Лабораторна робота №3

Шифрувальна система на основі шифру гаммування.

Мета:

Створити криптографічну систему на основі шифру гаммування 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 гаммування.
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.

Нехай у нас є відкрите повідомлення $t_1,\ldots,t_n$, що являє собою послідовність символів з табл.1.

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				

Ключ K являє собою послідовність чисел $k_1,\ldots,k_n$ з множини $\mathbf{M}=\{0,\ldots,32\}$. Зашифрований текст $s_1,\ldots,s_n$ обчислюється за наступною формулою:

$$s_i=(C(t_i)+k_i) \bmod 33, \qquad i=1,\ldots,n, \qquad (1)$$

де С – функція, що перетворює символ у його порядковий номер. Запис $d=(a+b) \bmod m$ означає, що d співпадає із залишком від ділення на m суми чисел $a+b$, наприклад, $1=(4+7) \bmod 10$.

Розшифрувати повідомлення можна за допомогою формули:

$$t_i= C^{-1}(s_i+(33-k_i)) \bmod 33.$$

У даному випадку через C^{-1} позначають функцію, яка виконує обернене перетворення: перетворює порядковий номер з множини 0-32 у символ алфавіту.

Будемо вважати, що елементи ключа k_i вибираються рівноймовірно і незалежно з множини М.

Визначений таким чином шифр називається *шифром гаммування з випадковою рівноймовірною гаммою* (*гаммою* прийнято називати послідовність чисел $k_1,\ldots,k_n$, що додається за модулем до шифрованого повідомлення).

При такому методі шифрування довжина шифрограми співпадає з довжиною відкритого повідомлення. Це полегшує криптоаналітикам задачу дешифрування повідомлення за частотним словником. Щоби сховати довжину повідомлення, його можна доповнити пробілами до певної фіксованої довжини, яку не перевищує стандартне повідомлення.

Розглянемо приклад використання спрощеного шифру гаммування. Спрощення полягають у наступному: 1) замість алфавіту з 33 літер перейдемо до 32, замінивши пробіл літерою „Ф", що сама по собі дуже рідко використовується; 2) випадкову гамму замінимо псевдовипадковою, яка ґрунтується на простому ключі, що складається з трьох випадкових чисел.

Нехай ключ $K=(Y_1;Y_2;Y_3)$ складається з трьох чисел, які вибрано випадковим чином незалежно і рівноймовірно з множини (0,...,31). За допомогою рекурентного співвідношення $Y_t=(Y_{t-1}+Y_{t-3}) \bmod 32$ формується послідовність $Y_1,...,Y_{n+1}$ для $t>3$. Далі, за формулою

$$Z_t=(Y_t+Y_{t+1}) \bmod 32, \qquad t=1,\ldots,n \tag{2}$$

обчислюється псевдовипадкова послідовність $Z_1,...,Z_n$, що використовується в якості випадкової гамми. Саме шифрування полягає у додаванні за модулем 32 елементів гамми з порядковими номерами літер у таблиці 1.

Зашифруємо на ключі $K=(04,31,15)$ повідомлення „ПРИКАЗЫВАЮФНАСТУПАТЬ".

Послідовність $Y_1,...,Y_{n+1}$ у даному випадку буде мати вигляд: „04 31 15 19 18 01 20 06 07 27 01 08 03 04 12 15 19 31 14 01 00".

Додамо за модулем 32 порядкові номери символів нашого повідомлення з елементами псевдовипадкової послідовності (гамми), отриманої за формулою (2):

15 16 08 10 00 07 27 02 00 30 20 13 00 17 18 19 15 00 18 28 – повідомлення
03 04 02 05 19 21 26 13 02 28 09 11 07 16 27 02 18 13 15 01 – гамма
18 30 10 15 19 28 21 15 02 26 29 24 07 01 13 21 01 13 01 29 – шифрограма.

Розшифрувати повідомлення можна за допомогою формули:

$$t_i= C^{-1}((s_i+(32-k_i)) \bmod 32, \tag{3}$$

якщо згенерувати гамму за відомим секретним ключем K.

Тепер розглянемо метод дешифрування нашого повідомлення. Загальна кількість текстів з 20 літер складається 32^{20}, а кількість різних ключів у даному випадку $32^3=32768$. Таким чином, кількість можливих варіантів дешифрування при невідомому ключі не перевищує 32768. Маючи перехоплену шифрограму, методом „грубої сили" (тобто прямого перебору всіх ключів) нам знадобиться не більше 32768 варіантів для дешифрування повідомлення. Зрозуміло, що під час роботи будуть зустрічатися абсолютно „нечитабельні", а всі логічні повідомлення необхідно відфільтрувати за допомогою простої логіки (тобто, може бути таке повідомлення, чи ні). Згідно з дослідженнями К.Шеннона, кількість змістовних текстів з 20 літер в англійській мові приблизно 10^6. Приблизно така ж оцінка справедлива і для російської мови. Імовірність появи серед всіх варіантів дешифровок іншого змістовного тексту менша $2.6\text{x}10^{-20}$. Для порівняння, відгадати 6 чисел з 36 більша за 10^{-10}. Якщо криптоаналітик буде відкидати по одному невірному повідомленню за секунду, то йому потрібно буде на те, щоби продивитися всі повідомлення приблизно 9 годин. Таким чином, трудовитрати ручного дешифрування даного повідомлення методом прямого перебору ключів складає 555

годин. Процес можна прискорити, якщо застосувати ЕОМ. У цьому випадку результати генерування всіх ключів та дешифрування всіх варіантів буде отримано практично миттєво, і лише 9 годин знадобиться криптоаналітику для відбору істинного повідомлення серед хибних.

У сучасних алгоритмах шифрування використовують ключі набагато більшої довжини, ніж у даному прикладі. Зокрема, у широко відомому алгоритмі DES ключ має об'єм 56 біт. З таким ключем на метод „грубої сили" знадобиться 2 млрд. років при швидкості один варіант за секунду. Варіант „грубої сили" можна значно прискорити, якщо врахувати неможливі сполучення літер мови.

Якщо ми маємо частину зашифрованого повідомлення, наприклад, знаємо, що воно починається з літер „ПРИ". У алгоритмі заміни номер П=15, Р=16, И=08. Це означає, що виконуються співвідношення: $(15+ Z_1) \bmod 32 = 18$; $(16+ Z_2) \bmod 32 = 30$ і $(8+ Z_3) \bmod 32 = 10$. Звідси можна знайти перших три знаки гамми: 3; 14; 2. Тепер можна скласти систему з таких трьох рівнянь:

$$(Y_1+Y_2) \bmod 32 = 3;\ (Y_2+Y_3) \bmod 32 = 14;\ (Y_3+Y_4) \bmod 32=2,$$

розв'язуючи яку, ми отримаємо секретний ключ: $Y_1=4$; $Y_2=31$; $Y_3=15$. Як бачимо, секретний ключ ми отримали дуже легко, розв'язавши усього систему з трьох рівнянь з трьома невідомими.

Таким чином, ми можемо розділити криптографічні алгоритми на три великих групи.

До першої групи відносяться досконалі алгоритми, які не піддаються розкриттю при правильному використанні (наприклад, алгоритм одноразових блокнотів, або шифр гаммування випадковою рівноймовірною гаммою).

Другу групу формують шифри, що допускають неоднозначне дешифрування. Наприклад, така ситуація виникає, коли шифрують за допомогою простої заміни коротке повідомлення.

До третьої групи належать шифри, криптограми яких можуть бути однозначно розшифровані, однак складність дешифрування забезпечується трудомісткістю алгоритму дешифрування. Тобто в останньому випадку стійкість шифру забезпечується складністю алгоритмів дешифрування.

Практична частина.

1. Створіть просту криптографічну систему, яка використовує шифр гаммування, описаний у теоретичній частині.
2. Система шифрування повинна задовольняти наступним вимогам: 1) читати відкрите повідомлення з текстового файлу і застосовувати просту заміну за допомогою табл. 1; 2) запитувати сеансовий секретний ключ, що складається з 3 чисел; 3) генерувати гамму за формулою (2), довжина якої дорівнює довжині відкритого повідомлення; 4) шифрувати за допомогою формули (1) відкрите повідомлення і записувати його у файл.
3. Система розшифровування повинна задовольняти таким вимогам: 1) читати шифрограму з текстового файлу; 2) запитувати сеансовий секретний ключ; 3) генерувати гамму на основі ключа; 4) розшифровувати шифрограму за допомогою формули (3) і виводити її у файл та на екран монітора.

Контрольні запитання.

1. Який шифр називається шифром гаммування?
2. Яким умовам повинен задовольняти ідеальний шифр гаммування?
3. Що називається додаванням за модулем m?
4. Як залежить від ключа даний алгоритм шифрування?
5. Яким умовам повинен задовольняти ключ шифрування?
6. Як оцінити трудомісткість криптоаналітика для дешифрування даного шифру гаммування?
7. Що потрібно знати криптоаналітику для швидкого і точного визначення ключа шифрування?
8. На які групи поділяються криптографічні алгоритми? Чим вони характеризуються?
9. Які Ви знаєте методи розкриття шифру, застосованого у цій ЛР?
10. Як можна, на Вашу думку, ускладнити дану систему шифрування?