Лабораторна робота №9

Шифрувальна система на основі шифру простої заміни.

Мета:

Створити криптографічну систему на основі шифру простої заміни та дослідити її роботу.

Обладнання:

- персональний комп'ютер з встановленою операційною системою Windows
- будь-яка мова програмування.

Завдання:

1. Створити криптографічну систему на основі шифру простої заміни.
2. Перевірити її роботу.

Література:

1. М.Масленников. Практическая криптография. БХВ-Петербург,2003. – 464с.
2. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. 1996.
3. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. М."ДМК", 2004. – 616 с.

Теоретичні відомості.

Під *криптографією* будемо розуміти область знань, що відноситься до методів і засобів перетворення повідомлень у незрозумілу для сторонніх осіб форму, а також перевірки істинності цих повідомлень.

Під *криптоаналітикою* будемо розуміти засоби і методи, спрямовані на подолання криптографічного захисту.

Сукупність криптографії та криптоаналітики називається *криптологією*.

Розшифровуванням будемо називати відновлення вихідного повідомлення при відомому ключі шифрування.

Дешифруванням будемо називати процес відновлення вихідного повідомлення при невідомому ключі шифрування.

Таким чином, ті, кому призначено шифроване повідомлення його *розшифровують*, а ті, хто перехоплює його, намагаються *дешифрувати*.

Розглянемо невеликий приклад. Припустимо, що відкрите повідомлення складається з символів алфавіту і пробілу. Нехай у нас є таблиця 1, що задає відповідність між символами і числами від 0 до 32.

Таблиця 1. Таблиця заміни при шифруванні.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я				
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32			

Шифрування методом простої заміни полягає у даному випадку в тому, що кожна літера повідомлення замінюється числом згідно з таблицею 1. Звичайно, найкращим є той варіант, коли набір чисел у таблиці генерується випадково і служить ключем для розшифровування повідомлення. У нашому простому прикладі повідомлення „МОЯ ПЕРВАЯ ШИФРОГРАММА" буде у зашифрованому на табл.1 вигляді мати вигляд: „12 14 31 32 15 05 16 02 00 31 32 24 08 20 16 14 03 16 00 12 12 00".

Для розшифровування повідомлення необхідно провести обернену заміну згідно з табл. 1. В цьому випадку другий рядок табл. 1 виступає в якості ключа, який використовується як для шифрування, так і для розшифровування повідомлення.

Системи шифрування, яка використовує один і той же ключ для шифрування і розшифровування повідомлень, називається *симетричною*. Якщо повідомлення шифрують за допомогою одного ключа, а розшифровують за допомогою іншого, така система носить назву *асиметричної*.

Дуже часто використовують кілька алгоритмів шифрування, наприклад, зсув на певну кількість знаків алфавіту, а потім застосування простої заміни за допомогою табл.1. Таке невелике ускладнення шифрування може призвести до значного ускладнення при його дешифровці, чого, в принципі, і прагнуть досягти при застосуванні криптографічних систем.

Практична частина.

1. Підгрупа розбивається на пари за бажанням.
2. Один з членів пари модифікує програму ЛР№1 так, щоби вона спочатку використовувала алгоритм Цезаря, так як у ЛР№1, а потім, при другому проході, виконувала просту заміну згідно з генерованою таблицею заміни типу табл. 1.
3. Система шифрування повинна задовольняти таким вимогам: а) читати відкритий текст повідомлення з текстового файлу; б) запитувати величину і напрям зсуву; в) генерувати таблицю простої заміни за допомогою генератора випадкових чисел; в) записувати зашифроване повідомлення, величину зсуву і таблицю заміни у текстовий файл для передачі.
4. Система розшифрування повинна задовольняти таким вимогам: а) читати з текстового файла зашифроване повідомлення разом з таблицею заміни і величиною зсуву; б) виводити розшифроване повідомлення у текстовий файл і на екран монітора.
5. Протокол дій та отримані результати включіть у звіт з лабораторної роботи.

Контрольні запитання.

1. Що називається криптографією? Для чого вона використовується?
2. Що називається криптоаналізом? Для чого він використовується?
3. Що називається криптологією?
4. Яка різниця між розшифровкою і дешифровкою?
5. Охарактеризуйте шифр простої заміни. Які його переваги і недоліки?
6. Які Ви знаєте типи шифрів? Наведіть приклади.
7. Які системи шифрування називаються симетричними?
8. Які системи шифрування називаються асиметричними?
9. Як можна, на Вашу думку, модифікувати дану систему шифрування?