1. Цель

Вариант 17. Реализовать алгоритм шифрования при помощи моноалфавитной подстановки. Провести его частотный анализ. Найти расстояние единственности.

2. Описание алгоритма

Шифр моноалфавитной подстановки

Ключом шифрования при использовании моноалфавитного подстановочного шифра является таблица замены. Для шифрования каждого символа открытого текста находится соответствующий символ в таблице и записывается в качестве шифртекста.

3. Описание реализации

При запуске программа составляет ключ, длина которого равна мощности алфавита используемого текста (которая известна заранее), и записывает его в файл.

В режиме шифрования программа посимвольно считывает входной текст из файла, после чего, используя ключ-таблицу, посимвольно создает новый текст.

Режим дешифрования аналогичен режиму шифрования, с той лишь разницей, что поиск символов по ключу происходит в обратном порядке.

4. Примеры

После запуска программы был сгенерирован и записан в файл key.txt ключ, представленный на рисунке 1.

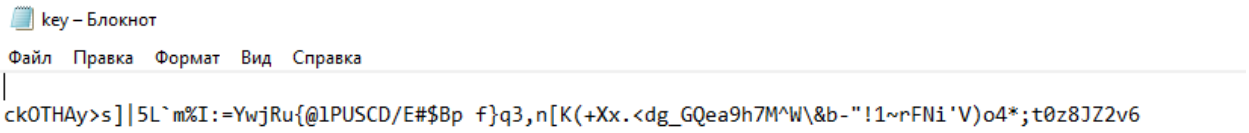

Рисунок 1

Зашифруем содержимое файла text.txt, которое можно увидеть на рисунке 2.

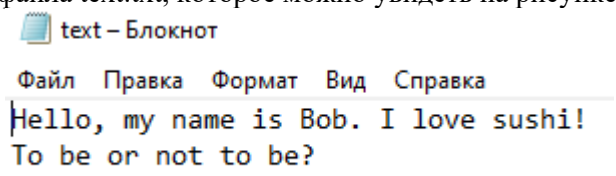

Рисунок 2

Полученный шифртекст записан в файл cryptoText.txt (рисунок 3).

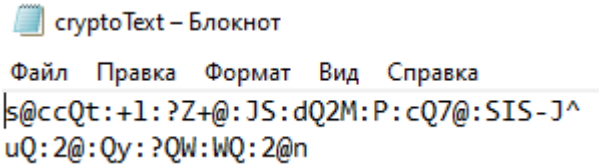

Рисунок 3

Расшифруем полученный текст и запишем результат в файл decryptoText.txt (рисунок 4).

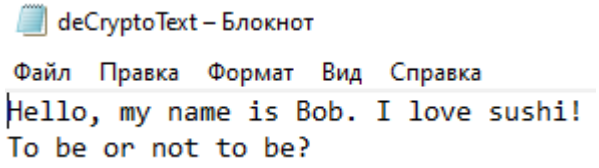

Рисунок 4

Таким образом, программа показала ожидаемые результаты, следовательно, её работа корректна

На рисунке 5 представлено расстояние единственности и частотный анализ изначального текста

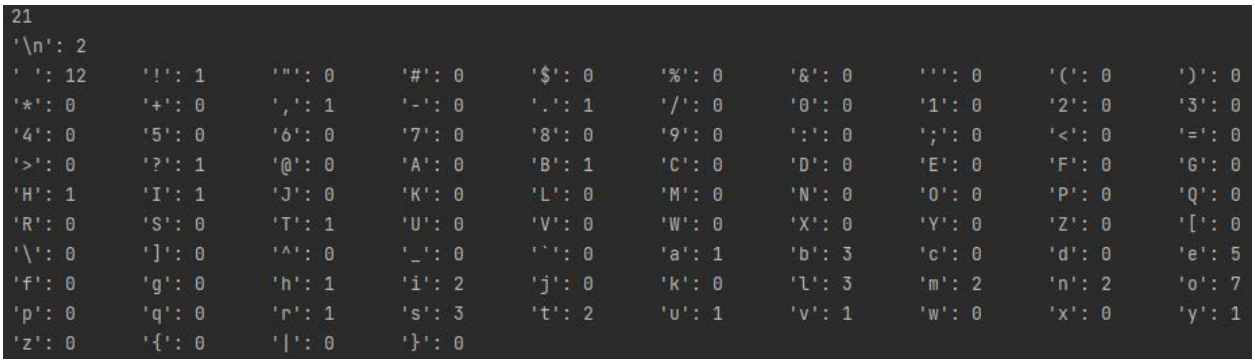

Рисунок 5

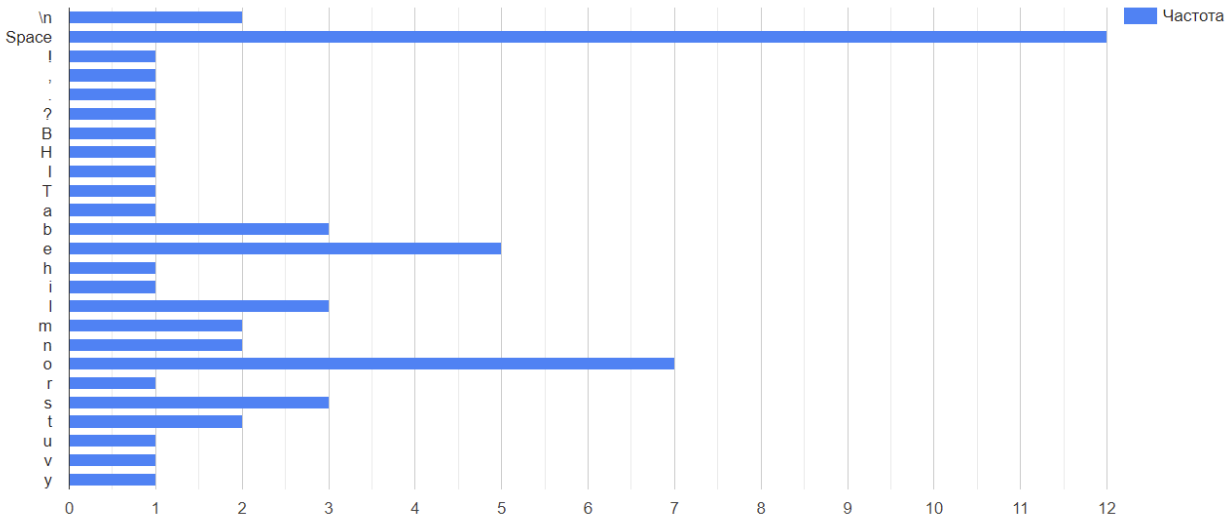

Рисунок 6 – частотный анализ в графическом представлении

5. Вывод

Шифр моноалфавитной подстановки довольно легко расшифровать без знания ключа – с помощью частотного анализа шифртекста, что делает его применение неэффективным в большинстве случаев.

Но есть оговорка: частотный анализ хорошо работает на больших текстах. Если текст маленький или очень специфический по используемым словам, то частотность букв будет отличаться от эталонной по языку, и времени на разгадывание придётся потратить гораздо больше.

6. Список литературы

[1] А. А. Овчинников, Основы информационной безопасности. Исторические шифры, Санкт-Петербург : Редакционно-издательский центр ГУАП, 2018.

[2] Р. Чёрчхаус, Коды и шифры. Юлий Цезарь, "Энигма" и Интернет, Весь мир, 2005.