# **ЛАБОРАТОРНАЯ РАБОТА № 1**

**Дослідження шифр перестановки**

**Мета роботи:** Ознайомитися з різними шифрами перестановки і методами їх дешифрування.

1. Короткі теоретичні відомості

Шифри перестановки є найпростішими, і, ймовірно, найдавнішими шифрами. При шифруванні перестановкою символи шіфруемоготексту переставляються за певним правилом в межах блоку цього тексту. 1.1 Шифр ​​перестановки "скитала" У V столітті до нашої ери правителі Спарти, найбільш войовничого з грецьких держав, мали добре відпрацьовану систему секретної військової зв'язку і шифрували свої послання за допомогою скитала, першого найпростішого криптографічного пристрою, що реалізує метод простий перестановки.

Шифрування виконувалося наступним чином. На стрижень циліндричної форми, який називався скитала, намотували спіраллю (виток до витка) смужку пергаменту і писали на ній уздовж стрижня кілька рядків тексту повідомлення (рисунок 1.1).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| В | С | Т | Р | Е |
| Ч | А | Й | Т | Е |
| У | Т | Р | О | М |

Рисунок 1.1 – Шифр “скитала”

Потім знімали зі стрижня смужку пергаменту з написаним текстом. Букви на цій смужці виявлялися розташованими хаотично:

**В Ч У С А Т Т Й Р Р Т О Е Е М.**

Такий же результат можна отримати, якщо букви повідомлення писати по кільцю не підряд, а через певне число позицій до тих пір, поки не буде вичерпано весь текст. Для розшифрування такого шифротекста потрібно не тільки знати правило шифрування, але і володіти ключем у вигляді діаметра стрижня.

## **Шифр таблиці**

В кінці XIV століття з початком епохи Відродження починає відроджуватися і криптографія. Поряд з традиційними застосуваннями криптографії в політиці, дипломатії і військовій справі з'являються й інші завдання - захист інтелектуальної власності від переслідувань інквізиції або запозичень зловмисників. У розроблених шифрах перестановки того часу застосовуються шифрувальні таблиці, які по суті задають правила перестановки літер в повідомленні.

Як ключ в шифруючих таблицях використовуються:

- розмір таблиці;

- слово або фраза, що задають перестановку;

- особливості структури таблиці.

Одним з найбільш примітивних табличних шифрів перестановки є проста перестановка, для якої ключем служить розмір таблиці. Цей метод шифрування схожий з шифром скитала. Наприклад, повідомлення.

**НАД ВСЕЙ ИСПАНИЕЙ БЕЗОБЛАЧНОЕ НЕБО**

Записується в таблицю по черзі по стовпцях.

Результат заповнення таблиці з 5 рядків і 6 стовпців показаний в таблиці 1.2 Після заповнення таблиці текстом повідомлення по стовпцях для формування шифротекста зчитують вміст таблиці по рядках.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Н** | **Е** | **А** | **Б** | **Л** | **Е** |
| **А** | **Й** | **Н** | **Е** | **А** | **Н** |
| **Д** | **И** | **И** | **З** | **Ч** | **Е** |
| **В** | **С** | **Е** | **О** | **Н** | **Б** |
| **С** | **П** | **Й** | **Б** | **О** | **О** |

Таблиця 1.2 - Заповнення таблиці з 5 рядків і 6 стовпців

Якщо шифротекст записувати групами по 5 букв, виходить таке шифрування повідомлення:

**НЕАБЛ ЕАЙНЕ АНДІІ ЗЧЕВС ЕОНБС ПЙБОО**

Природно, відправник і одержувач повідомлення повинні заздалегідь домовитися про загальному ключі у вигляді розміру таблиці. Об'єднання букв шифротекста в 5-ти літерні групи не входить в ключ шифру і здійснюється для зручності запису несмислового тексту. При розшифровці дії виконуються в зворотному порядку.

Дещо більшою стійкістю до розкриття володіє метод шифрування, званий одиночній перестановкою по ключу. Він відрізняється від попереднього тим, що стовпчики таблиці переставляються за ключовим словом, фразою або набору чисел довжиною в рядок таблиці. Застосуємо як ключ, наприклад, слово

**ЦУНАМИ,**

а текст повідомлення візьмемо з попереднього прикладу. У таблицях 1.3 і 1.4 показано заповнення до перестановки і після перестановки повідомлення з ключовим словом.

Таблиця 1.3 – Заповнення до перестановки

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ц** | **У** | **Н** | **А** | **М** | **И** |
| **6** | **5** | **4** | **1** | **3** | **2** |
| **Н** | **Е** | **А** | **Б** | **Л** | **Е** |
| **А** | **Й** | **Н** | **Е** | **А** | **Н** |
| **Д** | **И** | **И** | **З** | **Ч** | **Е** |
| **В** | **С** | **Е** | **О** | **Н** | **Б** |
| **С** | **П** | **Й** | **Б** | **О** | **О** |

Таблиця 1.4 – Заповнення після перестановки

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **А** | **И** | **М** | **Н** | **У** | **Ц** |
| **1** | **2** | **3** | **4** | **5** | **6** |
| **Б** | **Е** | **Л** | **А** | **Е** | **Н** |
| **Е** | **Н** | **А** | **Н** | **Й** | **А** |
| **З** | **Е** | **Ч** | **И** | **И** | **Д** |
| **О** | **Б** | **Н** | **Е** | **С** | **В** |
| **Б** | **О** | **О** | **Й** | **П** | **С** |

У верхньому рядку таблиці 1.3 записаний ключ, а номери під буквами ключа визначені відповідно до природного порядком букв в алфавіті. Якби в ключі зустрілися однакові букви, вони б були пронумеровані зліва направо.

У таблиці 1.4 стовпці переставлені відповідно до впорядкованими номерами букв ключа. При зчитуванні вмісту таблиці 1.4 по рядках і записи шифротекста групами по п'ять букв отримаємо шифрування повідомлення:

**БЕЛАЕ НЕНАН ЙАЗЕЧ ИИДОБ НЕСВБ ООЙПС**

Для забезпечення додаткової скритності можна повторно зашифрувати повідомлення, яке вже пройшло шифрування. Такий метод шифрування називається подвійний перестановкою. У випадку подвійної перестановки стовпців і рядків таблиці перестановки визначаються окремо для стовпців і окремо для рядків. Спочатку в таблицю записується текст повідомлення, а потім по черзі переставляються стовпці, а потім рядки. При розшифрування порядок перестановок повинен бути зворотним.

Приклад виконання шифрування методом подвійного перестановки показаний в таблиці 1.5. Якщо зчитувати шифротекст з таблиці 1.6 через підрядник блоками по чотири літери, то вийде наступне повідомлення:

**ГРУЗИТЕ АПЕЛЬСИНЫ**

Ключем до шифру подвійний перестановки служить послідовність номерів стовпців і номерів рядків вихідної таблиці 1.3.4: в нашому прикладі послідовності 4132 і 3142 відповідно.

Таблиця 1.5 – Заповнення до перестановки

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **4** | **1** | **3** | **2** |
| **3** | **Г** | **Р** | **У** | **З** |
| **1** | **И** | **Т** | **Е** | **А** |
| **4** | **П** | **Е** | **Л** | **Ь** |
| **2** | **С** | **И** | **Н** | **Ы** |

Таблиця 1.3.6 – Перестановка рядків

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** |
| **3** | **Р** | **З** | **У** | **Г** |
| **1** | **Т** | **А** | **Е** | **И** |
| **4** | **Е** | **Ь** | **Л** | **П** |
| **2** | **И** | **Ы** | **Н** | **С** |

Число варіантів подвійний перестановки швидко зростає при збільшенні розміру таблиці:

- для таблиці 3 х 3 86 варіантів;

- для таблиці 4 х 4 576 варіантів;

- для таблиці 5 х 5 14400 варіантів.

Однак подвійна перестановка не відрізняється високою стійкістю і порівняно просто зламується при будь-якому розмірі таблиці шифрування.

## **Магічні квадрати**

У середні століття для шифрування перестановкою застосовувалися і магічні квадрати.

Магічними квадратами називають квадратні таблиці з вписаними в їх клітини послідовними натуральними числами, починаючи з 1, які дають в сумі по кожному стовпцю, кожному рядку і кожній діагоналі одне і те ж число.

Шифруемий текст вписували в магічні квадрати відповідно до нумерації їх клітин. Якщо потім виписати вміст такої таблиці по рядках, то вийде шифротекст, сформований завдяки перестановці букв вихідного повідомлення. У ті часи вважалося, що створені за допомогою магічних квадратів шифротекста охороняє не тільки ключ, але і магічна сила.

Приклад магічного квадрата і його заповнення повідомленням.

**ГРУЗИТЕ АПЕЛЬСИНЫ**

Таблиця 1.3.7 - Магічний квадрат

|  |  |  |  |
| --- | --- | --- | --- |
| **16** | **3** | **2** | **13** |
| **5** | **10** | **11** | **8** |
| **9** | **6** | **7** | **12** |
| **4** | **15** | **14** | **1** |

Таблиця 1.3.8 – Магічний квадрат, заповнений повідомленням

|  |  |  |  |
| --- | --- | --- | --- |
| **Ы** | **У** | **Р** | **С** |
| **И** | **Е** | **Л** | **А** |
| **П** | **Т** | **Е** | **Ь** |
| **З** | **Н** | **И** | **Г** |

Шифротекст, що отримується при зчитуванні вмісту таблиці 1.3.8 за рядками, має такий вигляд.

**ЫУРС ИЕЛА ПТЕЬ ЗНИГ**

Число магічних квадратів швидко зростає зі збільшенням розміру квадрата. Існує лише один магічний квадрат розміром 3 х 3 (якщо не враховувати його повороти). Кількість магічних квадратів 4 х 4 становить вже 880, а кількість магічних квадратів 5 х 5 – близько 250 000.

Магічні квадрати середніх і високих розмірів могли служити оптимальною базою задля забезпечення потреб шифрування на той час, оскільки майже неможливо виконати вручну перебір всіх варіантів такого шифру.

Хід роботи

1. Опис програми.

Програма призначена для кодування та декодування слів шифром подвійної перестановки

1. Текст програми.

using System;

namespace Laba1\_Csh

{

class Program

{

const int n = 5;

public static string str = "";

public static int[] keycolms = new int[n] { 0, 1, 4, 3, 2 };

public static int[] keyrows = new int[n] { 1, 0, 3, 2, 4 };

public static string[,] Encryptio = new string[n, n];

public static string[,] Decryptio = new string[n, n];

public static void encryption(string[,] table)

{

for (int i = 0; i < 5; i++)

{

for (int j = 0; j < 5; j++)

{

str += (table[keyrows[j], keycolms[i]]);

Encryptio[i, j] += table[keyrows[i], keycolms[j]];

}

}

for (int i = 0; i < 5; i++)

{

for (int j = 0; j < 5; j++)

{

Console.Write(Convert.ToString(Encryptio[i, j] + " "));

}

Console.WriteLine();

}

}

public static void decryption()

{

str = "";

for (int i = 0; i < 5; i++)

{

for (int j = 0; j < 5; j++)

{

str += (Encryptio[keyrows[i],keycolms[j]]);

Decryptio[i,j] += (Encryptio[keyrows[i], keycolms[j]]);

}

}

for (int i = 0; i < 5; i++)

{

for (int j = 0; j < 5; j++)

{

Console.Write(Convert.ToString(Decryptio[i, j] + " "));

}

Console.WriteLine();

}

}

static void Main(string[] args)

{

string[,] table = new string[n, n] {

{"Г","Р","У","З","И"},

{"Т","Е"," ","А","П"},

{"Е","Л","Ь","С","И"},

{"Н","Ы"," ","В"," "},

{"Я","Щ","И","К","И"}

};

Console.WriteLine("Оригинал: ");

for (int i = 0; i < 5; i++)

{

for (int j = 0; j < 5; j++)

{

Console.Write(Convert.ToString(table[i, j] + " "));

}

Console.WriteLine();

}

Console.WriteLine();

Console.WriteLine("Зашифровано: ");

encryption(table);

Console.WriteLine();

Console.WriteLine("Расшифровано: ");

decryption();

Console.ReadLine();

}

}

}

1. Контрольний приклад.

На рисунку 1.2 зображено результат програми.

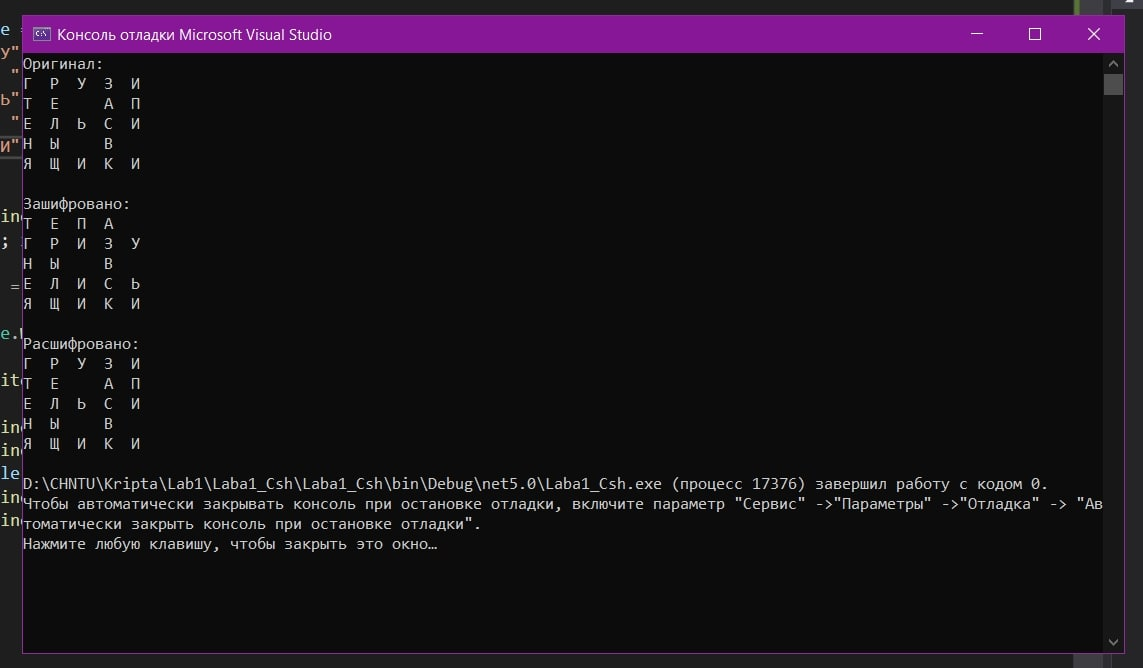


Рисунок 1.2 – Результат шифрування

**Висновок:** ознайомилися з різними шифрами перестановки і методами їх дешифрування.