

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
імені ТАРАСА ШЕВЧЕНКА**



**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №7**

**3 курсу**

**«Безпека мереж і комп'ютерних систем»**

*студента 2 курсу  
групи ПП-22  
спеціальності 122 «Комп'ютерні науки»  
ОП «Прикладне програмування»  
Шевлюк Вікторії Віталіївни*

*Перевірів:  
д.т.н, професор  
Сайко В. Г.*

**Київ 2022**

**Тема:** Дослідження принципів роботи найпростіших алгоритмів шифрування (шифр Цезаря, шифрування з використанням логічної операції XOR). Криптографічний аналіз даних алгоритмів.

**Мета:** Ознайомитися з найпростішими методами криптографічного захисту інформації. Вивчити шифр Цезаря і методи його криптоаналізу. Засвоїти алгоритм шифрування за використанням логічної операції XOR.

**Завдання:**

1. Вивчити основні теоретичні положення щодо основ криптографічного захисту інформації, шифру Цезаря і алгоритму шифрування, заснованого на використанні логічної операції XOR, принципів злому даних шифрів.

2. Реалізувати програмно шифрування/дешифрування шифром Цезаря:

- алфавіт задається в тілі програми і виводиться на екран (АБВГГДЕСЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЮЯ \_.,0123456789);

- значення ключа вводиться з клавіатури;

- результат шифрування виводиться на екран і в файл «cypher1.txt».

3. Реалізувати програмно злам шифротексту, отриманого на етапі 2:

- алфавіт задається в тілі програми і виводиться на екран (АБВГГДЕСЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЮЯ \_.,);

- шифротекст вводиться з файлу «cypher1.txt»;

- величина ключа підбирається методом перебору в циклі від 1 до кількості символів у вихідному алфавіті;

- результат дешифрування виводиться на екран і в файл "open1.txt".

4. Реалізувати програмно XOR-шифрування:

- в якості відкритого тексту взяти текст із завдання 2;

- значення ключа шифрування вводиться з клавіатури;

- результат шифрування виводиться на екран і в файл «cypher2.txt».

5. Реалізувати програмно XOR-дешифрування:

- рядок шифротексту вводиться з файлу «cypher2.txt»;

- значення ключа дешифрування вводиться з клавіатури;
- результат дешифрування виводиться на екран і в файл "open2.txt".

### Хід роботи:

Вивчивши теоретичний матеріал та вимоги до програми, я написала наступний код, що здійснює шифрування Цезарем і Ксором:

```

1  using System;
2  using System.IO;
3  using System.Text;
4
5
6  namespace lab7
7  {
8      class Program
9      {
10         public static char cipher(char ch, int key)
11         {
12             if (!char.IsLetter(ch))
13             {
14                 return ch;
15             }
16
17             char d = char.IsUpper(ch) ? 'A' : 'a';
18             return (char)((((ch + key) - d) % 26) + d);
19         }
20
21         public static string Encipher(string input, int key)
22         {
23             string output = string.Empty;
24
25             foreach (char ch in input)
26             {
27                 output += cipher(ch, key);
28             }
29             File.WriteAllTextAsync("encipher.txt", output);
30             return output;
31         }
32
33         public static string Decipher(string input, int key)
34         {
35             File.WriteAllTextAsync("decipher.txt", Encipher(input, 26 - key));
36             return Encipher(input, 26 - key);
37         }
38     }
39 }

```

```

Ссылка: 1
public static string BruteForce(string input)
{
    string output = string.Empty;

    for (int bruteKey = 0; bruteKey < 26; bruteKey++)
    {
        foreach (char ch in input)
            output += cipher(ch, bruteKey);
    }

    File.WriteAllTextAsync("bruteForce.txt", output);
    return output;
}

Ссылка: 2
public static string XOREncryptOrDecrypt(string text, string key)
{
    var result = new StringBuilder();

    for (int c = 0; c < text.Length; c++)
        result.Append((char)((uint)text[c] ^ (uint)key[c % key.Length]));

    File.WriteAllTextAsync("xor.txt", Convert.ToString(result));
    return result.ToString();
}

```

```

Ссылка: 0
static void Main(string[] args)
{
    Console.WriteLine("Type a string to encrypt:");
    string UserString = Console.ReadLine();

    Console.WriteLine("\n");

    Console.Write("Enter your Key");
    int key = Convert.ToInt32(Console.ReadLine());
    Console.WriteLine("\n");

    Console.WriteLine("Encrypted Data");

    string cipherText = Encipher(UserString, key);
    Console.WriteLine(cipherText);
    Console.WriteLine("\n");

    Console.WriteLine("Decrypted Data:");

    string t = Decipher(cipherText, key);
    Console.WriteLine(t);
    Console.WriteLine("\n");

    string bruteForceCipherText = File.ReadAllText("encipher.txt");
    string y = BruteForce(bruteForceCipherText);
    Console.WriteLine(y);
    Console.WriteLine("\n");

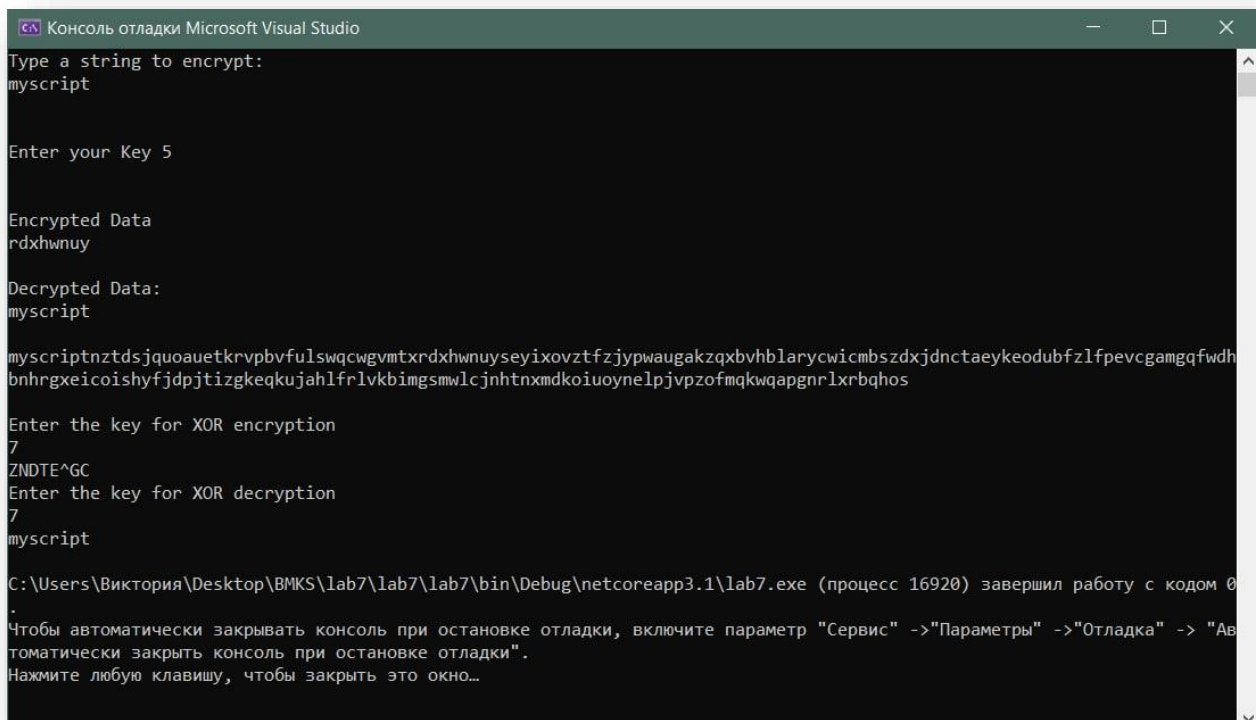
    Console.WriteLine("Enter the key for XOR encryption");
    string xorKey = Console.ReadLine();
    Console.WriteLine(XOREncryptOrDecrypt(UserString, xorKey));

    Console.WriteLine("Enter the key for XOR decryption");
    string xorDecryptKey = Console.ReadLine();
    string xorEncrypted = File.ReadAllText("xor.txt");
    Console.WriteLine(XOREncryptOrDecrypt(xorEncrypted, xorDecryptKey));

    Console.ReadKey();
}

```

## Результат роботи програми:



```
Консоль отладки Microsoft Visual Studio
Type a string to encrypt:
myscript

Enter your Key 5

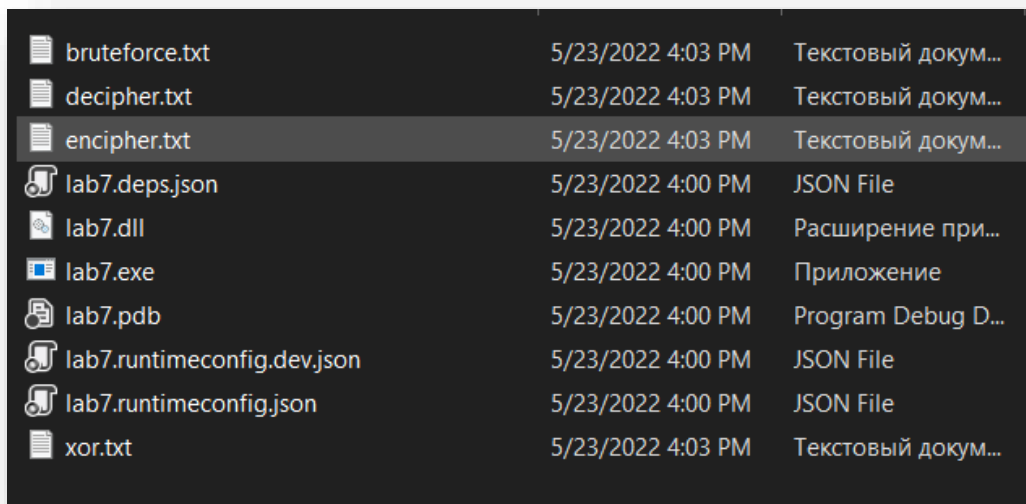
Encrypted Data
rdxhwnuy

Decrypted Data:
myscript

myscriptnztzdsjqouaetkrvpbvfulswqcgwmtxrdxhwnuyseyixovztfzjypwaugakzqxvvhblarycwmbszdxjdnctaeykeodubfzlfpevcgamgqfwdh
bnhrgrxeicoishyfdpjtizgkeqkujahlfrlvkbimgsmwlcjnhntxmdkoiuoyneipjvpzofmqkwapgnrlxrbqhos

Enter the key for XOR encryption
7
ZNDTE^GC
Enter the key for XOR decryption
7
myscript

C:\Users\Виктория\Desktop\BMKS\lab7\lab7\bin\Debug\netcoreapp3.1\lab7.exe (процесс 16920) завершил работу с кодом 0
.
Чтобы автоматически закрывать консоль при остановке отладки, включите параметр "Сервис" -> "Параметры" -> "Отладка" -> "Автоматически закрыть консоль при остановке отладки".
Нажмите любую клавишу, чтобы закрыть это окно...
```



bruteforce.txt	5/23/2022 4:03 PM	Текстовый докум...
decipher.txt	5/23/2022 4:03 PM	Текстовый докум...
encipher.txt	5/23/2022 4:03 PM	Текстовый докум...
lab7.deps.json	5/23/2022 4:00 PM	JSON File
lab7.dll	5/23/2022 4:00 PM	Расширение при...
lab7.exe	5/23/2022 4:00 PM	Приложение
lab7.pdb	5/23/2022 4:00 PM	Program Debug D...
lab7.runtimeconfig.dev.json	5/23/2022 4:00 PM	JSON File
lab7.runtimeconfig.json	5/23/2022 4:00 PM	JSON File
xor.txt	5/23/2022 4:03 PM	Текстовый докум...

**Висновок:** у ході даної лабораторної роботи я навчилась реалізовувати шифрування Цезаря і з використанням операції Ксор. У шифрі Цезаря кожна буква алфавіту замінюється буквою, яка знаходиться на три позиції далі в цьому ж алфавіті. Якщо кожній букві призначити числовий

еквівалент (  $a=1$ ,  $b=2$  і т.д.), то кожна буква відкритого тексту  $P$  замінюється буквою шифрованого тексту  $C$ :

$$c = E(p) = (p + 3) \bmod p.$$

У загальному випадку зсув може бути будь-яким, тому узагальнений алгоритм Цезаря описується формулою

$$c = E(p) = (p + k) \bmod p,$$

де  $k$  приймає значення в діапазоні від 1 до 25. Принцип дешифрування:

$$p = D(c) = (c - k) \bmod p.$$

Якщо відомо, що певний текст був зашифрований за допомогою шифру Цезаря, то для зламу досить перевірити 25 можливих варіантів ключів.

Найпростішим і одним з найефективніших алгоритмів шифрування є так зване XOR-шифрування. Як відомо з булевої алгебри, операція логічного додавання « $\oplus$ » по модулю 2 (або логічного виключаючого АБО - XOR, eXclusive OR) має наступну семантику:

таблиця істинності для XOR:

$x_i$	$y_i$	$x_i \oplus y_i$
0	0	0
0	1	1
1	0	1
1	1	0

тобто:

$$\begin{array}{rcl}
 x & = & 10011101 \\
 & \oplus & \\
 y & = & 01001100 \\
 \hline
 z & = & 11010001
 \end{array}$$

Число  $y$  можна назвати кодуємим (або шифруємим) ключем. Дане криптографічне перетворення можна описати таким співвідношенням:

$$(z)_i = (x)_i \oplus y$$

Тут  $(z)_i$  – шифротекст, а  $(x)_i$  – відповідний йому відкритий текст.

Дешифрування шифротекста за відомим ключем згідно описаним властивостям операції XOR проводиться таким чином:

$$(x)_i = (z)_i \oplus y$$

### **Контрольні питання:**

#### **1. Дайте визначення криптографії та криптоаналізу.**

Криптоаналіз – це наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.

#### **2. Перерахуйте розділи криптології.**

Криптографія та криптоаналіз

#### **3. Що таке алфавіт?**

Набір символів, з яких складається відкритий/закритий текст.

#### **4. Дайте визначення поняттям закритий і відкритий текст.**

Відкритий текст - нешифроване повідомлення; закритий - шифроване

#### **5. Що таке ключ?**

Секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення.

#### **6. У чому полягає відмінність симетричних і асиметричних систем шифрування?**

У симетричному і відправник, і отримувач мають однаковий ключ. В асиметричному використовують пару ключів - закритий (відомий власнику) та відкритий

#### **7. Що таке крипостійкість, і які її основні показники?**

Здатність криптографічного алгоритму протистояти криптоаналізу; обчислювальна складність повного перебору, виявлені слабкості

## **8. Які загальні вимоги висуваються до криптосистем?**

Число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів.

Число операцій, необхідних для розшифрування інформації шляхом перебору всіляких ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережових обчислень).

Знання алгоритму шифрування не повинно впливати на надійність захисту.

Незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа.

Структурні елементи алгоритму шифрування повинні бути незмінними.

Додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті.

Довжина шифрованого тексту повинна бути рівною довжині вихідного тексту.

Не повинно бути простих і легко встановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування.

Будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації.

Алгоритм повинен допускати як програмно, так і апаратну реалізацію, при цьому зміна довжини ключа не повинно вести до якісного погіршення алгоритму шифрування.



**9. У чому суть шифрування методом Цезаря?**

Зсув букв в повідомленні на певну кількість символів за алфавітом.

**10. Які істотні недоліки методу Цезаря?**

Загально відомий, нестійкий

**11. Яким чином проводиться злом методу Цезаря?**

Перебором у циклі зі зміною зсуву

**12. У чому суть шифрування з використанням логічної операції XOR?**

$x_i$	$y_i$	$x_i \oplus y_i$
0	0	0
0	1	1
1	0	1
1	1	0

тобто:

$x$	=	10011101
		$\oplus$
$y$	=	01001100
$z$	=	11010001

Число  $y$  можна назвати кодуєчим (або шифруючим) ключем. Дане криптографічне перетворення можна описати таким співвідношенням:

$$(z)_i = (x)_i \oplus y$$

Тут  $(z)_i$  – шифротекст, а  $(x)_i$  – відповідний йому відкритий текст.

Дешифрування шифротекста за відомим ключем згідно описаним властивостям операції XOR проводиться таким чином:

$$(x)_i = (z)_i \oplus y$$