаються із символами абетки A_m, за допомогою яких утворюються відкриті повідомлення, а шифроперетворювання – із символами абетки B_n, з якої утворюються криптограми, причому B_n найчастіш є підстановкою на A_m, що утворюється за допомогою відображення $A_m \to A_m$. Тоді $n = m$ і $N = M$. Шифри, які передбачають збіжність довжини шифровеличин та відповідних до них шифроперетворювань, називають *шифрами рівнозначної заміни*. У противному разі мають місце *шифри різнозначної заміни*.

Прикладом такого шифру є шифр Цезаря, котрий вважається за один з перших історично відомих шифрів. Згідно із засадою шифрування, яку він передбачає, кожен символ a_i закритого повідомлення T_i перетворюється на відповідний до нього символ b_i закритого повідомлення T_i' за правилом

$$b_i' = (a_i + k) \bmod m, \quad 1 \le k < m,$$

де k – є ключ до шифру.

У цьому шифрі використовуються лише адитивні операції над елементами множини A_m. Потужність його ключового простору обмежується довжиною абетки, тобто величиною m. Через це його стійкість є надто низька, але, зважаючи на те, що він використовувався в ті часи, коли переважна більшість людей взагалі читати не вміла, вона була достатньою.

Інший варіант цього шифру, котрий з'явився значно пізніше і відомий під назвою афінної системи підстановок Цезаря, окрім адитивних, використовує мультиплікативні операції, передбачає шифрування за правилом

$$b_i' = (ca_i + d) \bmod m, \quad 1 \le c, d < m, \quad (c, m) = 1,$$

де c, d – є цілими числами, причому числа c та m мають бути взаємнопростими для того, щоби забезпечувалась однозначність шифрування.

Потужність ключового простору такого шифру є значно більша по відношенню до попередньої його реалізації й дорівнює $m!$, але він так само має дуже низьку криптографічну стійкість. Статистичні характеристики символів відкритого тексту за таких способів шифрування цілковито переходять на символи у відповідній до нього криптограмі. Це відбувається через те, що обидва наведені приклади відповідають шифрам безваріантної заміни, коли кожен символ відкритого тексту під час його зашифровування завжди перетворюється на один і той самий символ криптограми. Існує багато інших прикладів таких шифрів. До їхнього складу можна віднести шифр Полібія, шифрування за допомогою магічних квадратів, шифрування за допомогою таблиць Трисемуса тощо.

Щоби запобігти повному перенесенню статистичних характеристик відкритих повідомлень на відповідні до них криптограми, минулими часами до складу абетки B_n, з якої утворюються закриті криптограми, додавали додаткові символи в такий спосіб, щоби n було менше за m. Під час зашифровування повідомлень у такий спосіб кожен символ відкритого тексту можна було замінити на один з кількох різних символів заздалегідь окресленої підмножини абетки B_n. Ця засада добре ілюструється рисунком 2.4. Шифри такого типу називають *шифрами багатозначної заміни,* або *шифрами пропорційної заміни*.

Ідея пропорційної заміни полягає в тому, що символи відкритого тексту, які зустрічаються доволі рідко порівняно з іншими, повинні передбачати більшу кількість варіантів заміни. Така процедура є вельми ефективним способом підвищення стійкості шифру стосовно способів його статистичного криптоаналізу. На відміну від шифрів багатозначної заміни, шифри, котрі передбачають лише один варіант заміни, називають *шифрами безваріантної заміни*.

Наведені вище приклади шифрів заміни є одноабетковими шифрами. Намагання подальшого підвищення їхньої стійкості стосовно різноманітних способів статистичного криптоаналізу призвело до побудови так званих багатоабеткових шифрів. Їхнє формальне подавання наведено вище. *Багатоабетковим шифром* заміни є шифр, у якому залежність поміж шифровеличинами у відкритому тексті та відповідними до них шифроперетворюваннями у закритому тексті зберігається лише для окремих частин повідомлення, котре підлягає шифруванню.

Щоби зреалізувати багатоабеткову заміну, повідомлення, котре підлягає зашифровуванню, має бути поділене на блоки однакової довжини (останній блок може мати меншу довжину). Надалі кожен символ чергового блока, котрий має бути зашифрованим, перетворюється на символ криптограми шляхом заміни його на відповідний символ окремої абетки.

Сумарна кількість таких абеток дорівнює довжині блока.

Зрозуміло, що шифри багатоабеткової заміни мають вищу стійкість до різноманітних способів статистичного криптоаналізу порівняно з одноабетковими шифрами. Розроблено багато варіантів таких шифрів, котрі забезпечують достатньо високу криптографічну стійкість навіть з огляду вимог нинішнього часу. З-посеред них найбільш цікавими були роторні машини, які дозволяли змеханізовувати процедури шифрування великих обсягів повідомлень.

Шифрування відкритих текстів способом перестановки передбачає зміну позицій шифровеличин у відкритому повідомленні. У сучасних криптосистемах такі шифри використовуються зазвичай у комбінації з іншими типами криптографічних перетворювань.

Для подальшої формалізації шифрів перестановки надамо означення перестановки.

Перестановкою набору цілих чисел від 0 до N - 1 називатимемо змінювання порядку їхнього запису. Для того, щоби зазначити, що символ a_i переставлено з i-тої позиції на позицію (i), де 0 $(i) < n$, скористаємось таким записом:

$$\sigma = (\sigma(0), \sigma(1),..., \sigma(N-1)).$$

Сумарна кількість переставлянь на множині $(0, 1, \ldots, N-1)$ дорівнює

$$n! = (1 \cdot 2 \cdot 3 \cdot ... \cdot (N-1) \cdot N).$$

Далі перестановку набору $S = \{ S_0, S_1, ..., S_{N-1}\}$ символів розглядатимемо як взаємно-однозначне відображення на себе:

$$\sigma : S \to S,$$

$$\sigma : s_i \to s_{\sigma(i)}, \quad 0 \le i < N-1.$$

Якщо повідомлення, котре підлягає зашифровуванню, сформоване символами абетки A, сумарна кількість яких дорівнює m, сумарна кількість варіантів, які дають змогу утворити перестановку у групі з n символів, дорівнює $(m^n)!$.

Реалізація шифрів перестановки засадничо вимагає попереднього поділу відкритого тексту на блоки однакової довжини в тих ситуаціях, коли сумарна довжина тексту перевищує певну величину, яка визначається типом шифру. При такому поділі кожен блок зашифровується незалежно від решти блоків.

Довжина блока визначає потужність ключового простору. Якщо вона складається з бінарних символів і дорівнює п’яти, існує 120 способів її переставлянь. Це означає, що для реалізації такого шифру потрібен пристрій, пам’ять якого має вміщувати всі 120 таблиць відповідних переставлянь, тобто 2880 біт. У разі ж, коли довжина блока становить 128 символів, операція переставляння стає технічно неможливою, хоча потужність ключового простору, який вона може забезпечити, дорівнюватиме 2^{128}, або 10^{38}. В цьому полягає фундаментальна дилема криптографії: ми знаємо, що є ідеал, але для нас він є практично недосяжний.

Щодо згаданої ситуації, то слід пам’ятати, що очевидною слабкою стороною шифрів перестановки є повне перенесення статистичних характеристик символів відкритих текстів на символи криптограм. Однак ця властивість не є їхньою невід’ємною негативною властивістю – вона зумовлена обраною довжиною блока.

За приклади шифрів перестановки може слугувати велика кількість табличних шифрів, використовуваних у “докомп’ютерний” період криптографії. У сучасних криптографічних системах операції переставляння символів входять як обов’язкова складова частина загального алгоритму.

2.3.3 Побудова композиційних шифрів

Будь-яка секретна система являє собою відображення множини повідомлень M, які мають передаватись через незахищений канал, у

множину криптограм M'. Раніше було показано, що реалізація таких відображень за допомогою елементарних перетворювань супроводжується перенесенням статистичних характеристик відкритих текстів на відповідні до них криптограми. Намагання скасувати цей недолік певного часу породило ідею побудови композиційних шифрів, суть якої полягає в тому, що комбінація двох чи більшої кількості секретних систем має більшу криптографічну стійкість, аніж кожна зі складових систем окремо. Дотепер існує два основних способи перетворювання двох чи більшої кількості секретних систем на певну спільну систему.

Першим таким способом є використовування операції *множення* кількох секретних систем. Приміром, якщо їх дві R_1 і R_2 (як це подано на рис.2.5), то спочатку повідомлення зашифровується за допомогою системи R_1, а потім, утворена в такий спосіб криптограма, знову підлягає зашифровуванню вже за допомогою секретної системи R_2. Ключ спільної системи S, який являє собою добуток складових систем і визначається за правилом

$S = R_1 \cdot R_2$

містить у собі обидва відповідні складові ключі, що обираються незалежно один від одного, кожен з власною ймовірністю.

Отже, якщо система R_1 передбачає наявність m ключів, які обираються відповідно з імовірностями

$p_1, p_2, ..., p_m,$

а система R_2 – n ключів, які обираються відповідно з імовірностями

$p_1', p_2', ..., p_n',$

спільна секретна система матиме mn ключів, які обираються з імовірностями $p_i p_j'$ відповідно.

Слід пам'ятати, що множення секретних систем у загальному випадку не є комутативним (тобто $R_1 R_2 \neq R_2 R_1$), хоча можуть існувати й виняткові ситуації.

Принцип реалізації складної секретної системи зв'язку з використовуванням множення простих систем подано на рис. 2.5. З цього рисунка видно, що на приймальному боці процедури розшифровування мають виконуватись у зворотному порядку у відповідності до процедур зашифровування на боці джерела повідомлень.

Множення секретних систем у сучасних криптографічних системах використовується досить часто. Наприклад, спочатку використовується шифрування способом підстановки (заміни), а потім — шифрування способом перестановки, або ще якось інакше. Саме такий *лінійний спосіб* побудови складних секретних систем свого часу було рекомендовано К. Шенноном. Він стверджував, що досягнення необхідної стійкості має відбуватись за рахунок чергування достатньої кількості різних елементарних операцій криптографічного перетворювання. При цьому слід зауважити, що набір функційних перетворювань, використовуваних у якості елементарних, обмежується набором команд процесора обчислювального пристрою. Найоптимальніше, якщо такі елементарні перетворювання будуть параметричними, тобто такими, котрі залежать кожне від власного ключа (рис. 2.6).

Дотримання рекомендацій, запропонованих К. Шенноном, забезпечує необхідну стійкість за рахунок *перемішування* та *розсіювання* символів відкритого тексту.

Розсіювання – це властивість шифру, яка вказує на те, в який спосіб кожен символ у відкритому тексті впливає на шифрування символів у закритому тексті. У оптимальному разі кожен із символів відкритого тексту має впливати на всі символи у закритому тексті. Це означає, що коли у відкритому тексті (блоці) змінити хоча б один символ, то у відповідному до нього закритому тексті (блоці) кожен символ змінить власне значення на протилежне з імовірністю, дорівнюваною 0,5.

Перемішування – це здатність шифру приховувати статистичну залежність поміж символами відкритого тексту та символами у відповідній до нього криптограмі. Якщо алгоритм зашифровування забезпечує доволі якісне перемішування символів відкритого тексту, то поміж символами відкритого та закритого текстів не існуватиме жодних статистичних та функційних залежностей.

Шифр, який достатньою мірою відповідає цим умовам, може бути розкрито лише повним перебиранням ключів по всій їхній множині. Першою серйозною спробою побудувати такий шифр була система “Люцифер”. Вона передбачає поступове чергування замін та переставлянь символів відкритого тексту.

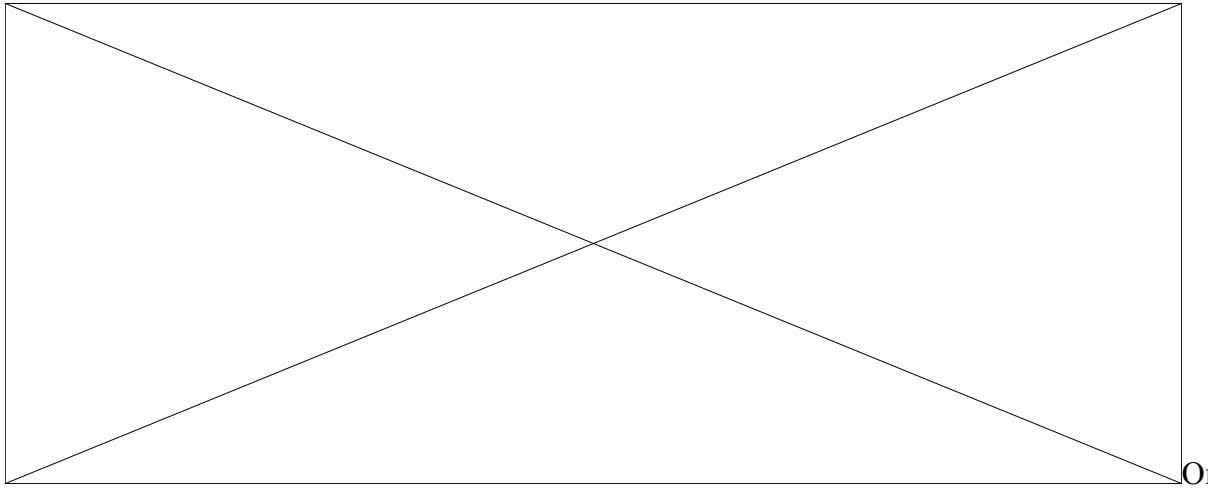
Спрощену систему “Люцифер” наведено на рис. 2.7.

Перед тим як виконувати зашифровування, повідомлення поділяють на блоки фіксованої довжини.

У зв’язку з тим, що реалізація замін та перестановок символів потребує доволі великої пам’яті, черговий блок інформації, який підлягає зашифровуванню, поділяється на блоки меншої довжини. У наведеному на рисунку прикладі 16-розрядний блок поділяється на чотири 4-розрядні блоки, для кожного з яких передбачається наявність 32-бітового блока пам’яті S, що забезпечують заміну вхідних

символів.

Виходи всіх блоків S під'єднуються до загального блока P, який забезпечує переставляння вхідних символів. Загальна пам'ять, якої потребує реалізація такого блока, має становити лише 32 біти.

 Ошибка: источник перёкрестной ссылки не найден

Саме виконання рівномірного переставляння у межах всього 16-розрядного блока надає ефективності розсіюванню символів блока, який підлягає зашифровуванню.

Для того щоби наведена система забезпечувала високу криптографічну стійкість, кількість етапів чергування замін та переставлянь повинна бути великою, а кожен символ на її виході має бути складною функцією від символів на всіх її входах. Що стосується секретності цієї системи, то для її забезпечення необхідно, щоби заміни та переставляння, які виконуються блоками S та P відповідно, були параметричними. Це означає, що для кожного етапу криптографічного перетворювання має існувати власний окремий і незалежний від інших ключ K_i.

Система "Люцифер" була майже єдиною спробою зреалізувати ефективну лінійну систему криптографічного перетворювання, котра виконувалась корпорацією IBM. Як стало зрозуміло пізніше, забезпечення необхідної криптографічної стійкості у такій системі потребувало великої кількості етапів шифрування і, як наслідок, великих обчислювальних ресурсів.

Другий спосіб формування складних криптографічних систем називається *виваженою сумою* і передбачає наявність кількох простих систем (двох і більш, наприклад R_1 та R_2). Кожного разу перед зашифровуванням чергового повідомлення, випадково, з імовірністю p, обирається система шифрування R_1 або система шифрування R_2, з імовірністю $q = 1 - p$. Отже, в загальному випадку, у криптографічному перетворюванні повідомлення братиме участь одна з двох окремих секретних систем із спільною областю визначання за правилом

$S = p_1R_1 + p_2R_2$. Щоби таку систему можна було практично зреалізувати, необхідно, аби вибір секретної системи повністю зумовлювався складом ключа. В цьому разі буде забезпечено збіжність процедур зашифровування та розшифровування як на боці джерела повідомлень, так і на приймальному боці.

Наведена система передбачає наявність m ключів, які обираються відповідно з імовірностями

$p_1, p_2, ..., p_m,$

кожен з яких перетворює повідомлення M_i на одну з m можливих криптограм. Якщо на підставі обраного ключа буде обрано систему R_1, то повідомлення M_i буде перетворене на одну з криптограм $M_1^1, M_2^1, ..., M_m^1$, з імовірностями $pp_1, pp_2, ..., pp_m$. Якщо ж, навпаки, буде обрано систему R_2, це повідомлення буде перетворене на одну з криптограм $M_1^2, M_2^2, ..., M_m^2$, з імовірностями $qp_1, qp_2, ..., qp_m$.

Наведений спосіб формування композиційного шифру дає змогу робити вибір з будь-якої кількості секретних систем. У загальному випадку її можна подати як

$$S = p_1R_1 + p_2R_2 + p_3R_3 + ... + p_nR_n, \quad \sum p_i = 1.$$

Це означає, що криптоаналітик злочинника, окрім визначення ключа, має робити вибір щодо секретної системи, що значно ускладнює дешифрування. Щоби це було насправді так, алгоритм вибору системи повинен також триматись у секреті.

2.4 Блочні шифри

2.4.1 Загальні відомості про блочні шифри

При блочному шифруванні вихідний текст спочатку розбивається на однакові за довжиною блоки, а потім для перетворювання блока відкритого тексту на блок шифртексту застосовується функція шифрування, яка залежить від ключа.

Поділ повідомлення на блоки є пов’язаний з технічними та алгоритмічними особливостями реалізації криптографічних систем.

Вибір довжини блока визначає потужність вхідної абетки. Збільшення такої потужності зумовлює необхідність

попереднього досліджування обраних способів криптографічних перетворювань, які обираються до складу алгоритму шифрування. При цьому за критерій якості способу поділу на блоки та архітектури створеного алгоритму обираються експлуатаційні характеристики криптографічної системи. Власне кажучи, потужність вхідної абетки першою чергою залежить від довжини слова мікропроцесора, який використовується обчислювальною системою, котра є у розпорядженні власників інформаційних ресурсів та потенційних порушників. Блочні шифри, на відміну від поточних, мають додаткові можливості підвищування їхньої криптографічної стійкості.

Під час шифрування текстів з малою ентропією існує можливість побудови для них статистичних способів дешифрування, подібних до тих, котрі використовуються при аналізуванні шифрів простої заміни. Підвищування довжини вхідного слова зумовлює зростання середньої ентропії на знак, а це, своєю чергою, призводить до нелінійного зростання складності статистичного криптоаналізу зашифрованого тексту.

Зворотний бік зростання складності криптоаналізу блочних шифрів –складність доказового обґрунтовування їхньої криптографічної стійкості.

Щоби позбутись цієї проблеми, довжина блока обирається не надто великою і операції шифрування, котрі входять до складу алгоритму шифрування, повторюються кілька разів. У переважної більшості криптографічних систем, які було запропоновано розробниками у якості державних стандартів упродовж 70–80 років двадцятого сторіччя, довжина блока дорівнює 64 бітам. Якщо зменшити довжину блока, дешифрування криптограм легко виконується із застосовуванням незначних обчислювальних ресурсів. Збільшення цієї довжини, навпаки, призводить до зростання терміну шифрування та кількості необхідних обчислювальних ресурсів.

Усі блочні шифри мають ще два суттєвих недоліки, для усунення яких треба вживати спеціальних заходів.

Перший полягає у тому, що довжина вхідного слова, передбаченого алгоритмом шифрування, є фіксованою, а повідомлення, які підлягають шифруванню, в загальному випадку мають довжину, що не є кратною довжині вхідного слова. Це означає, що останній блок, як правило, буде мати меншу довжину. Якщо доповнити його будь-якими символами, наприклад нулями, то, у середньому, половина останнього блока буде відома криптоаналітикові злочинника. А це, своєю чергою, значно зменшить криптографічну стійкість алгоритму шифрування. З метою усунення такого недоліку розроблено як загальні, прийнятні для усіх блочних алгоритмів способи, так й індивідуальні, прийнятні для конкретних криптографічних систем.

Друга проблема полягає у тому, що однакові блоки будуть зашифровані однаково, а це дозволить злочинникові отримувати допоміжну інформацію, що значно підвищить його можливості у виконанні статистичного криптоаналізу.

Для усунення цього недоліку також свого часу було запропоновано відповідні заходи щодо захисту, опис яких буде наведено далі.

У сучасних блочних шифрах блоки відкритого тексту та шифртексту являють собою двійкові послідовності довжиною зазвичай 64 біти, тобто кожний блок може набувати 2^{64} значень. Тому підстановки виконуються в абетках надто великого обсягу ($2^{64} \approx 10^{19}$ символів).

Під *N-розрядним блоком* розумітимемо послідовність з одиниць та нулів довжини N:

$$x = (x_0, x_1, \ldots, x_{n-1}) \in Z_{2,N},$$

де x в $Z_{2,N}$ можна тлумачити як вектор та як двійкове подавання цілого числа

$$\|x\| = \sum_{i=0}^{N-1} x_i 2^{N-i-1}.$$

Приміром, якщо $N = 4$, то

(0,0,0,0) → 0	(0,1,0,0) → 4	(1,0,0,0) → 8	(1,1,0,0) → 12
(0,0,0,1) → 1	(0,1,0,1) → 5	(1,0,0,1) → 9	(1,1,0,1) → 13
(0,0,1,0) → 2	(0,1,1,0) → 6	(1,0,1,0) → 10	(1,1,1,0) → 14
(0,0,1,1) → 3	(0,1,1,1) → 7	(1,0,1,1) → 11	(1,1,1,1) → 15

Незважаючи на те, що блочні шифри є випадковою подією підстановок (лише на абетках надто великого розміру), їх треба розглядати окремо.

По-перше, більшість симетричних шифрів, використовуваних в системах передавання повідомлень, є блочними шифрами.

По-друге, блочні шифри зручніше описувати в алгоритмічному вигляді, а не як звичайні підстановки.

Блочним шифром називатимемо елемент $\in \overline{SYM}\,(Z_{2,N})$, $: x \to y = (x)$,
де $x = (x_0, x_1, \ldots, x_{N-1})$, $y = (y_0, y_1, \ldots, y_{N-1})$.

Припустімо, що

$$(x_i) = y_i,\ 0 \le i < m,$$

для певного $\in \overline{SYM}\,(Z_{2,N})$, вихідного тексту $X = \{ x_i : x_i \in Z_{2,N} \}$ та шифртексту $Y = \{y_i\}$.

Якщо $x \notin \{x_i\}$, то $(x_i) \notin \{y_i\}$, оскільки є перестановкою на $Z_{2,N}$.

Коли відомо, що належить до невеликої підмножині П з $\overline{SYM}\,(Z_{2,N})$, тоді можна зробити певний висновок. Наприклад, коли

$$\Pi = \{_j : 0 \le j < 2^N \},\ _j(i) = (i+j) \pmod{2^N},\ 0 \le i < 2,$$

то значення (x) за заданого значення x безваріантно визначає . В цьому разі X є підмножиною підстановки Цезаря на $Z_{2,N}$.

Криптографічне значення цієї властивості має бути явним: якщо вихідний текст шифрується підстановкою , яку обрано з повної симетричної групи, тоді злочинник, котрий шукатиме відповідність вихідного та шифрованного текстів

$$x_i \leftrightarrow y_i,\ 0 \le i < m,$$

не зможе визначити вихідний текст, який відповідав би $y \notin \{y_i\}$.

Якщо для шифрування вихідного тексту використовується підсистема з $\Pi \in \overline{SYM}\,(Z_{2,N})$, тоді систему, яку буде здобуто після підстановок П, називатимемо системою *блочних шифрів,* чи *системою блочних підстановок*.

Ключовою системою блочних шифрів є підмножина П[*K*] симетричної групи $\overline{SYM}\,(Z_{2,N})$

$$\Pi[K] = \{ \{K\} : K \in \overline{K}.\},$$

яка індексується за параметром $K \in \overline{K}$; де *K* – ключ, а $\overline{K}$. – простір ключей. При цьому треба, щоби різні ключі відповідали різним підстановкам $Z_{2,N}$.

Ключова система блочних шифрів П[*K*] використовується в такий спосіб. Користувач *i* та користувач *j* певним чином укладають угоду відносно ключа *k* з К, тобто обирають елемент з П[*K*] й передають текст, зашифровуваний з використанням обраної підстановки. Для того щоби позначити *N*-розрядний блок шифрованого тексту, який відповідає *N*-розрядному блокові вихідного тексту з використанням підстановки $\{K\}$ за допомогою ключа *K,* наведемо запис

$$y = \{K,x\}.$$

Припустімо, що злочинникові

- відомий простір ключів;
- відомий алгоритм визначання підстановки $\{K\}$ за значенням ключа *K*;
- невідомо, який саме ключ обрано користувачем.

Тоді злочинник може:

- здобути ключа внаслідок недбалості користувача i та користувача j;
- перехопити (шляхом перехоплення телефонних та комп'ютерних повідомлень) шифрований текст y, який передається від користувача i до користувача j, а потім „перебирати" усі ключі з ключового простору $\overline{K}$, доти, аж допоки не буде одержано повідомлення вихідного тексту, яке можна було б розуміти;
- здобути відповідні вихідний та шифрований тексти $(x \leftrightarrow y)$ та скористатися методом „перебирання" усіх ключів з ключового простору К;
- зробити каталог N-розрядних блоків, де записувалась частість їхньої появи у вихідному та шифрованому текстах.

Каталог надає змогу вишуковувати найвірогідніші слова, користуючись при цьому такою інформацією:

- лістинг мовою асемблера схарактеризовується вельми виявленим структурованим форматом;
- цифрове подавання графічної та звукової інформації має невеликий набір знаків.

Припустімо, що N=64 та кожний елемент $\overline{SYM}\,(Z_{2,N})$ може використовуватися як підстановка, так що $\overline{K} = \overline{SYM}\,(Z_{2,N})$.

Тоді:

- існує 2^{64} 64-розрядних блоків; злочинник не може використовувати каталог з $2^{64} \approx 1.8 \cdot 10^{19}$ рядками;
- випробування на ключ за кількості ключів, дорівнюваній $(2^{64})!$, практично є неможливими; відповідність вихідного та зашифровуваного текстів для певних N -розрядних блоків $\{K, x_i\} = y_i$, $0 \le i < m$, не надає злочинникові жодної інформації стосовно значення $\{K, x\}$ для $x \notin \{x_i\}$.

Системи шифрування з блочними шифрами, абеткою $Z_{2,64}$ та простором ключів $\overline{K} = \overline{SYM}\,(Z_{2,64})$ є неподільними (тому що виходять за межі можливостей як злочинника, так і того користувача, котрий створив вихідний текст).

Отже, вимоги щодо блочного шифру:

- доволі велике N (64 чи більше), для того щоби ускладнити користування каталогом;
- доволі великий простір ключів, для того щоби виключити можливість підбирання ключів;
- складні співвідношення $\{K, x\}$: $x \rightarrow y = (K, x)$ поміж вихідним повідомленням та шифртекстом, для того щоби аналітичні та/чи статистичні методи визначання вихідного тексту та/чи ключа на базі відповідності вихідного повідомлення та шифртексту не можна було зреалізовувати.

2.4.2 Генерування блочних шифрів

2.4.2.1 Використовування нелінійних структур задля побудови блочних шифрів

Комбінація простих шифрувальних перетворювань у лінійний ланцюжок дозволяє створити цілковито надійний складний шифр. Проблема полягає в тому, що для розв'язування такого завдання потрібна надто велика кількість перетворювань. З цієї причини в сучасних криптосистемах набула поширювання інша схема, відмінність якої полягає у використовуванні нелінійних структур та операцій над шифрувальними блоками даних. Нелінійність структури шифрувального перетворювання набагато ускладнює процедури криптоаналізу. Застосовування, на додаток до цього, в алгоритмі шифрування операцій функційного перетворювання також істотно ускладнює процедуру перетворювання шифрувального блока (кількості можливих варіантів).

Встановлено, що більш оптимально є не перетворювати переданий блок відповідно до застосовуваного ключа, а спочатку скомбінувати цей блок зі значенням ключа, а вже потім піддавати його певному перетворюванню.

Рисунок 2.10 – Операція над
шифрувальними даними на підставі

Рисунок 2.9 – Варіант попередньої
комбінації даних і ключа

У сучасних криптографічних системах, застосовують зазвичай адитивні та, значно рідше, мультиплікативні операції над шифрувальними даними.

Слід мати на увазі, що, застосовуючи певну операцію «», треба подбати, щоби для неї існувала обернена до неї операція «», тобто вона маєбути придатна для реалізації умов побудови симетричної криптосистеми (рис. 2.10):

$$(M \circ K)\ K = M.$$

Складність операції також може бути підвищено, якщо комбінуватиме дані не сам ключ, а певний скомбінований з нього код, котрий залежить від даних:

$$M_{i+1} = M_i \; f(M_i, K_i).$$

У загальному вигляді цю функцію можна записати як

$$M_{i+1} = F(M_i, K_i).$$

Відмінність цих виразів полягає в тому, що функція F повинна мати обернену операцію, а функція f – необов'язково.

Від функції f потрібні максимально можлива складність (кількість можливих варіантів перетворювання) та нелінійність перетворювань. Іншою вимогою до функції є виконання умови оберненості перетворювань.

M_i K_i

M_{i+1}

Рисунок 2.11– Операція над шифрувальними даними на підставі функційних перетворювань

Складність проблеми полягає в тім, що оберненість перетворювань є особливістю лінійних систем. Розв'язок нелінійних рівнянь щодо одного з аргументів у загальному вигляді є відсутній.

Оберненість виразу означає, що має існувати ефективна обчислювальна функція $G(M_{i+1}, K_i)$, яка задовольняла б умові

$$f(M_i, K_i) = G(M_{i+1}, K_i).$$

З розглянутого випливає, що задля побудови ефективного шифру слід визначати пари функцій, які були б нелінійні й, водночас, обернені одна до одної.

За приклад пари операцій такого типу, які широко застосовуються в сучасних симетричних криптосистемах, слугують подані нижче перетворювання.

2.4.2.2 Використовування мереж Фейстеля для побудови блочних шифрів

Найпоширеним способом створювання блочних шифрів є використовування мереж Фейстеля (рис. 2.12).

Рисунок 2.12 – Схема мережі Фейстеля

Підвищення ефективності шифрування було можливим лише у разі відмови від лінійної структури алгоритму. Але в цьому разі надто важко забезпечити обернений характер криптографічних перетворювань. Проблема полягала у тім, щоби побудувати алгоритм, який не містив би їх взагалі. І це завдання було розв'язано співробітниками лабораторії фірми IBM *Watson Research Lab* нової оригінальної архітектури симетричного шифру на базі необернених перетворювань.

Як відомо, ідея використовування оберненої операції додавання за модулем два, виникла доволі давно. Її запропонував Вернам ще 1925 року для побудови шифру, котрий, як стало зрозуміло значно пізніше, був досконалим. Стійкість такого способу визначається властивостями шифрувальної гамми. Спосіб її формування є найскладнішою з проблем сучасної криптографії.

Якщо гамма побудована за допомогою будь-якого, зреалізованого програмним методом генератора, вона неодмінно буде рекурентною, тобто її вміст матиме скінченну довжину й циклічно повторюватиметься через певну кількість кроків. Визначивши період повторювання такої гамми, віднайти її вміст не так вже й складно. В усякому разі, це завдання не є складним для криптоаналітика, котрий має доволі великі обчислювальні ресурси. Якщо ж формувати гамму за допомогою складних апаратних засобів, які використовують не рекурентні, а реальні випадкові процеси, процедура розподілу ключової інформації стає надто складною.

Хорст Фейстель підійшов до проблеми в такий спосіб. Він запропонував формувати шифрувальну гамму з самої інформації, яка підлягає шифруванню (див. рис.2.12).

Спочатку масив інформації, який має бути зашифрованим, поділяється на блоки фіксованої довжини. Кожен з таких блоків під час кожної ітерації шифрування поділяється на дві однакові частини: ліву L_i й праву R_i. Потім з правої частини формується шифрувальна гамма, довжина якої дорівнює половині блока. Принцип її формування визначається за допомогою складного нелінійного функційного перетворювання $F_i(R_i, K_i)$, яке залежить від ключа. Перша (ліва) половина нового (утвореного впродовж однієї ітерації) блока L_{i+1} утворюється з правої половини попереднього блока R_i, тобто

$$L_{i+1} = R_i.$$

Щодо другої (правої) половини нового блока, то вона є результатом гаммування лівої половини попереднього блока (складанням її "за модулем два" зі створеною гаммою) за правилом

$$R_{i+1} = L_i \ F_i(R_i, K_i)$$

Як видно з цього виразу, перетворювання правої частини блока залежить від вмісту ключа K_i. Це означає, що для кожної ітерації шифрування потрібен окремий ключ. Отже, як і у схемі, яку запропонував К. Шеннон, кожне перетворювання блока, який підлягає шифруванню, має бути параметричним (тобто таким, що залежить від певного параметра). Окрім того, зважаючи на те, що впродовж однієї ітерації буде зашифровано лише половину блока, сумарна їхня кількість має бути парною. І самі ключі K_i і функції $F_i(R_i, K_i)$ можуть мати власний вигляд для кожного етапу шифрування. Що стосується проміжних ключів, то вони можуть бути сформовані з головного ключа за допомогою певного алгоритму чи окремо, в такий спосіб, щоби вони були незалежні один від одного.

У разі якщо довжина лівої частини блока дорівнюватиме довжині його правої частини, матиме місце так звана *збалансована* схема Фейстеля; в іншому разі – це *розбалансована* схема Фейстеля. Це, своєю чергою, потребує формування різних за довжиною шифрувальних гамм та різних функцій для виконання відповідних нелінійних перетворювань, залежно від номера ітерації.

Зазвичай виникає запитання про те, чи буде перетворювання, зреалізоване за допомогою схеми Фейстеля, оберненим? Властивість схеми Фейстеля полягає в тому, що навіть коли в якості нелінійного перетворювання використовується функція, яка сама не є оберненою, або до якої не існує оберненої функції, перетворення залишається оберненим. Річ тут у тім, що для виконання оберненого перетворювання не треба обчислювати функцію $F_i^{-1}(R_i, K_i)$. Єдине, про що слід пам'ятати: під час розшифровування даних проміжні ключі мають використовуватися у зворотному порядку. Більш того, схема Фейстеля є симетричною.

Наявність в алгоритмі операції додавання за модулем два дозволяє виконувати операції розшифровування даних за допомогою того самого алгоритму, яким їх було зашифровано.

Стійкість криптосистеми, побудованої на базі схеми Фейстеля, цілком залежить від вигляду нелінійної функції гаммування $F_i(R_i, K_i)$, яке виконується впродовж кількох ітерацій. Через це, задля забезпечення надійного зашифровування загальна кількість етапів має бути доволі великою. Чим більше їхня кількість, тим оптимальніше виконується розсіювання та перемішування символів відкритого тексту й тим вище буде стійкість шифру до диференційного та лінійного криптоаналізу.

Практично всі відомі шифри побудовано на базі збалансованої схеми Фейстеля, а нелінійне функційне перетворювання, використовуване на кожному етапі шифрування, є одне й те саме. Такі схеми називають *гомогенними*, у

противному разі – *гетерогенними*. Використовування гетерогенної схеми Фейстеля забезпечує потужнішу стійкість шифрів, але їхня побудова являє собою надто складне завдання через необхідність забезпечення оберненості алгоритму шифрування. Популярність гомогенної збалансованої схеми визначається тим, що їхня реалізація є значно дешевше, швидкість шифрування вище, а потрібна стійкість легко досягається ускладненням нелінійної функції шифрування та незначним збільшенням кількості етапів перетворювання відкритого тексту.

Для того щоби ще більш употужнити стійкість гомогенних алгоритмів, ключ, який подається на вхід нелінійної функції, складається за будь-яким модулем із гаммою, утвореною на попередньому етапі. Така операція поширює вплив результатів шифрування кожної ітерації на шифрування на наступних етапах.

Майже всі шифри, котрі стали державними стандартами шифрування у різних країнах світу, використовують схему Фейстеля, яка вельми добре пройшла випробування часом. У таких шифрах незначні модифікації, як правило, стосуються додаткових початкових та завершальних операцій над блоком даних, який підлягає шифруванню, і виконують його рандомізацію.

Щодо рандомізації, то ця операція є не що інше як гаммування блока даних перед початком його шифрування. Гамма повинна мати такі статистичні дані, щоби символи у здобутому після цього блоці були рівномірно розподілені по його довжині.

Останніми роками зустрічаються модифікації, які передбачають збільшення кількості гілок у запропонованій схемі. Це пояснюється тим, що збільшення довжини блока понад 128 символів призводить до ускладнення виконання математичних операцій за модулем 64 й вище. Найчастіше зустрічаються схеми, котрі містять чотири гілки (рис.2.13 та рис. 2.14).

Насамкінець слід зауважити, що на понад 95 відсотків стійкість шифру, побудованого на базі схеми Фейстеля, визначається складністю функції нелінійного перетворювання $F_i(R_i, K_i)$ і правилом обчислювання ключа K_i.

2.5 Поточні шифри

Зазвичай, шифри, котрі потребують попереднього поділяння відкритого тексту на блоки однакової довжини й подальшого зашифровування кожного з них окремо, називають *блочними шифрами*. У противному разі, мають місце *поточні шифри.* Інакше кажучи, в поточних алгоритмах кожен символ відкритого тексту шифрується незалежно від інших і розшифровується в такий самий спосіб.

Поточне шифрування полягає в тому, що біти вихідного тексту додаються за модулем два до псевдовипадкової послідовності, яку іноді називають гаммою. Від того, наскільки утворена гамма матиме властивість рівноймовірності появи її символів, залежить стійкість поточних алгоритмів шифрування.

До переваг поточних шифрів слід віднести те, що вони мають високу швидкість шифрування, відносно просто зреалізовуються та при цьому методі шифрування відсутнє розповсюдження помилок. Недоліком їхнім є необхідність передавання синхронізувальної інформації раніш за повідомлення. Це може становити загрозу криптостійкості системи.

Тому використовують додатковий, випадковий ключ повідомлення, який має змодифіковувати ключі, які шифрують повідомлення.

На практиці цей метод шифрування використовують тоді, коли треба зашифрувати повідомлення потужної довжини.

2.6 Шифри гаммування

2.6.1 Накладання гамми шифру на відкритий текст

Гаммування не можна цілковито виокремити в окремий клас криптографічних перетворювань, позаяк ця псевдовипадкова послідовність може створюватися, наприклад, за допомогою блочного шифру.

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 накладанні здобутої гамми на вихідний відкритий текст у зворотний спосіб, приміром з використовуванням операції додавання за модулем два.

Слід зазначити, що перед зашифровуванням відкриті дані розбивають на блоки $M_0^{(i)}$ однакової довжини, зазвичай по 64 біти. Гамма шифру створюється у вигляді послідовності блоків $\Gamma_{\text{ш}}^{(i)}$ аналогічної довжини.

Рівняння зашифровування можна записати у вигляді

$$M_{\text{ш}}^{(i)} = \Gamma_{\text{ш}}^{(i)} \oplus M_0^{(i)}, \quad i = 1, ..., N,$$

де $M_{\text{ш}}^{(i)}$ – i-тий блок шифртексту; $\Gamma_{\text{ш}}^{(i)}$ – i-тий блок гамми шифру; $M_0^{(i)}$ – i-тий блок відкритого тексту; N – кількість блоків відкритого тексту.

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

$$M_0^{(i)} = \Gamma_{\text{ш}}^{(i)} \quad M_{\text{ш}}^{(i)}.$$

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 злочинникові 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.

2.6.2 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 A = 00000, B = 00001, C = 00010 і т. д.), за допомогою побітового додавання за модулем два – і в результаті виходить шифрований текст.

Генерування непередбачуваних двійкових послідовностей великої довжини є однією з важливих проблем класичної криптографії. Для розв’язування 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 спричинюватись до значних технічних складностей.

Довжина періоду гамми є найважливішою характеристикою генератора псевдовипадкових чисел. По завершенні періоду числа розпочнуть повторюватися – і їх можна буде завбачати. Необхідна довжина періоду гамми визначається мірою 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: в який спосіб можна вірогідно переконатися, що псевдовипадкова гамма конкретного генератора є насправді незавбачуваною? На сьогодні 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 обчислюванням остачі 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, які 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:

$$\sum_{j=0}^{k} h_j a_{i+j} = 0 \quad ; \qquad (2.1)$$

$$a_{i+k} = -\sum_{j=0}^{k-1} h_j a_{i+j} \quad ,$$

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 (2.1) визначає правило обчислювання 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 вигляду легко зреалізовуються на комп'ютері; при цьому реалізація виходить надтопростою, якщо всі h_i та a_i набувають значень 0 та 1 з поля $GF(2)$.

На рис. 2.15 подано лінійну послідовну перемикальну схему, яку може бути використано для обчислювання суми (2.1) і, отже, для обчислювання значення a_k за значеннями k попередніх членів послідовності. Вихідні величини a_0, a_1, a_2, ..., a_{k-1} вміщують в розряди регістру зсування, послідовні зсунення вмісту якого відповідають обчислюванню послідовних символів; при цьому вихід i-го зсунення дорівнює a_i. Даний пристрій називають генератором послідовності чисел, побудованим на базі регістру зсування з лінійним зворотним зв'язком.

Позначення:

– суматор за модулем 2

– ланцюг (відвід) з коефіцієнтом передавання h, $h = 0$ або 1

– запам'ятовувальна комірка, котра зберігає a, тобто на виході комірки $a = 0$ або $a = 1$

Рисунок 2.15 – Генератор з регістром зсування

Розв’язки лінійних рекурентних співвідношень, зреалізовувані генератором з регістром зсування, 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

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

у вигляді послідовності елементів a_0, a_1, a_i, …, 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 $a_0, a_1, a_2, \ldots$ обчислюються в порядку зростання номерів, то коефіцієнти багаточлена $a(X)$ обчислюються, розпочинаючи з коефіцієнтів зі степенями 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 з регістром зсування. Інакше кажучи, якщо в багаточлена $h(X)$ коефіцієнт $h_j = 1$, це означає, що відвід h_j у схемі генератора є наявний, якщо ж у багаточлена $h(X)$ коефіцієнт $h_j = 0$, то відвід h_j в схемі генератора є відсутній. У якості $h(X)$ слід обирати незвідний примітивний багаточлен. За такого обрання багаточлена $h(X)$ зі старшим степенем m генератор забезпечує видавання псевдовипадкової послідовності двійкових чисел з максимально можливим періодом $2^m - 1$.

Розглянемо за приклад трирозрядний регістр зсування з лінійним зворотним зв'язком (рис. 2.16), побудований відповідно до незвідного примітивного багаточлена

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

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

Трибітовий ключ

1	0	1
0	1	0
0	0	1
1	0	0
1	1	0
1	1	1
0	1	1

Рисунок 2.16 – Трирозрядний регістр зсування зі зворотними зв'язками

Нехай ключем є 101. Регістр розпочинає працювати з цього стану; послідовність станів регістру наведено на рис. 2.16. 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 регістру зсування (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) $Г_ш$ регістру зсування зі зворотним зв'язком є послідовність 1010011, котра циклічно повторюється. У цій послідовності є чотири одиниці й три нулі та 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 відрізнюється 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. Щоби відзнайти m бітів ключового потоку, m бітів відомого відкритого тексту складають за модулем два з відповідними m бітами шифртексту. Здобуті m бітів надають стан регістру зсування 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-тий момент часу. Тоді

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

де A – матриця розміром mm, котра визначає положення відводів регістру зі зворотним зв'язком.

Для трирозрядного регістру (див. рис. 2.16)

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

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 mm:

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

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

пов'язані співвідношенням

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

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 розумного значення m.

Для криптографії послідовності максимальної довжини MLSRS можна зробити більш криптостійкими, використовуючи нелінійну логіку. Зокрема, як ключовий потік використовується нелінійно "фільтрований" вміст регістру зсування, а для здобуття послідовності максимальної довжини – лінійний зворотний зв'язок, як це подано на рис. 2.17.

Рисунок 2.17 – Лінійний регістр зсування
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 регістру зсування відповідно до незвідного примітивного багаточлена $h(X)$ степеня 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 регістру зсування з лінійним зворотним зв'язком, її завжди можна здобути за допомогою регістру зсування 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.

3 СИМЕТРИЧНІ КРИПТОГРАФІЧНІ СИСТЕМИ

3.1 Класичні симетричні криптосистеми

Класична криптографія, зокрема теорія зв'язку в секретних системах, заснована К. Шенноном, виходила з того, що для шифрування й розшифровування інформації використовується один ключ і його передавання має здійснюватися надійним каналом обміну ключовою інформацією. Подібні алгоритми названо симетричними.

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

Різноманітні симетричні криптосистеми базуються на поданих нижче основних класах перетворювань.

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.

Одно- та багатоабеткові підстановки. Одноабеткові підстановки – це простий метод перетворювань, який містить правило заміни символів вихідного тексту на інші символи тої самої абетки. В разі одноабеткової підстановки (шифри простої заміни) кожний символ вихідного тексту замінюється на символ шифрованого тексту за одним законом перетворювання.

При шифруванні за допомогою щифрів багатоабеткової підстановки (шифрів складної заміни) закон перетворювання змінюється від символу до символу. Іноді один і той самий шифр може розглядатися і як одно- , і як багатоабетковий залежно від визначуваної абетки. Наприклад, шифр Плейфейра (підстановка біграм) з огляду на звичайну абетку є одноабетковим, а з огляду на абетку біграм – багатоабетковим.

Через певний час симетричні алгоритми було поділено на два великих класи – блочні й поточні.

Блочні шифри. Фактично блочний шифр – це система підстановки в абетці блоків (вона може бути як одно-, так і

як багатоабетковою, залежно від режиму блочного шифру). Застосовування блочних алгоритмів криптозахисту припускає поділ переданої до каналу зв'язку послідовності символів відкритого тексту на блоки фіксованої довжини з подальшим шифруванням кожного блока окремо. При цьому однаковим шифрувальним блокам відповідатимуть однакові шифртексти. На сьогодні блочні шифри є найбільш поширені. Приміром, вітчизняний та американський стандарти шифрування належать до блочних шифрів.

Поточні шифри. У поточних алгоритмах кожен символ відкритого тексту шифрується незалежно від інших і розшифровується в такий же спосіб. Інакше кажучи, перетворювання кожного символу відкритого тексту змінюється від одного символу до іншого.

При поточному шифруванні довжина ключової послідовності дорівнює довжині вихідного повідомлення. Її іноді називають гаммою. Стійкість поточних алгоритмів шифрування залежить від того, наскільки утворена гамма матиме властивість рівноймовірності появи її символів.

Поточні алгоритми мають високу швидкість шифрування, а їхня структура дозволяє здійснювати ефективну апаратну реалізацію, однак при програмному використовуванні виникають певні труднощі, які звужують область практичного застосовування таких алгоритмів.

Гаммування – це перетворювання вихідного тексту, за якого символи відкритого тексту складаються з символами псевдовипадкової послідовності (гаммою). Гаммування не можна цілковито виділити в окремий клас криптографічних перетворювань, позаяк ця псевдовипадкова послідовність може утворюватися, приміром, за допомогою блочного шифру. В разі, коли послідовність є насправді випадковою і її кожний фрагмент використовується лише одиноразово, то маємо криптосистему з одноразовим ключем.

Ще однією проблемою використовування алгоритмів, котрі припускають гаммування, є вимога щодо синхронності виконування операцій шифраторами на приймальному й передавальному боці.

3.2 Криптосистема Хілла

Лестером Хіллом було сформульовано алгебричний метод, котрий узагальнює афінну підстановку Цезаря

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

де a, b – цілі числа, 0 a, $b < m$; НСД (найбільший спільний дільник) (a, m) = 1 для визначання n-грам.

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 перетворюванням, описуваним квадратною матрицею, причому

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

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 (табл. 3.1).

Таблиця 3.1 – Відповідність поміж англійською абеткою та множиною цілих

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

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

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

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.

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.

Приміром, 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 дешифровано за допомогою M^{-1}.

Важливим моментом у цих обчислюваннях 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 постановою – "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 раніш, 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.

Алгоритм шифрування в криптосистемі Хілла

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

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

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}, помножений 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 віднайдено правильно.

4 Зведення оберненої матриці за модулем 26:

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

Нотатка. Число 135 – це результат пошуку числа, яке дає залишок 5 за модулем 26. При цьому виконується додаткова умова – віднайдене число повинно ділитися на 9 без залишку. Аналогічно здобуваються числа 153; 180; 81.

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. 3.1; C – вектор, компонентами якого є номери літер закритого повідомлення відповідно до табл. 3.1.

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. 3.1.

Вихідне повідомлення HELP визначає два вектори:

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

Зашифровування має вигляд:

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

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

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

З таблиці 3.1 дістаємо криптотекст HIAT.

Процес розшифровування йде за оберненим алгоритмом:

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

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

Здобута послідовність 7; 4; 11; 15 відповідно до таблиці 3.1 надає можливість відновити вихідний текст: HELP.

3.3 Сучасні симетричні криптосистеми

К. Шеннон в своїх роботах з теорії зв′язку дійшов висновків, що в практичних шифрах слід використовувати дві засади: розсіювання та перемішування.

Розсіювання являє собою розповсюдження впливу одного знаку відкритого тексту на безліч знаків шифртексту, що дозволяє приховувати статистичні властивості вихідного тексту.

Перемішування припускає використовування таких перетворювань, які ускладнюють відновляння взаємозв′язку статистичних

властивостей вихідного та шифрованого текстів.

Поширеним способом досягання ефектів розсіювання та перемішування є використовування складного шифру, тобто такого шифру, який може бути зреалізовувано у вигляді певної послідовності простих шифрів, причому кожний з них має вкласти власний внесок в сумарне розсіювання та перемішування.

У складних шифрах, які будуються на підставі простих шифрів, в основі криптографічних алгоритмів лежать математичні перетворювання, котрі дозволяють вимагати високої практичної стійкості. В криптографії існують лише два основних типи криптографічних перетворювань – заміна й перестановка символів. Всі інші алгоритми є лише комбінацією цих двох типів.

За багаторазового переміжненю простих перестановок та підставлянь, за допомогою доволі довгого секретного ключа, можна здійснити стійке шифрування з добрим розсіюванням та перемішуванням. Сучасні криптографічні системи, які наведено нижче, побудовано згідно із зазначеною методологією.

Сучасні криптографічні системи може бути зреалізовувано програмним, програмно-апаратним чи апаратним шляхом.

3.4 Стандарт шифрування DES

Стандарт шифрування даних DES (Data Encryption Standard) було опубліковано 1977 року Національним бюро стандартів США. Типовий блочний шифр, стандарт DES призначено для захисту від несанкціонованого доступу до важливої, але несекретної інформації в державних та комерційних організаціях США. Алгоритм, покладений у підґрунтя стандарту, 1980 року було схвалено Національним інститутом стандартів та технологій США (НІСТ). Алгоритм DES найчастіш застосовується в системах захисту комерційної інформації. На сьогодні розроблено програмне забезпечення та спеціалізовані ЕОМ, які зреалізовують шифрування інформації в мережах передавання даних.

Суть алгоритму зводиться до такого.

Передана до каналу зв'язку послідовність розбивається на блоки довжиною в 64 біти. Кожний з цих блоків шифрується незалежно від інших за допомогою 64-бітового ключа, в якому значущими є лише 56 біт (інші 8 біт – перевірні біти для контролю на парність).

Система DES використовує операції заміни перестановок символів та додавання за модулем 2.

Зручністю застосовуваного алгоритму є те, що операції зашифровування й розшифровування в DES є оберненими. Узагальнена схема процесу зашифровування в алгоритмі DES має вигляд рис. 3.1.

Рисунок 3.1– Узагальнена схема шифрування в алгоритмі DES

З файла вихідного тексту зчитується черговий 64-бітовий блок *M*. Процес його зашифровування полягає в початковій перестановці, шістнадцятьох циклах шифрування і, врешті, у завершувальній перестановці бітів.

Вхідна послідовність $M = m_1, m_2, \ldots, m_{64}$ перетворюється блоком початкових перестановок на послідовність IP (M) $= m_{58}, m_{50}, \ldots, m_7$, де m_i може набирати значень 0 чи 1. Перетворювання виконуються за фіксованою табл. 3.2.

Таблиця 3.2 – Початкова перестановка

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

За допомогою матриці початкової перестановки IP, яка містить 8 стовпців і 8 рядків, здійснюється перестановка символів вхідного блока.

Символи блока вписують до таблиці по стовпцях, розпочинаючи з лівої нижньої клітинки. Потім рядки змінюють місцями в порядку 2, 4, 6, 8, 1, 3, 5, 7. Далі символи, розташовані у клітинках таблиці, зчитуються по рядках.

Завершальне перетворювання алгоритму – обернена перестановка –здійснюється за допомогою матриці оберненої

перестановки IP $^{-1}$.

Символи блока вписують до таблиці по стовпцях, розпочинаючи з лівої нижньої клітинки. Потім стовпці змінюють місцями в порядку 5, 1, 6, 2, 7, 3, 8, 4. Далі символи, розташовані в клітинках таблиці 3.3, зчитуються по рядках.

Таблиця 3.3 – Завершальна перестановка

40	8	48	16	
39	7	47	15	
38	6	46	14	
37	5	45	13	
36	4	44	12	
35	3	43	11	
34	2	42	10	
33	1	41	9	

Алгоритм побудовано на базі мережі Фейстеля (див. рис. 2.12)

Процес шифрування здійснюється в такий спосіб.

Здобута після першої перестановки 64-бітова послідовність M розбивається навпіл на два 32-розрядних блоки L_0 та R_0 .

Потім виконується ітеративний процес шифрування, котрий складається з 16-ти кроків.

Нехай M_i – результат i -тої ітерації:

$$M_i = L_i R_i ,$$

де $L_i = m_1, m_2, \ldots, m_{32}$; $R_i = m_{33}, m_{34}, \ldots, m_{64}$... У цьому разі результат ітерації описується формулами:

$$L_i = R_{i-1}, \quad i = 1, 2, \ldots, 15; \; L_{16} = L_{15} \; f(R_{15}, K_{16});$$

$$R_i = L_{i-1} \; f(R_{i-1}, K_i), \; i = 1, 2, \ldots, 15; \; R_{16} = R_{15}.$$

Функція f називається функцією шифрування. Її аргументами є послідовність R_{i-1}, здобута на попередньому кроці шифрування, та 48-бітовий ключ шифрування K, що формується за певним правилом з 64-бітового ключа шифрування K.

Усі перетворювання, виконувані в межах алгоритму DES, ілюструє схема подана на рис. 3.2.

Значення L_0 та R_0 здобувають звичайною розбивкою блока M, який було піддано початковій перестановці, навпіл. Далі блок L_1 визначають, за правилом $L_1 = R_0$. Задля одержання значення R_1, треба обчислити значення функції

$f(R_0, K_1)$. Ця операція здійснюється у відповідності з алгоритмом, поданим на рис. 3.3.

Рисунок 3.2 – Схема алгоритму DES

R_{i-1} 32 біти

K_i, 48 біт

$f(R_{i-1}, K_i)$, 32 біти

Рисунок 3.3 – Схема обчислювання функції шифрування $f(R_{i-1}, K_i)$

На початку 32-бітовий блок розширюється до 48-ми символів. При цьому додаткових 16 символів беруться, за певним правилом, з розширюваного блока згідно з табл. 3.4.

Таблиця 3.4 – Функція розширювання E

32	1	2
4	5	6
8	9	10
12	13	14
16	17	18
20	21	22

24	25	26
28	29	30

Потім до здобутого 48-розрядного блока додають за модулем два символи першого 48-розрядного ключа K_1. На наступному етапі здобута 48-розрядна послідовність розбивається на 8 груп по 6 символів. Кожна 6-символьна група вихідної послідовності B_j перетвориться на 4-символьну групу відповідно до шифрувальної таблиці 3.5. Після цього здобуті в такий спосіб вісім 4-символьних груп складатимуть 32-бітовий блок, який піддають черговій табличній перестановці (табл. 3.6).

Кожна з функцій $S_j(B_j)$ перетворює 6-бітову послідовність на 4-бітову за таким алгоритмом:

– перший та останній біти вихідної послідовності B_j ($B_j = b_1\, b_2\, b_3\, b_4\, b_5\, b_6$, де $b_j = 0$ чи 1) визначають номер рядка k. Тобто число $b_1 b_6$, яке переведено з двійкової системи обчислювання до десяткової, – це номер рядка в таблиці 3.5;

– другий, третій, четвертий та п’ятий біти послідовності B_j визначають номер стовпчика l. Тобто число $b_2\, b_3\, b_4\, b_5$, яке переведено з двійкової системи обчислювання до десяткової, – це номер стовпця в таблиці 3.5;

– результат перетворювання обирається на перетинанні рядка k та стовпця l.

П р и к л а д. Нехай $B = 011011$. Тоді $S(1)(B) = 0101$.

Дійсно, $k = 1$ ($b_1 b_6 = 01_B = 1_D$);

$l = 13$ ($b_2\, b_3\, b_4\, b_5 = 1101_B = 13_D$).

На перетинанні стовпця 13 та рядка 1 задано число $5_D = 0101_B$. Отже, послідовність 011011 перетворена на послідовність 0101.

Функція перестановки бітів P задається таблицею 3.6.

Таблиця 3.5 – Функційні перетворювання S_j

Рядки	**Стовпці**															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
S_1																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	4	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15

3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	15	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
0	2	12	14	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Таблиця 3.6 – Функція перестановки *P*

16	7	20	21
29	12	28	17

1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

На кожному кроці ітерації для функційного перетворювання використовується нове значення ключа K_i.

Нове значення ключа K_i обчислюється з його початкового значення. Ключ являє собою 64-бітовий блок з вісьмома бітами контролю за парністю, розташованих у позиціях 8, 16, 24, 32, 40, 48, 56, 64.

Задля вилучання контрольних бітів та підготовки ключа до роботи використовується функція первинної підготовки ключа *G* (табл. 3.7).

Таблиця 3.7 – Функція первинного встановляння ключа

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Результат перетворювання $G(K)$ розбивається на дві частини – C_0 та D_0 по 28 біт кожна. Перші чотири рядки матриці визначають біти послідовності C_0 (символи ключа зчитуються по рядках). Наступні чотири рядки матриці визначають біти послідовності D_0. Після визначення C_0 та D_0 рекурсивно визначаються значення C_i та D_i. З цією метою виконуються операції циклічного зсування ліворуч на кількість кроків, обумовлені таблицею 3.8

Таблиця 3.8 – Циклічні зсування

Номер ітерації	Кількість зрушень ліворуч	Номер ітерації	Кількість зрушень ліворуч
1	1	9	1
2	1	10	2
3	2	11	2
4	2	12	2
5	2	13	2
6	2	14	2
7	2	15	2
8	2	16	1

Операції зсування виконуються незалежно для послідовностей C_i та D_i. Ключ K_i, обумовлений на кожнім кроці ітерації, є результат вибору конкретних 48-ми бітів з 56-бітової послідовності та їхньої перестановки (рис. 3.4).

K_1

K_2

K_{16}

Рисунок 3.4 – Схема алгоритму обчислювання ключів K_i

Порядок вибору визначається функцією H:

$$K_i = H\,(\,C_i D_i\,).$$

Функція H визначається матрицею, яка завершує формування ключа за таблицею 3.9.

Символи послідовностей C_i та D_i. вписуються до матриці H відповідно до номерів її клітинок і потім зчитуються по рядках. Отже, виконується перестановка символів.

Усі перестановки й коди в таблицях добрано розроблювачами в такий спосіб, щоби максимально утруднити процес розшифровування шляхом підбирання ключа.

Таблиця 3.9 — Функція H

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8

16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Операції, виконувані в перебігу шифрування з використовуванням алгоритму DES, є обернені. Процедура розшифровування на боці приймача відрізнюється лише черговістю формування ключів K_i. Вони повинні подаватися у зворотному порядку – K_{16} ... K_1.

Початково стандарт DES використовувався лише для шифрування та розшифровування даних ЕОМ. Потім він став використовуватися для інших завдань, приміром задля автентифікації чи захисту повідомлень електронної системи платежів при операціях поміж клієнтами та банками. Щоби можна було використовувати алгоритм DES для розв'язування різноманітних криптографічних завдань, розроблено кілька режимів його використовування.

3.4.1 Режим „Електронна кодова книга"

Режим „Електронна кодова книга" ECB (Electronic Code Book) передбачає реалізацію криптографічних перетворювань у відповідності з головним алгоритмом DES. Кожний 64-розрядний блок перетворюють з використовуванням одного й того самого ключа (рис. 3.5).

Передавання

Приймання

Рисунок 3.5 – Режим електронної кодової книги

Головною перевагою такого алгоритму є простота зреалізовування. Однак він є найменш тривалий щодо спроб розшифровування. Це пояснюється тим, що за відносно невеликої довжини блока та великої довжини передаваного тексту певні блоки можуть повторюватися. Це надає криптоаналітикові певну інформацію щодо змісту повідомлення.

3.4.2 Режим „Зчеплювання блоків шифру”

Режим „Зчеплювання блоків шифру” CBC (Cipherblock Chaining) передбачає розбиття повідомлення, що передається, на блоки

$$M = M_1 M_2 M_3 \ldots$$

До першого блока додається за модулем два первинний вектор S, який регулярно змінюється на приймальному й передавальному боці. Після цього здобута сума шифрується з використовуванням алгоритму DES. Отже, в канал передається 64-бітове повідомлення C_1.

Здобута на боці приймача сума C_1 розшифровується, потім від неї віднімається первинний вектор S.

На наступному етапі шифрування, при передаванні наступного блока, замість первинного вектора S до зашифрованого повідомлення додається передаване повідомлення C_1. Ця процедура повторюється за передавання кожного наступного 64-розрядного блока (рис. 3.6).

Отже, останній блок шифртексту буде функцією секретного ключа, первинного вектора і кожного біта відкритого тексту, незалежно від його довжини. Цей блок називають кодом автентифікації повідомлення (КАП).

КАП можна легко здобути на боці приймача шляхом повторювання процедур, які виконуються на боці передавача.

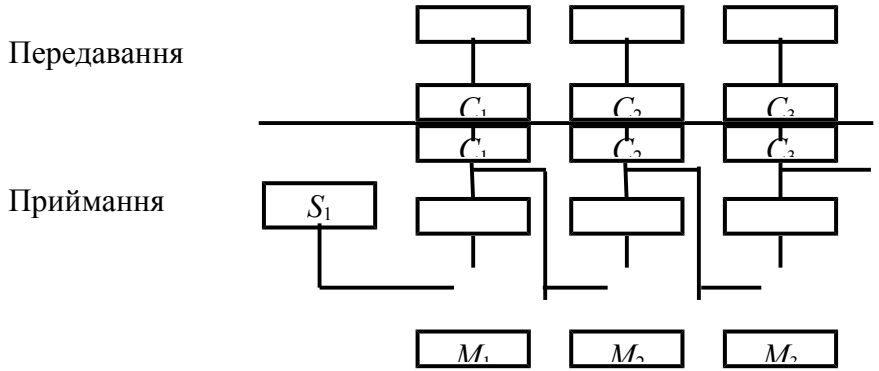


Рисунок. 3.6 – Режим "Зчеплювання блоків шифру"

3.4.3 Режим „Зворотний зв'язок за шифром"

Режим „Зворотний зв'язок за шифром" CFB (Cipher Feedback)припускає, щоби довжина блока відрізнювалась від 64 біт. Припустімо, що довжина блоків, на які розбивається зашифровувана послідовність, становить менше за 64 біти (рис. 3.7).

Зсування Зсування

Вх.бл. Вх. бл.

1 k 1 k

Вих.бл. Вих. бл.

Зашифровування Розшифровування

Рисунок 3.7 – Схема алгоритму в режимі зворотного зв’язку за шифром

До вхідного блока вписується вектор ініціалізації. Потім його вміст шифрується за допомогою алгоритму DES.

Припустімо, що внаслідок розбивання на блоки здобуто n блоків довжиною k біт кожний (залишок дописується нулями).Тоді для кожного $i = 1 \ldots n$ блок шифр тексту є

$$C_i = M_i \ P_{i-1},$$

де $P_{i-1} - k$ старших бітів попереднього зашифровуваного блока.

Оновлювання регістру здійснюється на ланцюзі зворотного зв’язку шляхом вилучання його k старших бітів та запису C_i до регістру.

Відновлювання прийнятого повідомлення здійснюється виконанням перелічених операцій у зворотному порядку:

$M_i = C_i \ P_{i-1}$.

3.4.4 Режим „Зворотний зв’язок за виходом”

Режим „Зворотний зв’язок за виходом” OFB (Output Feedback), аналогічно до розглянутого CFB, припускає, щоби довжина блока відрізнювалась від 64 біт. Різниця даного методу полягає в організації зворотного зв’язку. Оновлювання вмісту вхідного блока здійснюється не змістом шифртексту, передаваного до каналу зв’язку, а змістом зашифрованого вектора ініціалізіції на першому і наступних кроках шифрування блоків.

Нехай

$$M = M_1 M_2, \ \ldots, \ M_n.$$

Для усіх $i = 1, \ldots, n$