Лабораторна робота № 4.

Шифрувальна система на основі шифру гаммування

Нехай відоме відкрите повідомленні $t_1,\ldots,t_n$, що являє собою послідовність символів із табл. 9.

Таблиця 9

Таблиця заміни при шифруванні

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

Ключ К являє собою послідовність чисел $k_1,\ldots,k_n$ із множини М={0,..,31}. Зашифрований текст $s_1,\ldots,s_n$ обчислюється за формулою

$$s_i = (C(t_i) + k_i) \bmod 32, \qquad (1)$$

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

Розшифрувати повідомлення можна за допомогою формули

$$t_i = C^{-1}(s_i + (32 - k_i) \bmod 32. \qquad (2)$$

У даному випадку через C^{-1} позначають функцію, яка виконує обернене перетворення: перетворює порядковий номер із множини 0-31 у символ алфавіту.

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

Визначений у такий спосіб шифр називається шифром гаммування з випадковоюрівноймовірною гаммою {гаммою прийнято називати послідовність чисел $k_1,\ldots,k_n$, що додається за модулем до шифрованого повідомлення).

При такому методі шифрування довжина шифрограми збігається з

довжиною відкритого повідомлення. Це полегшує криптоаналітикам задачу дешифрування повідомлення за частотним словником. Щоб сховати довжину повідомлення, його можна доповнити пробілами до певної фіксованої довжини, яку не перевищує стандартне повідомлення.

Приклад.

Розглянемо приклад використання спрощеного шифру гаммування. Спрощення полягають у заміні випадкової гамми псевдовипадковою на простому ключі з трьох випадкових чисел.

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

$$Z_t = (Y_t + Y_{t+1}) \bmod 32, \quad t = 1,\ldots,n \tag{3}$$

обчислюється псевдовипадкова послідовність $Z_1,\ldots,Z_n$, що використовується як випадкова гамма. Шифрування полягає в додаванні за модулем 32 елементів гамми з порядковими номерами літер у табл. 9.

Зашифруємо на ключі $K = (04,31,15)$ повідомлення “НАКАЗУЮ НАСТУПАТИ”.

Послідовність $Y_1,\ldots,Y_{n+1}$ у даному випадку буде мати вигляд “04 31 15 19 18 01 20 06 07 27 01 08 03 04 12 15 19”.

Додамо за модулем 32 порядкові номери символів нашого повідомлення з елементами псевдовипадкової послідовності (Z_t), отриманої за формулою (3):

16 00 13 00 08 22 30 16 00 20 21 22 18 00 21 09 – повідомлення;

03 14 02 05 19 21 26 13 02 28 09 11 07 16 27 02 – гамма;

19 14 15 05 27 11 24 29 02 16 30 01 25 16 16 11 – шифрограма.

Розшифрувати повідомлення можна за допомогою формули (2), якщо згенерувати гамму за відомим секретним ключем K.

Тепер розглянемо метод дешифрування нашого повідомлення. Загальна кількість текстів із 16 літер складе 32^{16}, а кількість різних ключів у даному випадку $32^3 = 32768$. Отже, 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 можливе таке повідомлення чи ні). Згідно з дослідженнями К. Шеннона, кількість змістовних текстів із 16 літер в англійській мові приблизно 10^5. Приблизно така ж оцінка справедлива і для російської мови. Імовірність появи серед усіх варіантів дешифровок іншого змістовного тексту менша від $2{,}6 \times 10^{-20}$. Для порівняння -ймовірність вгадати 6 чисел із 36 більша за 10^{-10}. Якщо криптоаналітик буде відкидати по одному неправильному повідомленню за секунду, то йому потрібно буде нате, щоб продивитися всі повідомлення, приблизно 9 годин. Таким чином, трудовитрати ручного дешифрування даного повідомлення методом прямого перебору ключів складуть 500 годин. Процес можна прискорити, якщо застосувати ЕОМ. У цьому випадку результати генерування всіх ключів і дешифрування всіх варіантів буде отримано практично миттєво, і лише 9 годин знадобиться криптоаналітику для відбору істинного повідомлення серед хибних.

Завдання роботи.

1. Народне прислів’я українською мовою, обране для лаб. работи № 1, зашифрувати шифром гаммування. Для цього генератором випадкових чисел згенеруйте послідовність з трьох чисел з множини $(0,\ldots,31)$ та оберіть її в якості ключа.

2. Використовуючи згенеровану гамму за відомим секретним ключем K, розшифруйте повідомлення.