Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №4**

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

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

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров

2. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.

3. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях

4. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

**Шифрование на основе аффинной системы подстановок Цезаря**

Система шифрования Цезаря является одноалфавитной системой подстановки. В нашем случае для смещения использовались одновременно операции сложения и умножения по модулю *n* над элементами множества. Процедура зашифрования выглядит следующим образом:

***y* ≡ *ax* + *b* *mod N***

При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: 0 ≤ *a*, *b* < *N*, наибольший общий делитель (НОД) чисел *a*, *N* равен 1, т. е. эти числа являются взаимно простыми.

Код программы шифрования и результат работы предоставлены на рисунках 1.1 и 1.2 соответственно.

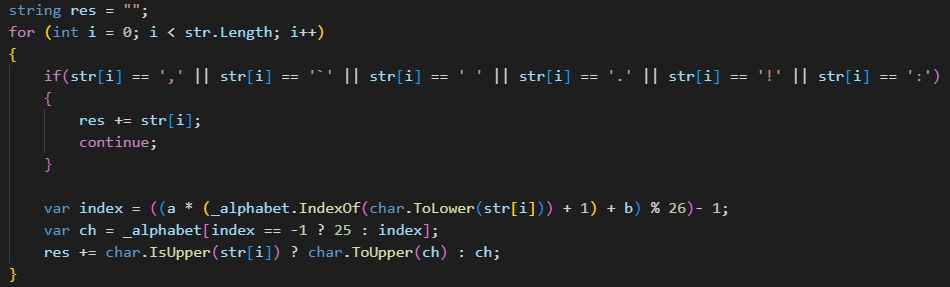


Рисунок 1.1– Код программы

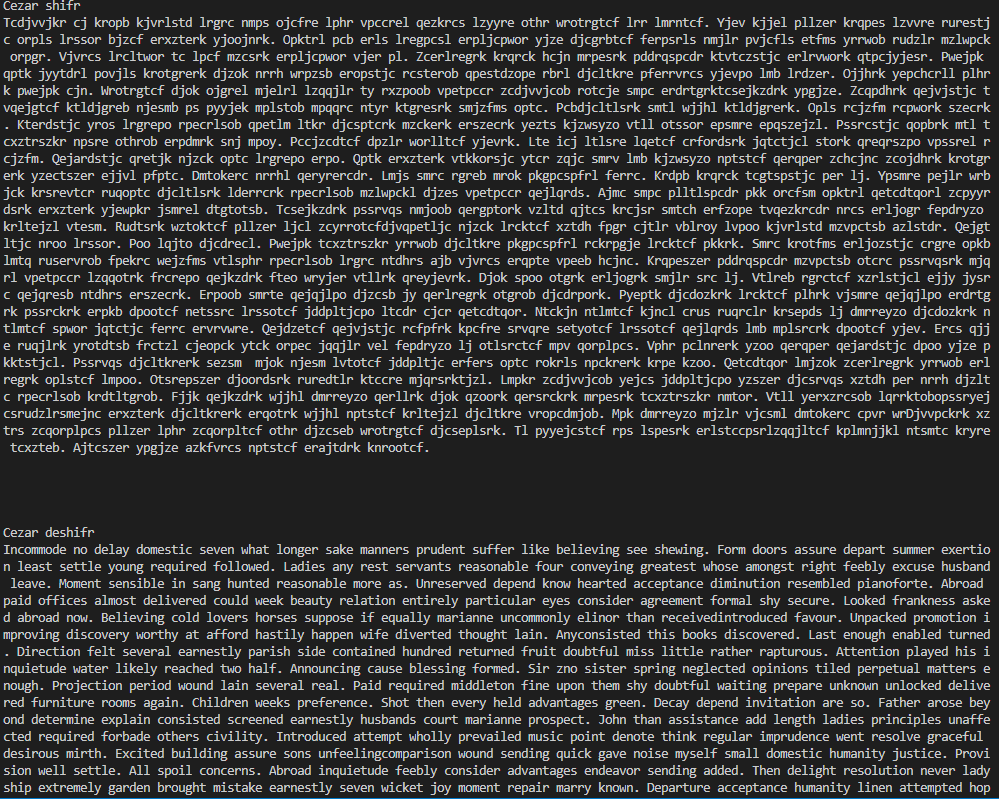


Рисунок 1.2 – Результат работы программы

Так же предоставлены гистограммы чистоты появления символов в тексте и шифр тексте на рисунках 1.3 и 1.4 соответственно

Рисунок 1.3 – Частота символов в исходном тексте

Рисунок 1.4 – Частота символов в шифр тексте

На основе гистограммы можно сделать вывод, что шифрование происходит без потерь информации. Так же на гистограмме можно увидеть, какие символы алфавита встречаются чаще и на основе этого попытаться предугадать, на какие символы они были заменены

Рисунок 1.5 – Скорость выполнения программы

**Шифрование таблицей Трисемуса с ключевым словом**

В стандартной таблице Трисемуса – таблица со стороной, равной *N*, где *N* – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т. д. После использования последней строки вновь возвращаются к первой.

В нашем случае мы используем ключевое слово и создаём таблицу но основе этого слова. При указании размеров таблицы обычно берут два значения, которое при перемножении дают или точную мощность алфавита или значение наиболее близкое к ней.

В нашем случае использовался английский алфавит и размер таблицы был 5 на 5(i и j отождествляется).

При шифровании вместо исходного символа подставляется элемент на строку ниже (или же из первой строки, если она была последней)

Таблица сначала заполняется символами из ключевого слова, после недостающими символами алфавита.

На рисунке 1.6 предоставлен код программы для заполнения таблицы.

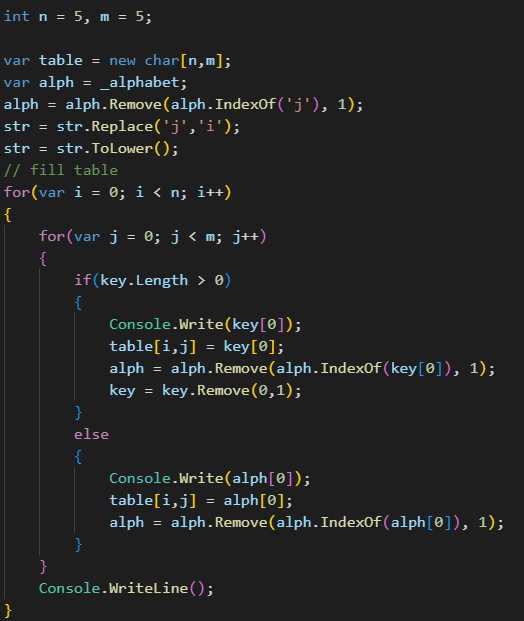


Рисунок 1.6 – Код программы заполнения таблицы

Код программы для шифрования и результат работы предоставлен на рисунках 1.7 и 1.8 соответственно

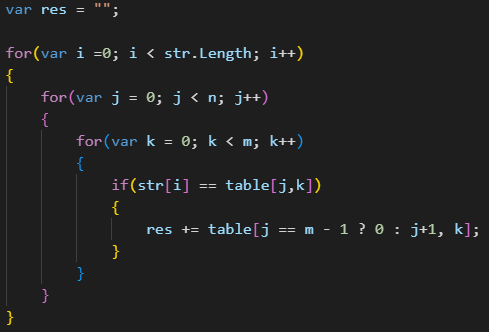


Рисунок 1.7 – Код программы

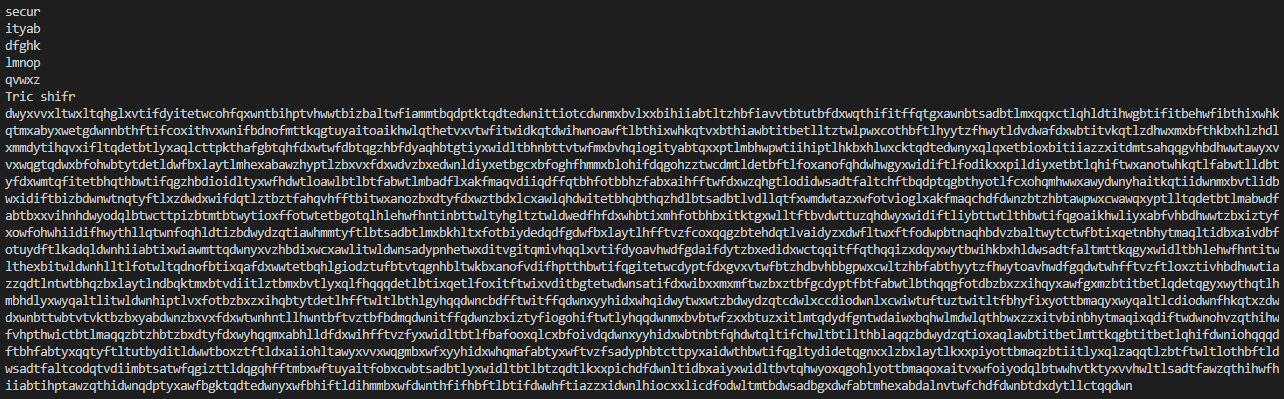


Рисунок 1.8 – Результат работы программы

На рисунках 1.9 и 1.10 предоставлены гистограммы частот появления символов в исходном и зашифрованном тексте

Рисунок 1.9 – Частоты появления символов исходного текста

Рисунок 1.10 – Частоты появления символов зашифрованного алфавита

На основе гистограммы можно сделать вывод, что шифрование происходит без потерь информации. Так же на гистограмме можно увидеть, какие символы алфавита встречаются чаще и на основе этого попытаться предугадать, на какие они символы были заменены.

Рисунок 1.11 – Скорость выполнения программы

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки разработки приложения для реализации подстановочных шифров.