МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Исследование криптографических шифров на основе подстановки(замены) символов»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

**1) Шифрование текста на основе соотношений с *k***

Для шифрования текста простой заменой мы используем формулу:

(1.1)

Где *x* – позиция символа в алфавите до замены, *k* – число смещения,   
*N* – число элементов в алфавите. Реализация данной формулы в разработанной программе имеет следующий вид:

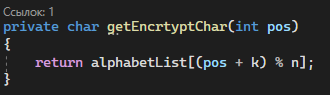


Рисунок 1.1 – Функция нахождения нового символа

Функция принимает индекс позиции элемента и возвращает новый символ. Для расшифрования сообщения необходимо коэффициент сдвига, которые далее подставляется в формулу:

(1.2)

Реализация данной формулы в программе имеет следующий вид:

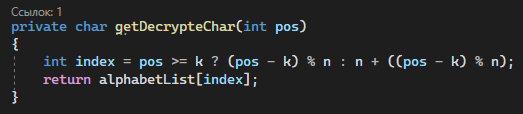


Рисунок 1.2 – Функция нахождения исходного символа

**2) Шифрование текста с помощью таблицы Трисемуса с ключевым словом**

Для шифрования текста таким путём, требуется составить саму таблицу учитывая ключевое слово. Сначала мы записываем ключевое слово, а далее все символы алфавита, которые ранее не повторялись. Далее для каждого последующего символа мы сдвигаем таблицу на 1 символ.

Функция, шифрующая текст путем таблицы Трисемуса выглядит следующим образом:

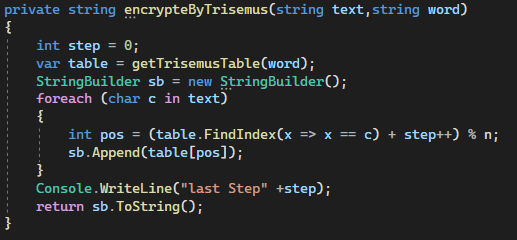


Рисунок 2.1 – Функция, шифрующая через таблицу Трисемуса

Функция принимает текст, который надо зашифровать и ключевое слово для таблицы Трисемуса. Сначала рассчитывается сама таблица, а далее вычисляется новый элемент. Функция, вычисляющая таблицу, выглядит следующим образом:

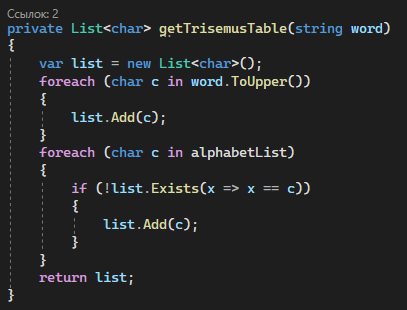


Рисунок 2.2 – Функция для расчета таблицы Трисемуса

Для расшифровки текста используется функция обратной предыдущей.

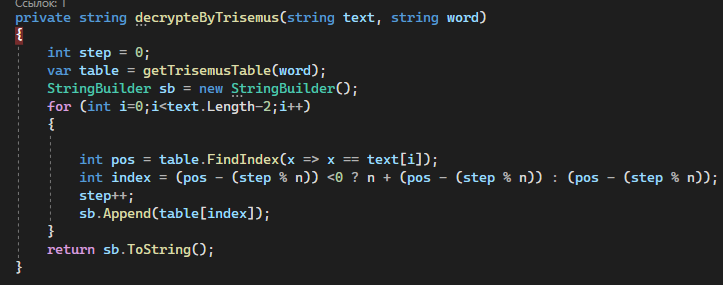


Рисунок 2.2 – Функция для расшифровки текста методом таблицы Трисемуса

**3) Сформировать гистограммы частот появления символов для исходного и зашифрованного сообщения**

Оба методы шифрования информации применяются к единому тексту, следовательно гистограмма частот появления символов, так же будет едина.

Рисунок 3.1 – Гистограмма для входного текста

Гистограмма частот появления символов для зашифрованного сообщения методом смещения выглядит похоже с гистограммой исходного текста. Единственное отличие это сдвиг символов на 7.

Рисунок 3.2 – Гистограмма для зашированного сообщения путем сдвига

Однако частота появления символов, в зашифрованом сообщении, с помощью таблицы Трисемуса, находится на одном уровне.

Рисунок 3.3 – Гистограмма для зашифрованного сообщения через таблицу Трисемуса

**4) Оценить время выполнения операций зашифрования и расшифрования**

Шифрования методом сдвига исходного текста длинной 5000 символов занимает в среднем менее 80 мс, в то время как расшифрования сообщения такой же длинны занимает около 85 мс. А вот шифрование с помощью таблицы Трисемуса занимает больше времени, а именно около 95 мс. Расшифровка сообщение тем же путем занимает около 105 мс. На это влияет то, что для шифрования сообщения с помощью таблицы Трисемуса, требуется рассчитать алфавит для определенного ключевого слова.

График времени шифрования и дешифрование методом сдвига выглядит следующим образом:

Рисунок 4.1 – График время выполнения шифрования методом сдвига

График времени шифрования и дешифрование методом таблицы Трисемуса выглядит следующим образом:

Рисунок 4.2 – График время выполнения шифрования таблицой Трисемуса

**Вывод**

При выполнении лабораторной работы были закреплены знания по алгебраическому описанию и реализацией операция шифрования и расшифрования и оценке криптостойкости подстановочных шрифтов.