Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет по лабораторной работе №2**

**«Исследование криптографических шифров на основе подстановки символов»**

Выполнил:

студентка 3 курса 2 группы

Черноок Ю. С.

Проверил:

ассистент

Копыток Д. В.

Минск 2021

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

**Теоретическая часть**

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. Если исходить из того, что используемые алфавиты являются конечными множествами, то в общем случае каждой букве ax алфавита AM (ax∈ AM) для создания сообщения Мi (Мi∈ M) соответствует буква ay или множество букв {АxC} для создания шифртекста Сi (Сi∈ С). Важно, чтобы во втором случае любые два множества (например, {АxC}b и {АxC}n, b ≠ n, 1 ≤ b, n, x, y ≤ N, N – мощность алфавита), используемые для замены разных букв открытого текста, не пересекались:

{АxC}b ∩ {АxC}n = 0.

Если в сообщении Мi содержится несколько букв ax, то каждая из них заменяется на символ ay либо на любой из символов {АxC}. За счет этого с помощью одного ключа можно сгенерировать различные Сi для одного и того же Мi. Так как множества {АxC}b и {АxC}n попарно не пересекаются, то по каждому символу Сi можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения Мi он заменяет. В силу этого открытое сообщение восстанавливается из зашифрованного однозначно. Приведенные утверждения справедливы для следующих типов подстановочных шифров:

* моноалфавитных (шифры однозначной замены или простые подстановочные);
* полиграммных;
* омофонических (однозвучные шифры или шифры многозначной замены);
* полиалфавитных.

Рассмотрим шифр Цезаря и шифр Виженера.

Шифр Цезаря. В моноалфавитных шифрах операция замены производится раздельно над каждым одиночным символом сообщения Мi. Для наглядной демонстрации шифра простой замены достаточно выписать под заданным алфавитом тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены.

Максимальное количество ключей для любого шифра этого вида не превышает N!, где N – количество символов в алфавите.

Для математического описания криптографического преобразования предполагаем, что зашифрованная буква ay (ay ∈ Сi), соответствующая символу ax(ax ∈ Мi), находится на позиции

y ≡ x + k mod N, (1)

где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите; k – ключ.

Для расшифрования сообщения Сi необходимо произвести расчеты, обратные выражению (2.1), т. е.

х ≡ у – k mod N. (2)

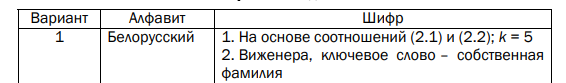
Соотношениям (1) и (2) соответствует классический шифр подстановки – шифр Цезаря. Согласно описаниям историка Светония в книге «Жизнь двенадцати цезарей», данный шифр использовался Гаем Юлием Цезарем для секретной переписки со своими генералами (I век до н. э.).

Шифр Виженера. Полиалфавитные (или многоалфавитные) шифры состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса. В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следующем. Создается таблица (таблица Виженера) размером N×N (N – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка), равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы

**Практическая часть**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции**:**

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;
* сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений**;**
* оценить время выполнения операций зашифрования/расшифрования.



Реализация шифра Виженера представлена на рисунке 1.

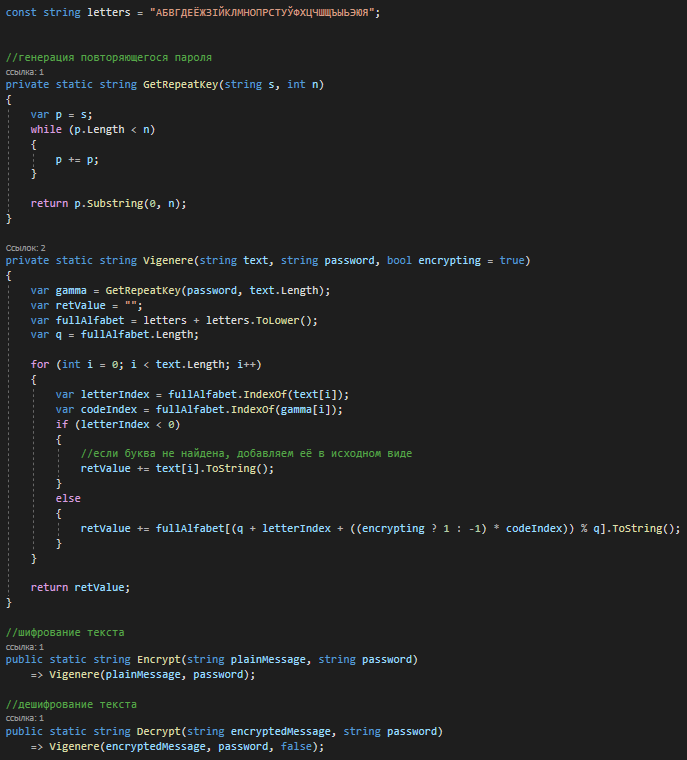


Рисунок 1 – Шифр Виженера

Реализация классического шифра Цезаря представлена на рисунке 2.

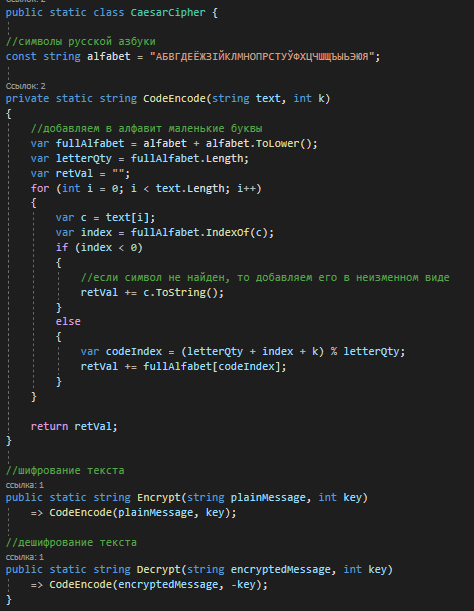


Рисунок 2 – Шифр Цезаря

Выполнение шифрования и расшифрования с помощью шифра Цезаря представлено на рисунке 3.

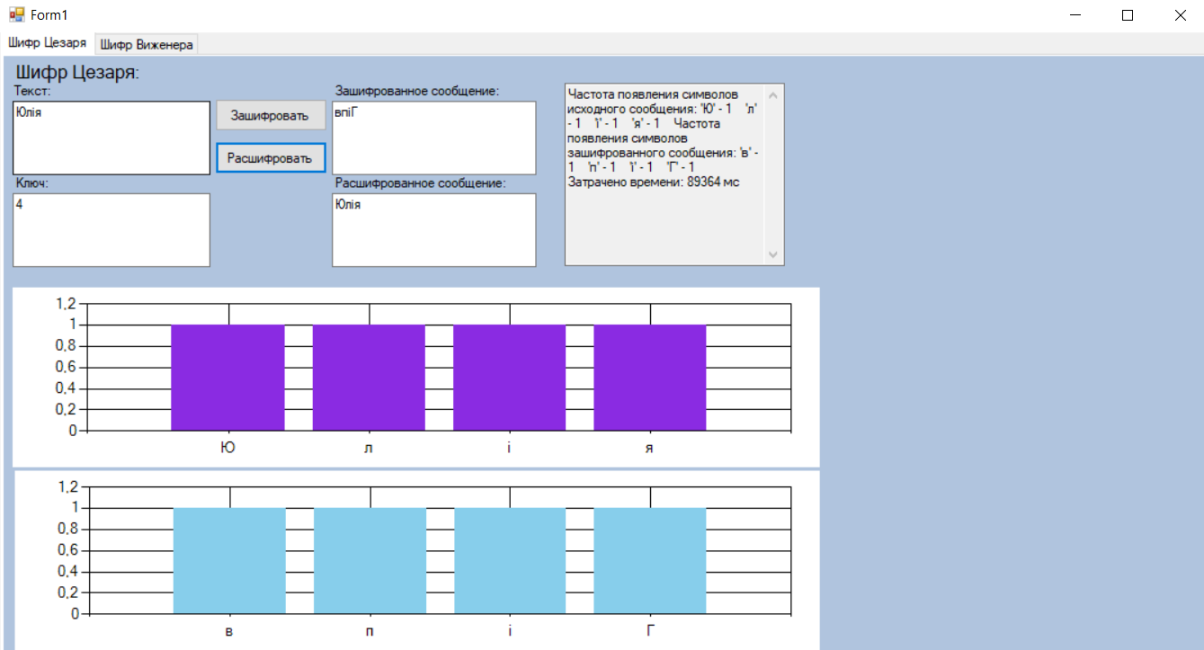


Рисунок 3 – Шифрование и расшифрование с помощью шифра Цезаря

Выполнение шифрования и расшифрования с помощью шифра Виженера представлено на рисунке 4.

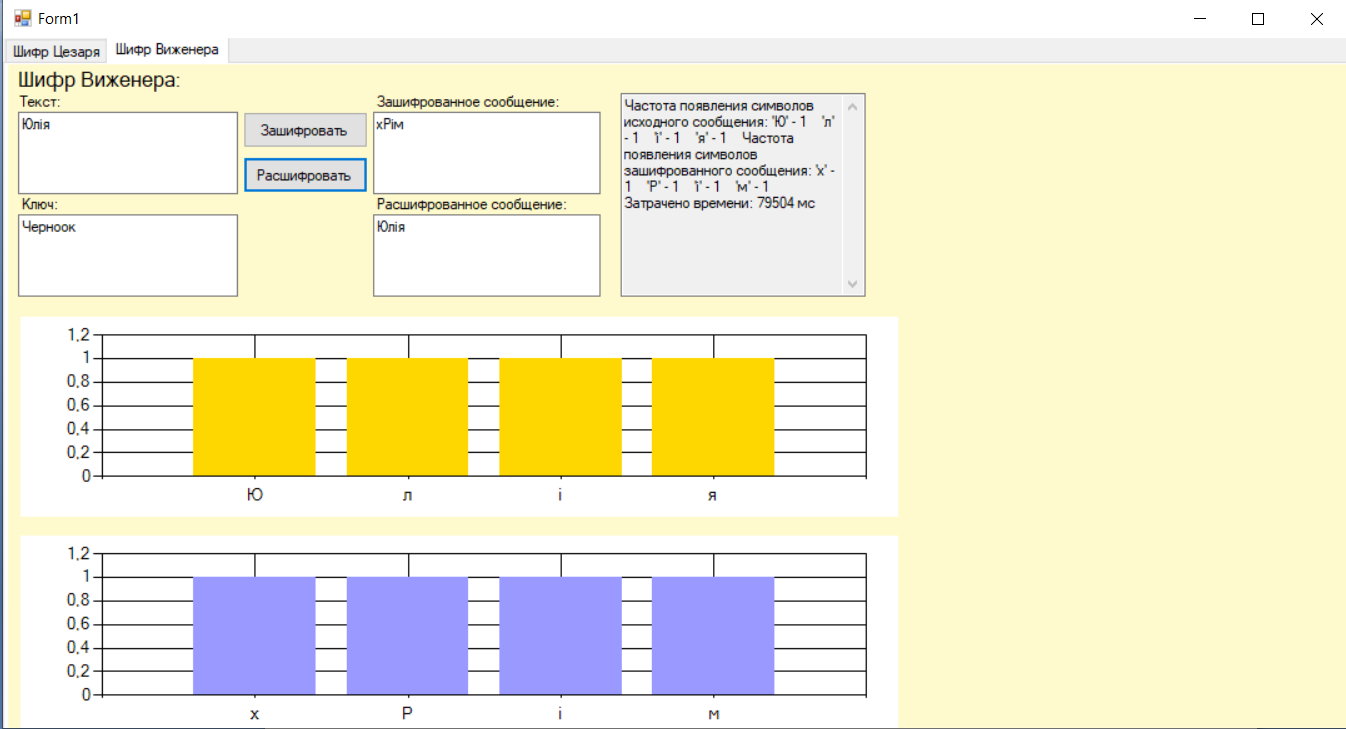


Рисунок 4 – Шифрование и расшифрование с помощью шифра Виженера

Вывод: я изучила и приобрела практические навыки разработки и использования приложений для реализации подстановочных шифров.