Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 4**

«ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ»

Выполнил:

Студент: Белицкий В.Д.

ФИТ 2 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2022

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* Зашифровать сообщение на основе соотношений (*k* = 5)
* Расшифровать сообщение на основе соотношений (*k* = 5)
* Зашифровать шифром Виженера (Ключ = фамилия)
* Расшифровать шифр Виженера (Ключ = фамилия)
* Оценить время выполнения каждого шифра

Сущность подстановочного шифрования состоит в том, что исходный текст (из множества *М*) и зашифрованный текст (из множества *С*) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки

1. **Методика выполнения расчетов**

В данной лабораторной работе была поставлена цель создания приложения, позволяющее произвести зашифрование и расшифрование на основе соотношений, а также шифром Виженера. Добавлена функция оценки времени выполнения метода шифрования

public string Vigenere(string text, string password, bool encrypting = true)

{

var gamma = GetRepeatKey(password, text.Length);

var retValue = "";

var q = letters.Length;

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

{

var letterIndex = letters.IndexOf(text[i]);

var codeIndex = letters.IndexOf(gamma[i]);

if (letterIndex < 0)

{

//если буква не найдена, добавляем её в исходном виде

retValue += text[i].ToString();

}

else

{

retValue += letters[(q + letterIndex + ((encrypting ? 1 : -1) \* codeIndex)) % q].ToString();

}

}

return retValue;

}

**Листинг 2.1 – Шифр Виженера**

public string CodeEncode(string text, int k)

{

//добавляем в алфавит маленькие буквы

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)

{

//если символ не найден, то добавляем его в неизменном виде

retVal += c.ToString();

}

else

{

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

retVal += fullAlfabet[codeIndex];

}

}

return retVal;

}

**Листинг 2.2 – Шифрование на основе соотношений (*k* = 5)**

**Рис 2.1 – График оценки времени выполнения зашифрования Виженера**

**Рис 2.2 – График оценки времени выполнения зашифрования на основе соотношений**

**3. Результаты работы приложения**

Для выполнения расчетов достаточно необходимо запустить приложение, выбрать необходимый пункт задания и ввести числа. Следующие рисунки показывают необходимые расчеты и вызовы методов, требуемые в данной лабораторной работе.

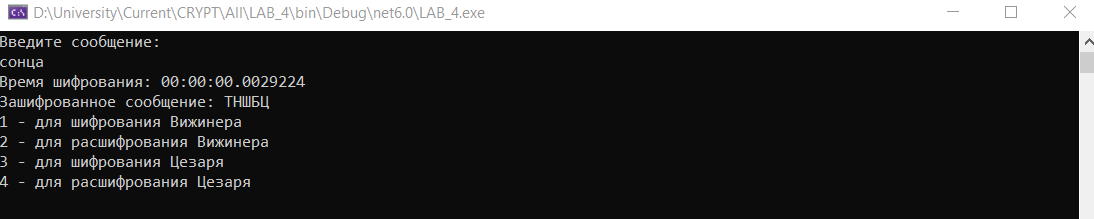


Рисунок 3.1 – Результат зашифрования сообщения шифром Виженера

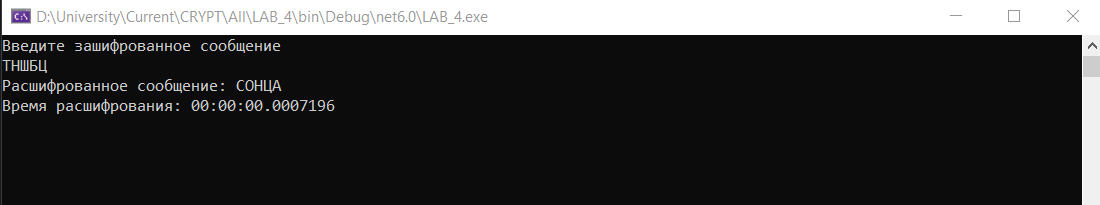


Рисунок 3.2 – Результат расшифрование сообщения шифром Виженера

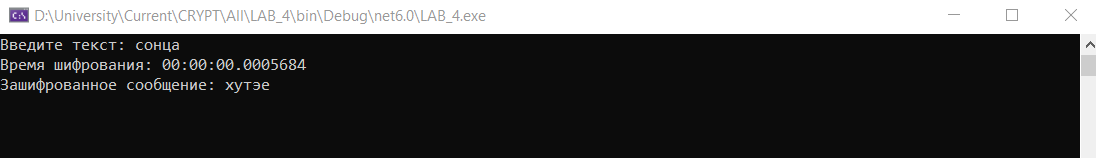


Рисунок 3.3 – Результат зашифрования сообщения на основе соотношений

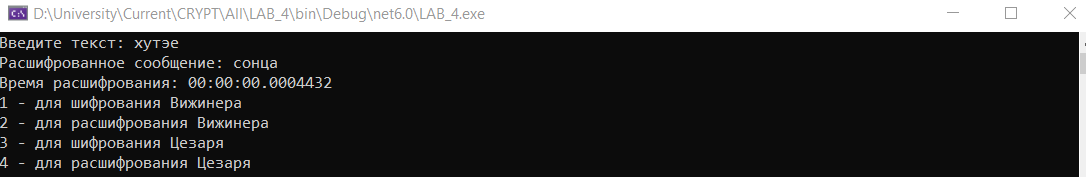


Рисунок 3.4 – Результат расшифрования сообщения на основе соотношений

**Вывод**

В ходе изучения теоретических материалов лабораторной работы и выполнения её практической части было разработано авторское приложение для шифрования ми расшифрования заданного текста. Использовались:

1. Шифр на основе соотношений (*k* = 5)
2. Шифр Виженера (Ключ = фамилия)

Также приложение оценивает время всех произведенных операций с текстом.