# ЛАБОРАТОРНАЯ РАБОТА № 2

# ДОСЛІДЖЕННЯ ШИФРІВ ПРОСТОЇ ЗАМІНИ

**Мета роботи:** ознайомитись з різними шифрами простої заміни (шифрами підстановки) та методами їх дешифрування.

# Короткі теоретичні відомості

## Система шифрування Цезаря

Шифр Цезаря є окремим випадком шифру простої заміни (одноалфавітної підстановки). Свою назву цей шифр отримав на ім'я римського імператора Гая Юлія Цезаря, який використовував цей шифр під час листування з Цицероном (близько 50 р. до н.е.).

При шифруванні вихідного тексту кожна літера замінювалася іншу літеру того ж алфавіту за наступним правилом. Замінювана літера визначалася шляхом зміщення по алфавіту від вихідної літери К літер. При досягненні кінця алфавіту виконувався циклічний перехід для його початку. Цезар використовував шифр заміни при зміщенні К = 3. Такий шифр заміни можна встановити таблицею підстановок, що містить відповідні пари букв відкритого тексту і шифротексту. Сукупність можливих підстановок для К = 3 показано в таблиці 1.1.

Таблиця 2.2.1 – Одноалфавітні підстановки (К = 3, m = 26)

|  |  |  |
| --- | --- | --- |
| A → D | J → M | S → V |
| B → E | K → N | T → W |
| C → F | L → O | U → X |
| D → G | M → P | V → Y |
| E → H | N → Q | W → Z |
| F → I | O → R | X → A |
| G → J | P → S | Y → B |
| H → K | Q → T | Z → C |
| I → L | R → U |  |

Наприклад, послання Цезаря

**VENI VIDI VICI**

(у перекладі російською означає "Прийшов, Побачив, Переміг"), спрямоване його другу Амінтію після перемоги над понтійським царем Фарнаком, сином Мітрідата, виглядало б у зашифрованому вигляді так:

**YHQL YLGL YLFL**

Перевагою системи шифрування Цезаря є простота шифрування та розшифрування.

Недоліки цієї системи такі:

- підстановки, що виконуються відповідно до системи Цезаря, не маскують частот появи різних літер вихідного відкритого тексту;

- зберігається алфавітний порядок у послідовності замінних літер. При зміні змінюються тільки початкові позиції такої послідовності;

- число можливих ключів мало;

- шифр Цезаря легко розкривається з урахуванням аналізу частот появи букв у шифротексті.

Криптоаналітична атака проти системи одноалфавітної заміни починається з підрахунку частот появи символів. Визначається кількість появ кожної літери в шифротексті. Потім отриманий розподіл частот літер у шифротексті порівнюється з розподілом частот літер в алфавіті вихідних повідомлень, наприклад, англійською. Літера з найвищою частотою появи в шифротексті замінюється буквою з найвищою частотою появи в англійській мові і т.д. Імовірність успішного розкриття системи шифрування підвищується із збільшенням довжини шифротексту. Концепція, закладена у систему шифрування Цезаря, виявилася дуже плідною, що свідчать її численні модифікації.

## Хід роботи

1. Опис програми.

Програма призначена для кодування та декодування слів шифром Цезаря,

текст програми наведено в лістингу 1.2.

Лістинг 1.2

using System;

namespace Lav2

{

public class CaesarCipher

{

//символи української абетки

const string alfabet = "АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ";

private string CodeEncode(string text, int k)

{

//додаємо до алфавіту малі літери

var fullAlfabet = alfabet + alfabet.ToLower();

var letterQty = fullAlfabet.Length;

var retVal = "";

for (int i = 0; i < text.Length; i++)

{

var c = text[i];

var index = fullAlfabet.IndexOf(c);

if (index < 0)

{

//якщо літеру не знайдено, додаємо її незмінною

retVal += c.ToString();

}

else

{

var codeIndex = (letterQty + index + k) % letterQty;

retVal += fullAlfabet[codeIndex];

}

}

return retVal;

}

//шифрування тексту

public string Encrypt(string plainMessage, int key)

=> CodeEncode(plainMessage, key);

//дешифрування тексту

public string Decrypt(string encryptedMessage, int key)

=> CodeEncode(encryptedMessage, -key);

}

class Program

{

static void Main(string[] args)

{

var cipher = new CaesarCipher();

Console.Write("Введіть текст повідомлення: ");

var message = Console.ReadLine();

Console.Write("Введіть ключ: ");

var secretKey = Convert.ToInt32(Console.ReadLine());

var encryptedText = cipher.Encrypt(message, secretKey);

Console.WriteLine("Зашифроване повідомлення: {0}", encryptedText);

Console.WriteLine("Розшифроване повідомлення: {0}", cipher.Decrypt(encryptedText, secretKey));

Console.ReadLine();

}

}

}

1. Контрольний приклад.

На рисунку 1.3 зображено результат програми шифрування да дешифрування шифром Цезаря.

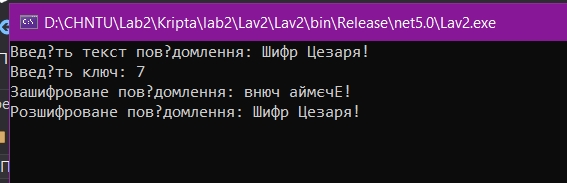


Рисунок 1.3 – Результат шифрування

**Висновок:** ознайомились з різними шифрами простої заміни (шифрами підстановки) та методами їх дешифрування.