Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе подстановки символов**

Студент: Каспер Н.В.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* осуществлять подстановку на основании алгоритма Цезаря с ключом;
* осуществлять подстановку на основании алгоритма Трисемуса с ключевым словом;
* оценивать время выполнения операция зашифрования.

1. **Методика выполнения поставленных задач**

Для выполнения зашифрования сообщения при помощи алгоритма Цезаря с ключом используется функция CeasarChipher. Реализация данной функции представлена на рисунке 2.1.

В данном шифре каждый одиночный символ заменяется другим одиночным символам. Используется тот же алфавит, но уже в другом порядке – со смещением.

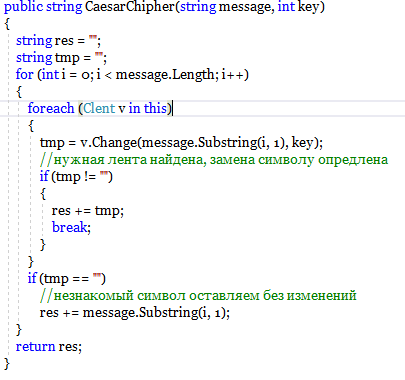


Рисунок 2.1 – Функция для зашифрования

Функция для изменения позиции символа согласно ключа представлена на рисунке 2.2. Для того, чтобы вычислить новую позицию символа необходимо сложить текущую позицию символа с ключом k и поделить результат суммирования по модулю N. Где N – количество символов в алфавите.

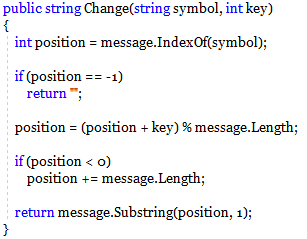


Рисунок 2.2 – Функция изменения позиции символа

Для реализации алгоритма Трисемуса используется таблица, заполнение которой представлено на рисунке 2.3.

В таблицу сначала вписывалось по стрелкам ключевое слово, причем повторяющиеся буквы также отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

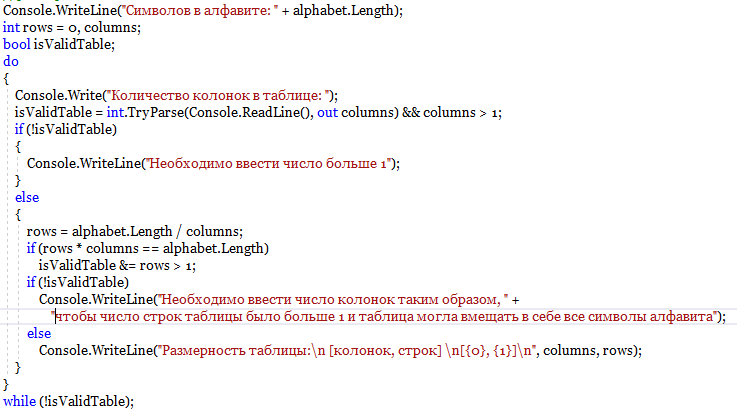


Рисунок 2.3 – Заполнение матрицы

Шифрование с помощью алгоритма Трисемуса представлено на рисунке 2.4.

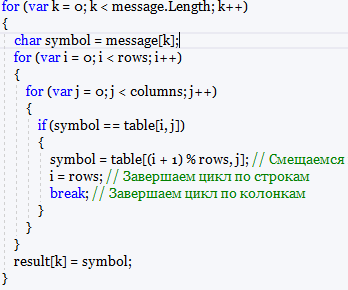


Рисунок 2.4 – Функция для зашифрования

Результат работы алгоритма Цезаря на основании ключа представлен на рисунке 2.5.

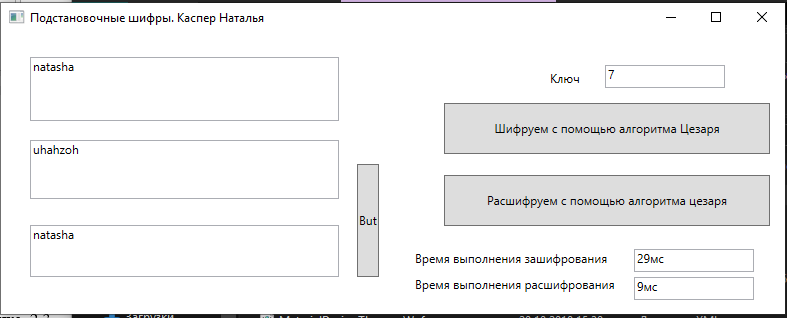


Рисунок 2.5 – Результат работы алгоритма Цезаря

Результат работы шифрования на основании алгоритма Трисемуса представлен на рисунке 2.6.

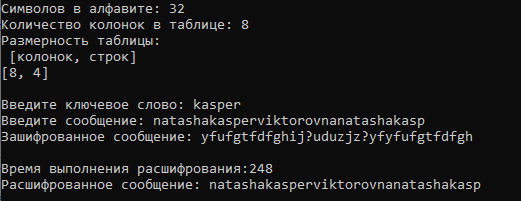


Рисунок 2.6 – Результат работы приложения

Таким образом, были реализованы все поставленные задачи.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования шифров подстановки.

Также было разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.