**Лабораторна робота №3**

Лабораторна робота містить 2 завдання.

Завдання 1. **Шифрувння методом Хілла**

Завдання 2. **Шифрувальна система на основі шифру гамування**

**Шифрувння методом Хілла**

***Теоретичні відомості.*** Спочатку символи алфавіту кодуємо числами, наприклад порядковими номерами символів. Далі вибираємо матрицю n × n, яка буде ключем шифру. Вихідне повідомлення розбиваємо на блоки розміром n букв, числові значення яких розглядаємо як вектори розміру n. Кожний з векторів множимо на матрицю шифрування n × n. Результуючий блок (вектор) розміру n — відповідний вихідному блоку зашифрований текст. Операції додавання і множення виконуються за модулем m, де m — потужність алфавіту.

Ключ, можна задавати матрицею, але вигідніше задавати кодовим словом, числове представлення якого трансформують у матрицю. Для того, щоб отримати квадратну матрицю n x n, довжина кодового речення має бути квадратом цілого числа, наприклад 4, 9, 16, 25, і т. д.

Для розшифрування необхідно шифротекст помножити на обернену матрицю.

BA=C \to CA^{-1}=BAA^{-1}=BE=B

Щоб операція розшифрування була можливою, матриця шифрування повинна мати обернену в {Z}}_{{m}}^{n} .

Отже:

1. детермінант матриці повинен бути відмінним від 0,
2. детермінант матриці повинен мати обернений елемент в кільці {Z}}_{{m}}^{n}. Необідною умовою існування оберненого елемента є: детермінант і модуль (довжина алфавіту) повинні бути взаємно простими числами.

***Практична частина.***

1. Створіть криптографічну систему, яка використовує шифр Хілла, описаний у теоретичній частині.
2. Система шифрування повинна задовольняти наступним вимогам: 1) читати відкрите повідомлення з текстового файлу і перетворювати його у цифрове представлення; 2) запитувати ключове слово (9 і більше літер); 3) генерувати ключ-матрицю по ключовому слову; 4) шифрувати за допомогою алгоритму Хілла відкрите повідомлення і записувати його у файл.
3. Система розшифровування повинна задовольняти таким вимогам: 1) читати шифрограму з текстового файлу; 2) запитувати ключове слово; 3) генерувати ключ-матрицю; 4) розшифровувати шифрограму і виводити її у файл та на екран монітора.

**Шифрувальна система на основі шифру гаммування**

***Теоретичні відомості.*** Нехай у нас є відкрите повідомлення *t1,…,tn,* 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 *К* являє собою послідовність чисел *k1,…,kn* з множини **M**={0,…,32}. Зашифрований текст *s1,…,sn* обчислюється за наступною формулою:

*si=(C(ti)+ki)* mod 33, *i*=1,…*,n*, (1)

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

Розшифрувати повідомлення можна за допомогою формули:

*ti= C*-1*(si+(*33*-ki))* mod 33.

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

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

Визначений таким чином шифр називається *шифром гамування з випадковою рівноймовірною гамою* (*гамою* прийнято називати послідовність чисел *k1,…,kn*, 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 гамування. 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 *К*=(*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) mod 32 формується послідовність *Y*1,..., *Y*n+1 для *t*>3. Далі, за формулою

*Z*t=(*Y*t+*Y*t+1) mod 32, *t*=1,…,*n* (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 *К*=(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:

*ti= C*-1*((si+(*32*-ki))* mod 32, (3)

якщо згенерувати гамму за відомим секретним ключем *К*.

Тепер розглянемо метод дешифрування нашого повідомлення. Загальна кількість текстів з 20 літер складається 3220, а кількість різних ключів у даному випадку 323=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 106. Приблизно така ж оцінка справедлива і для української мови. Імовірність появи серед всіх варіантів дешифровок іншого змістовного тексту менша 2.6х10-20. 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) mod 32 =18; (16+ *Z*2) mod 32 =30 i (8+ *Z*3) mod 32 =10. Звідси можна знайти перших три знаки гамми: 3; 14; 2. Тепер можна скласти систему з таких трьох рівнянь:

(*Y*1+*Y*2) mod 32 = 3; (*Y*2+*Y*3) mod 32 = 14; (*Y*3+*Y*4) mod 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 гамування 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 гамування, 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.