Лабораторна робота №8
ШИФРУВАННЯ ІНФОРМАЦІЇ

Мета роботи: навчитися складати програми для шифрування інформації методами перестановки та заміни.

Теоретичні відомості

Перші протоколи та мережі зв'язку були спроектовані таким чином, щоб забезпечити можливість передавання інформації між кінцевими вузлами. Це дозволило вирішити основну задачу телекомунікацій — надання зв'язку. Завдяки поступовому розвитку протоколів та збільшенню швидкостей передавання, актуальність використання мереж зв'язку в процесі обміну інформацією між людьми є більшою, ніж при використанні звичайних засобів зв'язку. Прикладом такої мережі є глобальна мережа Інтернет, яка в даний час забезпечує передавання найбільшого обсягу інформації. Оскільки інформація, яка передається у мережах спільного використання (мережі Інтернет), є загальнодоступною - виникає можливість її перехоплення.

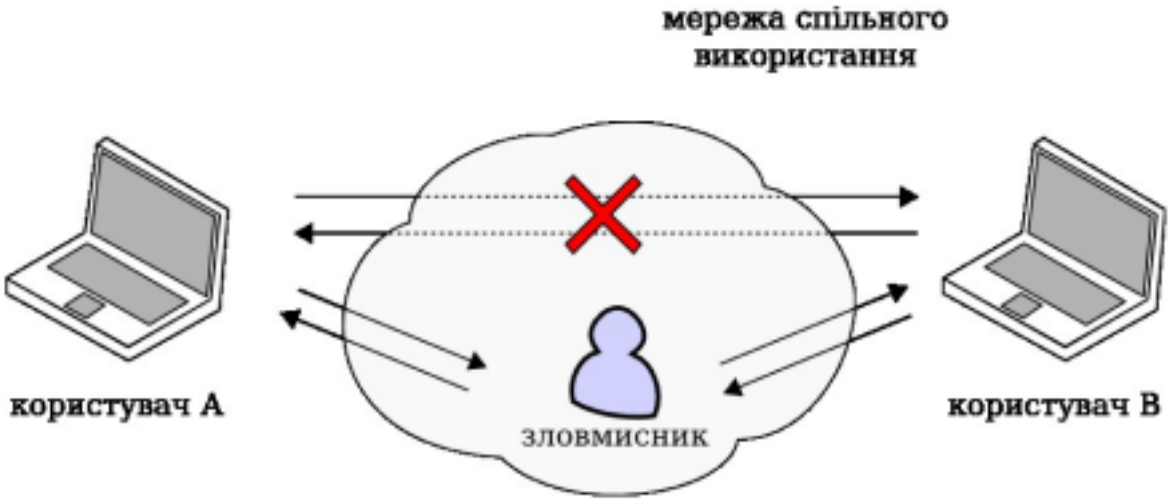

Рис. 8.1. Схема перехоплення інформації “man in the middle”

Актуальність проблеми захисту інформації виникала ще задовго до появи мереж зв'язку та протоколів передавання інформації. Ця проблема зумовила необхідність застосування спеціальних заходів щодо захисту інформації від несанкційованого доступу. В сучасних мережах захист інформації

забезпечується двома способами - обмеженням доступу до неї певних осіб чи шифруванням. В першому випадку мережа зв'язку проектується таким чином, щоб обмежити доступ до її ресурсів стороннім особам і надати лише авторизованим користувачам. Цей спосіб пов'язаний з аспектом фізичної реалізації мережі, оскільки зловмисник не має доступу до каналів передавання інформації. Другий спосіб базується на зміні способу представлення інформації таким чином, щоб його можна було відновити лише знаючи алгоритм (метод шифрування), або маючи таємні відомості (ключ) цієї зміни.

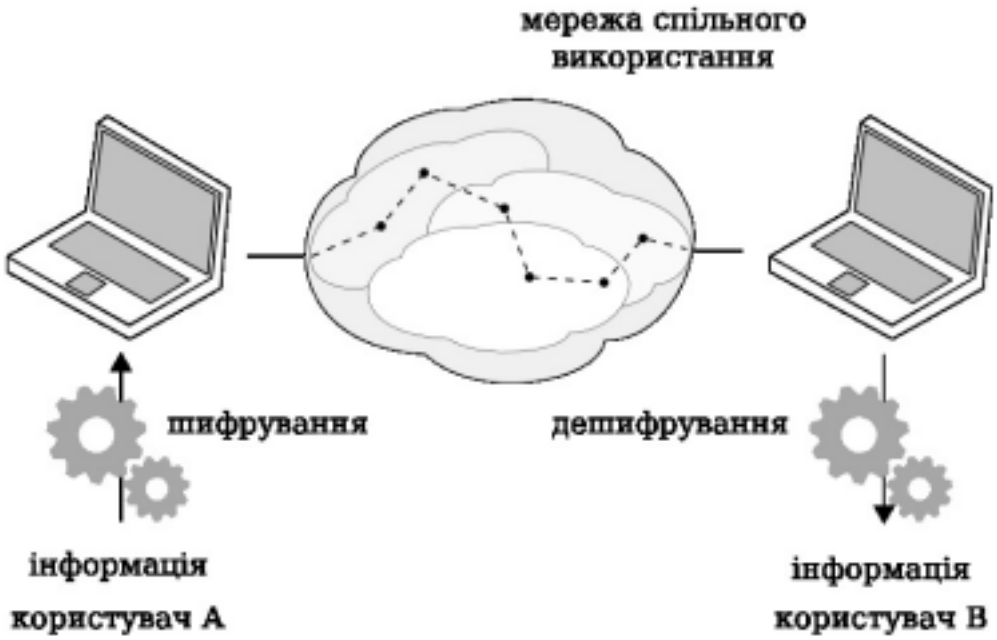

Рис. 8.2. Схема використання шифрування інформації в мережах зв'язку

Якщо зловмисник отримає доступ до каналів передавання інформації слід вважати, що інформація вже перехоплена. Проте, внаслідок попереднього шифрування інформації він не зможе її розпізнати та скористатися нею.

Наука яка займається створенням та дослідженням шифрів називається криптографією. Шифром називається алгоритм перетворення інформації із одного виду в інший, а шифруванням — процес цього перетворення. Ключем шифрування є інформація, яка використовується в процесі шифрування та дешифрування повідомлень. Система криптографічного захисту формується на основі шифру з використанням пристрою шифрування та дешифрування. На відміну від перших криптографічних систем, захист інформації в сучасних відбувається на основі ключа, а не алгоритму. Використання ключа в якості основи для захисту інформації зумовлено тим, що для знаходження

правильного ключа необхідно затратити набагато більше ресурсів, ніж для встановлення алгоритму шифрування.

Застосування науки криптографії в сучасних мережах забезпечує вирішення ряду задач пов'язаних із проблемою захисту інформації:
• забезпечення конфіденційності передавання інформації каналами зв'язку шляхом її шифрування; процес шифрування інформації здійснюється програмним, або апаратним забезпеченням мережевих пристроїв;
• здійснення аутентифікації - надання доступу до ресурсів мережі особам які пройшли етап перевірки з використанням паролю; процес аутентифікації використовується не тільки для отримання доступу в мережах, а і на локальних комп'ютерах з використанням одного із сучасних методів шифрування, наприклад MD5, SHA256.
• створення електронного підпису (файл зашифрований певним чином) для однозначної ідентифікації об'єкта; механізм електронного підпису використовується для ідентифікації особи, web-сайту, тощо.

В теорії криптографічного захисту інформації інформації відомо багато шифрів. Більша частина із них була розроблена для шифруванням інформації в символьній, або алфавітній формі. З розвитком цифрових технологій шифрування почали здійснювати для інформації представленій у двійковій формі.

Прикладами простих шифрів є шифри перестановки та заміни. Вони використовуються для шифрування відкритого тексту у зашифровані повідомлення. Сучасні шифри забезпечують перетворення інформації в цифровій формі і характеризуються довжиною ключа, яка може складати від 56 (DES) до 256 (AES) біт.

Примітивні алгоритми шифрування

Шифр перестановки

Процес шифрування інформації при використанні шифру перестановки полягає у зсуві символів інформаційного повідомлення в алфавіті на кількість позицій, яка визначається заданим ключем. Зашифроване повідомлення буде складатися із тієї ж кількості символів що і інформаційне, але замінених на нові.

Рис. 8.3. Відповідність між символами початкового алфавіту та символами алфавіту зсунутого на N позицій

Взаємний зв'язок між символами встановлюється за допомогою ключа, який визначає кількість позицій в алфавіті на яку необхідно їх зсунути для отримання початкового повідомлення. Оскільки ключем в шифрі перестановки є циклічний зсув позицій символів алфавіту, криптостійкість цього шифру визначається розміром алфавіту.

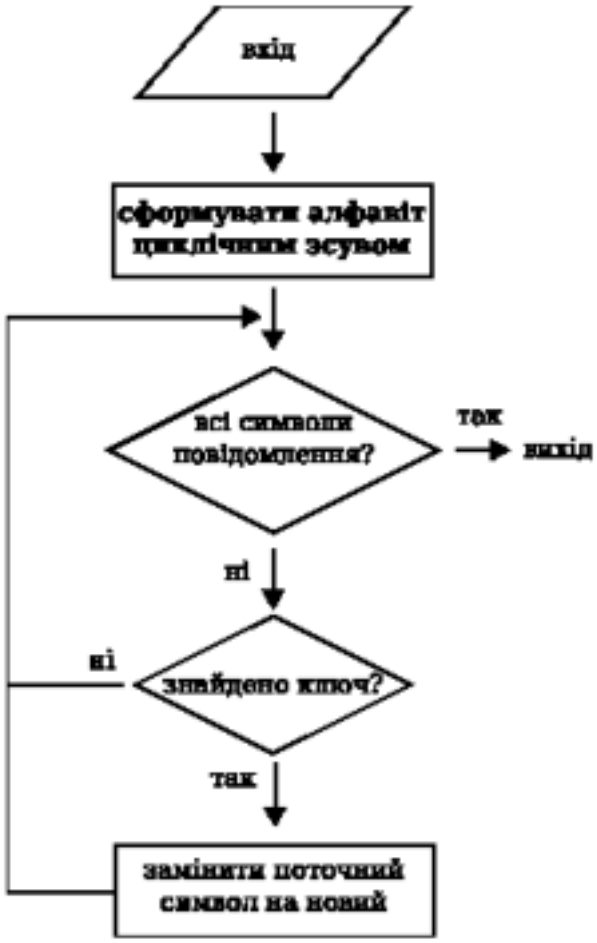

Рис. 8.4. Блок-схема шифрування інформації з використанням перестановки

Приклад шифрування повідомлення ABC шифром перестановки:
етап 01: визначимо значення ключа

N = 9

етап 02: сформуємо алфавіт для шифрування шляхом циклічного зсуву символів початкового алфавіту вліво; отримали такий алфавіт

KLMNOPQRSTUVWXYABCDEFGHIJ

етап 03: замінюємо символи повідомлення символами алфавіту отриманого на попередньому етапі в тих самих позиціях; наприклад A – K, B – L, C – M

ABCDEFGHIJKLMNOPQRSTUVWXY
| | | | | | | | | | | | | | | | | | | | | | | | |
KLMNOPQRSTUVWXYABCDEFGHIJ

етап 04: після операцій заміни зашифроване повідомлення (ABC) має вигляд:

KLM

Основними недоліками шифру перестановки є мала кількість ключів, яка при використанні стандартного алфавіту латинських символів складає лише 26 штук і можливість застосування методу частотного аналізу для отримання початкового повідомлення.

Шифр заміни

Для усунення недоліку шифру перестановки — недостатньої кількості ключів було розроблено шифр заміни. Процес шифрування інформації з використанням шифру заміни є подібним до шифру перестановки. В якості початкового алфавіту тут використовується не впорядкована послідовність циклічно зсунутих символів, а **попередньо змінена!**

A B C D E F G H I J ...
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
M P K N L R U S T O ...

Рис. 8.5. Відповідність між символами початкового алфавіту та символами алфавіту отриманого шляхом перестановки з використанням деякого закону

Закон перестановки символів початкового алфавіту і є ключем шифрування. Для визначення ключа шифру необхідно записати початковий та відповідний йому алфавіт символів із зміненими позиціями. Шифрування полягає у заміні символів початкового повідомлення на символи утвореного

алфавіту який і є ключем. Для дешифрування необхідно виконати зворотню операцію.

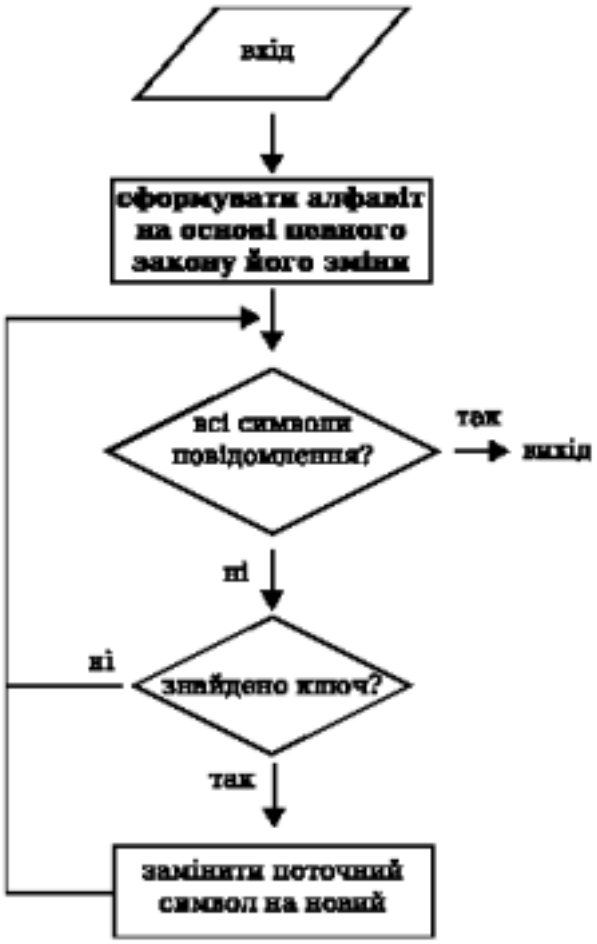

Рис. 8.6. Блок-схема шифрування інформації з використанням заміни

Приклад шифрування повідомлення ABC шифром перестановки:
етап 01: визначимо ключ шифрування (певний закон перестановки)
етап 02: сформуємо алфавіт для шифрування використовуючи ключ;

BADCFEHGJILKNMPORQTSVUXWZY

етап 03: замінюємо символи повідомлення символами алфавіту отриманого на попередньому етапі в тих самих позиціях; наприклад A – B, B – A, C – D

ABCDEFGHIJKLMNOPQRSTUVWXY
| | | | | | | | | | | | | | | | | | | | | | | | | |
BADCFEHGJILKNMPORQTSVUXWZY

етап 04: після операцій заміни зашифроване повідомлення (ABC) має вигляд:

BAD

Порядок роботи

1. Запустити середовище розробки програм на мові C/C++ (BorlandC, GCC, MinGW, Dev-C++, Visual Studio, тощо).
2. Вибрати із залікової книжки дві останні цифри **m** (передостання) та **n** (остання).
3. Вибрати згідно варіанту (табл. 8.1) текстове повідомлення.
4. Скласти програму для шифрування текстового повідомлення з використанням шифрів перестановки та заміни.
5. Порівняти отримані результати.

Таблиця 8.1

Варіанти завдань

Варіант mod(mn, 20)	Текстове повідомлення
0	“Telecommunication device”
1	“Packet of information”
2	“Network flow diagram”
3	“Communication protocol”
4	“Protocol data unit”
5	“Open shortest path first”
6	“Routing information protocol”
7	“Cyclic redundancy check”
8	“Information database”
9	“Telecommunication unit”
10	“Database structure”
11	“Border gateway protocol”
12	“Communication device A”
13	“Short circuit problem”
14	“Transmission protocol”
15	“Multiple in multiple out”
16	“Universal asynchronous receiver”
17	“Wireless fidelity”
18	“Code data multiple access”
19	“Long term evolution”

Контрольні запитання

1. Що таке шифрування?
2. Для чого використовується шифрування?
3. Які типи шифрів існують?
4. Що таке криптографія?
5. Чим характеризується шифр?
6. В чому полягає надійність шифру?
7. Що таке ключ?
8. Для чого використовується ключ?
9. Як здійснюється шифрування перестановкою?
10. Як здійснюється шифрування заміною?

Зміст звіту

1. Титульний лист
2. Тема та мета роботи
3. Короткі теоретичні відомості
4. **Результати виконаної роботи**
5. **Висновок**

ЛІТЕРАТУРА

1. Бабаш А.В., Шанкин Г.П. Криптография - М.: Солон-пресс, 2007. - 512 с.
2. Березин Б.И., Березин С.Б. Программирование на С и С++ - М.: ДИАЛОГ-МИФИ, 2001. - 288 с.
3. Керниган Б., Ритчи Д.. Язык программирования С, 2-е издание - М.: Вильямс — 2009. - 292 с.
4. Лафоре Л. Объектно-ориентирование программирование в С++, 4-е издание — М.: Питер, 2004. - 923 с.
5. Левитин А.В. Алгоритмы: введение в разработку и анализ — М.: Издательский дом “Вильямс”, 2006.
6. Папас К., Мюррей У. Программирование на С и С++ - К.: Издательская група BHV, 2000. - 320 с.
7. Смарт Н. Криптография - М.: Техносфера, 2005. - 528 с.
8. Шилдт Г. Справочник программиста С/С++, 3-е изд.: Пер. с англ. - М. Издательский дом “Вильямс”, 2003. - 432 с.