

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № 9**

на тему «Использование классических криптоалгоритмов подстановки и

перестановки для защиты текстовой информации»

Выполнил обучающийся гр. ВКБ42

Михайлов А.С.

Проверил:

Доцент к.т.н Сафарьян О.А.

Ростов-на-Дону

2024

**Цель работы:** Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

**Выполнение работы:**

1. Одноалфавитный метод с фиксированным смещением.

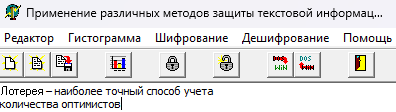


Рисунок 1 – Исходный текст

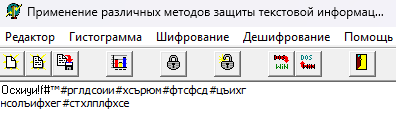


Рисунок 2 – Зашифрованный текст

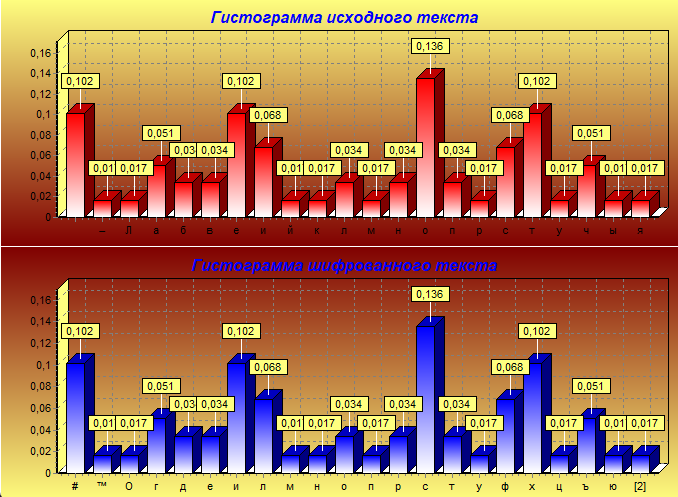


Рисунок 3 – Гистограммы исходного и шифрованного текста

Верхняя гистограмма состоит из данных об исходном тексте. В ней указаны встречающиеся символы, и частота встречаемости каждого. Аналогичные данные показаны в нижней гистограмме, но для зашифрованного текста. При таком методе шифрования частота встречаемости символа исходного текста и зашифрованного символа будет одинаковая. Зная смещение, можно расшифровать зашифрованный текст.

Берём самый часто встречающийся символ из гистограммы шифрованного текста: 0,136 = “о” и самый часто встречающийся символ из гистограммы исходного текста: 0,136 = “с”. Возьмём коды символов из ASCII таблицы. “о” = 238, “с” = 241. Вычислим смещение символов с помощью вычитания кодов: 232 – 229 = 3. Смещение равно 3 это значит, что все остальные символы в шифрованном файле сдвинуты на 3 позиции.

1. Одноалфавитный метод с задаваемым смещением (шифр Цезаря)

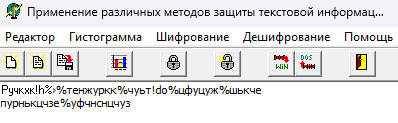


Рисунок 4 – Зашифрованный текст

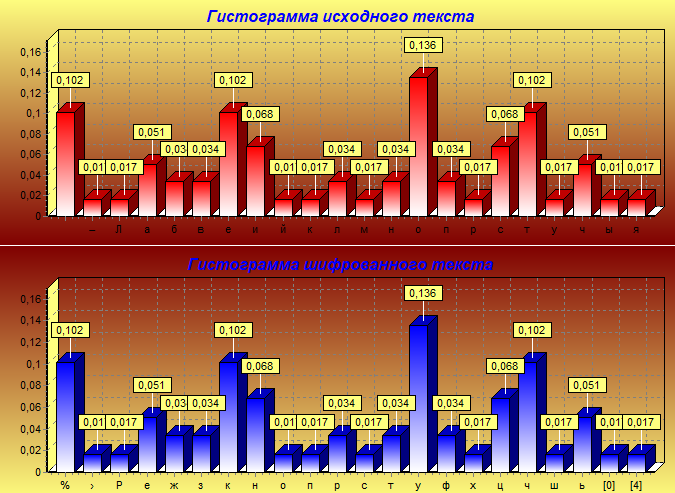


Рисунок 5 – Гистограмма исходного и шифрованного текста

Берём самый часто встречающийся символ из гистограммы шифрованного текста: 0,136 = “о” и самый часто встречающийся символ из гистограммы исходного текста: 0,136 = “у”. Возьмём коды символов из ASCII таблицы. “о” = 238, “у” = 243. Вычислим смещение символов с помощью вычитания кодов: 232 – 229 = 5. Смещение равно 5 это значит, что все остальные символы в шифрованном файле сдвинуты на 5 позиции.

Указав данное смещение при дешифровании в программе, получим исходный текст:

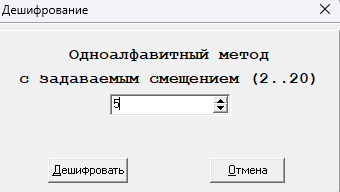


Рисунок 6 – Задание смещения

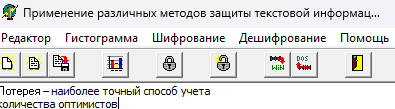


Рисунок 7 - Дешифрованное сообщение

1. Перестановка символов

Произведём шифрование исходного текста следующим ключом:

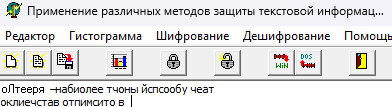


Рисунок 8 - Зашифрованный текст

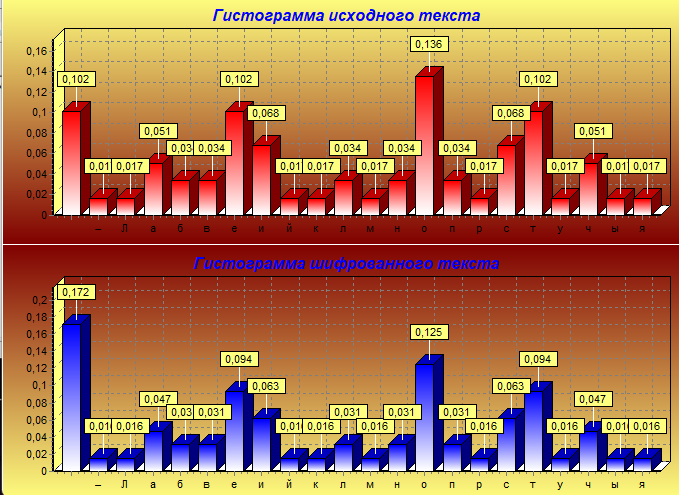


Рисунок 9 – Гистограмма исходного и зашифрованного текста

Гистограммы не совпадают значит количество символов не является кратным длине ключа. Это происходит из-за добавления в конец недостающих для кратности пробелов. Гистограмма не содержит полезной информации для дешифрования, т.к. данный метод основан на перестановке символов, следовательно, частота появления отдельных символов совпадает.

Дешифрование происходит по блокам текстам равным длине ключа. Для ключа длиной 4 берём первые 4 символа “оЛте”. Сравнив с первыми 4 символа исходного текста определим правило смещения: и – 2 находится на первой позиции, М – 1 находится на второй позиции, х – 3 находится на третьей позиции и а – 4 находится на четвёртой позиции. Следовательно, можем составить правило перестановки равное 2314. Применим это правила перестановки к остальным частям текста получим исходное сообщение.

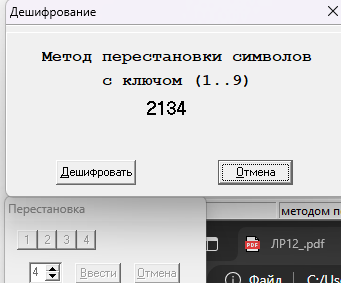


Рисунок 10 – Установка правила перестановок

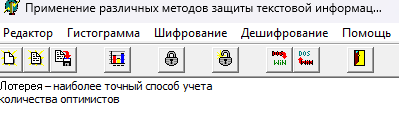


Рисунок 11 – Расшифрованный текст

1. Метод инверсивного кодирования (по дополнению до 255)

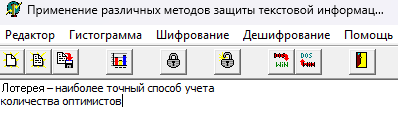


Рисунок 12 – Исходный текст

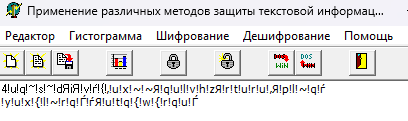


Рисунок 13 – Зашифрованный текст

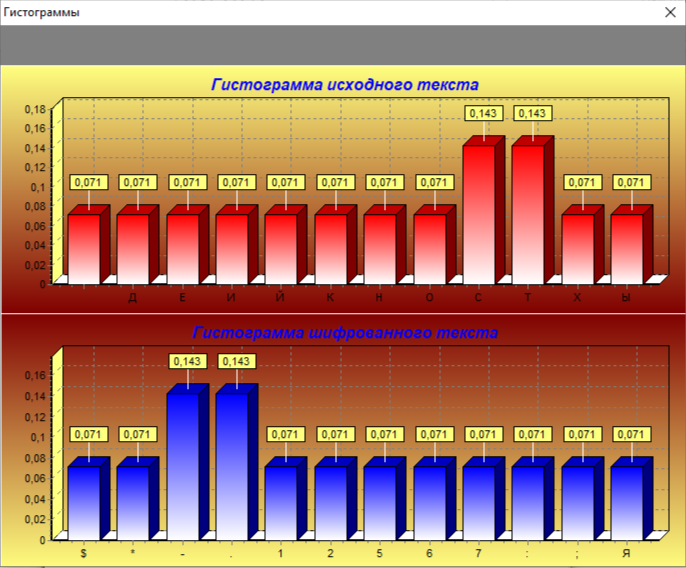


Рисунок 14 – Гистограмма исходного и шифрованного текста

Шифрование происходит путём вычитания из 255, кода в таблице ASCII текущего символа и последующей замены на новый символ, который берётся из таблицы ASCII. Дешифрования происходит тем же самым образом. Гистограмма не содержит полезной информации для дешифрования так как вся информация берётся из таблицы кодирования ASCII (в виде кодов зашифрованного и исходного сообщения). При таком методе частота встречаемости символов на обоих гистограммах будет совпадать.

Построим таблицу для дешифрования:

|  |  |
| --- | --- |
| 4!u!q!~!s!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | Расшифровка символа |
| Л!u!q!~!s!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 42 = 203 | |
| Лоu!q!~!s!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 17 = 238 | |
| Лот!q!~!s!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 13 = 242 | |
| Лоте!~!s!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 36 = 229 | |
| Лотер~!s!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 15 = 240 | |
| Лотере~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 50 = 229 | |
| Лотерея!~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 0 = 255 | |
| Лотерея ~!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 95 = 160 | |
| Лотерея -!dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 105 = 150 | |
| Лотерея - dЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 95 = 160 | |
| Лотерея - нdЯiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 18 = 237 | |
| Лотерея - наiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 53 = 202 | |
| Лотерея - наиiЯ!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 46 = 209 | |
| Лотерея - наиб!v!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255– 45 = 210 | |
| Лотерея - наибоv!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 17 = 238 | |
| Лотерея - наибол!ѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 55 = 200 | |
| Лотерея - наиболеѓ!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 55 = 200 | |
| Лотерея - наиболее!{!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 59 = 240 | |
| Лотерея – наиболее {!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 50 = 229 | |
| Лотерея – наиболее т!‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 36 = 255 | |
| Лотерея – наиболее то‚!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 54 = 160 | |
| Лотерея – наиболее точ!u!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 223 = 150 | |
| Лотерея – наиболее точнu!x!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 45 = 160 | |
| Лотерея – наиболее точныx!~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 55 = 200 | |
| Лотерея – наиболее точный~!~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 55 = 160 | |
| Лотерея – наиболее точный !~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 42 = 203 | |
| Лотерея – наиболее точный с~Я!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 17 = 238 | |
| Лотерея – наиболее точный спЯ!q!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u! | 255 – 13 = 242 | |
| Лотерея – наиболее точный споq!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 36 = 229 | |
| Лотерея – наиболее точный спос!u!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 15 = 240 | |
| Лотерея – наиболее точный спосоu!l!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 50 = 229 | |
| Лотерея – наиболее точный способl!v!h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 0 = 255 | |
| Лотерея – наиболее точный способ !h!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 95 = 160 | |
| Лотерея – наиболее точный способ уh!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 105 = 150 | |
| Лотерея – наиболее точный способ уч!zЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 95 = 160 | |
| Лотерея – наиболее точный способ учеЯ!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w!{!r!q!u!Ѓ | 255 – 18 = 237 | |
| Лотерея – наиболее точный способ учет!r!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 53 = 202 | |
| Лотерея – наиболее точный способ учетаr!t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 55 = 203 | |
| Лотерея – наиболее точный способ учета t!u!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 46 = 238 | |
| Лотерея – наиболее точный способ учета кu!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 42 = 242 | |
| Лотерея – наиболее точный способ учета коu!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 49 = 229 | |
| Лотерея – наиболее точный способ учета кол!r!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 59 = 240 | |
| Лотерея – наиболее точный способ учета колиr!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 50 = 229 | |
| Лотерея – наиболее точный способ учета колич!u!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 36 = 255 | |
| Лотерея – наиболее точный способ учета количе!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 54 = 160 | |
| Лотерея – наиболее точный способ учета количес!‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 223 = 150 | |
| Лотерея – наиболее точный способ учета количест ‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 45 = 160 | |
| Лотерея – наиболее точный способ учета количеств‚Я!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 58 = 237 | |
| Лотерея – наиболее точный способ учета количества!p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 53 = 202 | |
| Лотерея – наиболее точный способ учета количества p!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 46 = 209 | |
| Лотерея – наиболее точный способ учета количества о!l!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255– 45 = 210 | |
| Лотерея – наиболее точный способ учета количества опl!~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 55 = 200 | |
| Лотерея – наиболее точный способ учета количества опт~!q!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{! | 255 – 35 = 220 | |
| Лотерея – наиболее точный способ учета количества опти!ѓ  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 55 = 200 | |
| Лотерея – наиболее точный способ учета количества оптим  !y!u!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 59 = 191 | |
| Лотерея – наиболее точный способ учета количества оптимиu!x!{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w | 255 – 50 = 205 | |
| Лотерея – наиболее точный способ учета количества оптимс{!l!~!r!q!Ѓ!ѓЯ!u!t!q!{!w! | 255 – 36 = 219 | |
| Лотерея – наиболее точный способ учета количества оптимист r!q!Ѓ!ѓЯ!u!t!q!{!w | 255 – 54 = 201 | |
| Лотерея – наиболее точный способ учета количества оптимистr!q!Ѓ!ѓЯ!u!t!q!{!w | 255 – 223 = 232 | |
| Лотерея – наиболее точный способ учета количества оптимстоu!t!q!{!w! | 255 – 45 = 210 | |
| Лотерея – наиболее точный способ учета количества оптимистов | 255 – 55 = 200 | |

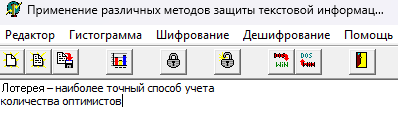


Рисунок 15 – Расшифрованный текст

1. Метод многоалфавитного шифрования с фиксированным ключом

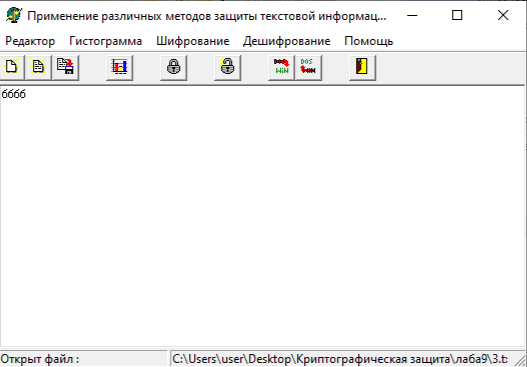


Рисунок 16 – Исходный текст

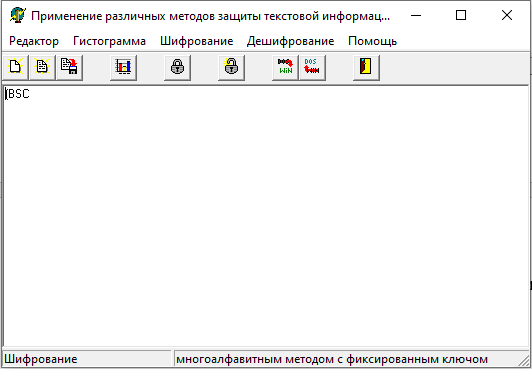


Рисунок 17 – Зашифрованный текст

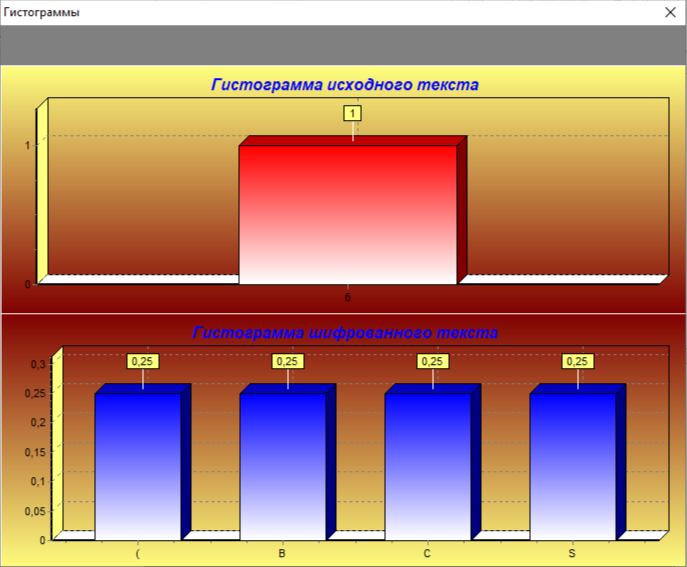


Рисунок 18 – Гистограмма исходного и зашифрованного текста

Так как используется многоалфавитный шифр то к каждому символу применяется отдельный одноалфавитный шифр, то есть разное смещение по определённому правилу.

( = 40, B = 66, C = 67, S = 83

б = 225

Для шифрования текста использовался следующий набор из 4-ёх смещений:

225 – 40 = 185

225 – 66 = 159

225 – 67 = 158

1. – 83 = 142

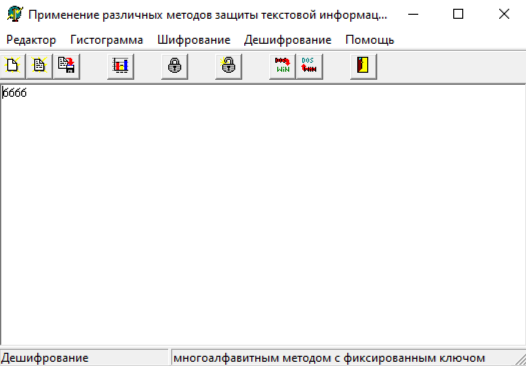


Рисунок 19 – Расшифрованный текст

1. Метод многоалфавитного шифрования с ключом фиксированной длины

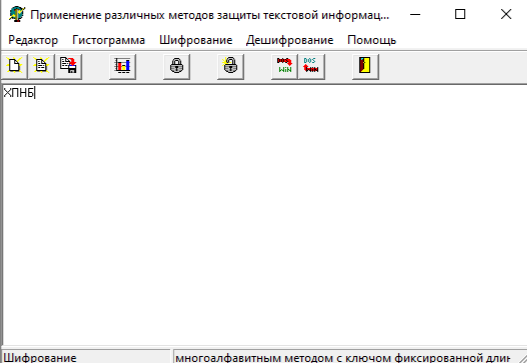


Рисунок 20 – Зашифрованный текст

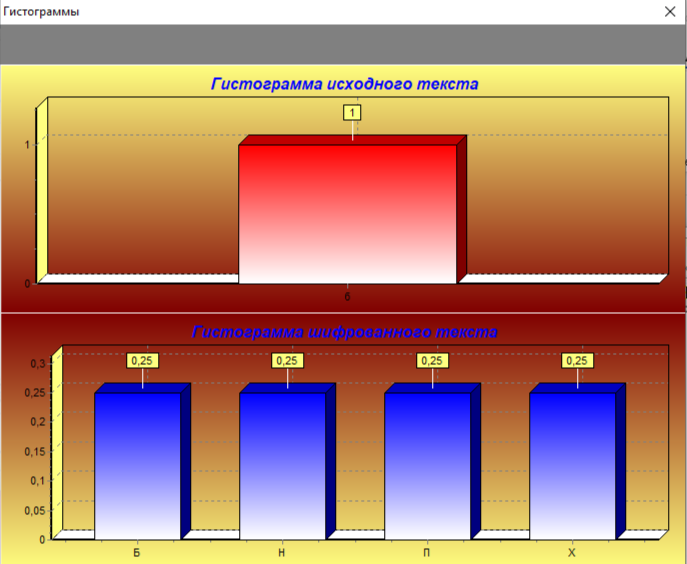


Рисунок 21 – Гистограмма исходного и шифрованного текста

По гистограмме можно определить длину ключа, которым зашифровывался исходный текст. Она соответствует кол-ву символов на гистограмме зашифрованного текста. В данном случае использовался ключ длиной в 4 символа.

Для шифрования используется формула Тш = (То + Тг) mod K, где– зашифрованный символ,– шифруемый символ (исход.),– задаваемая последовательность,– кол-во символов в алфавите.

б = 225

ф = 244, о = 238, м = 236, а = 224

X = 213, П = 207, Н = 205, Б = 193

(225 + 244) mod 256 = 213

(225 + 238) mod 256 = 207

(225 + 236) mod 256 = 205

(225 + 224) mod 256 = 193

Для расшифрования:

(213 - 244) mod 256 = 225

(207 - 238) mod 256 = 225

(205 - 236) mod 256 = 225

(193 - 224) mod 256 = 225

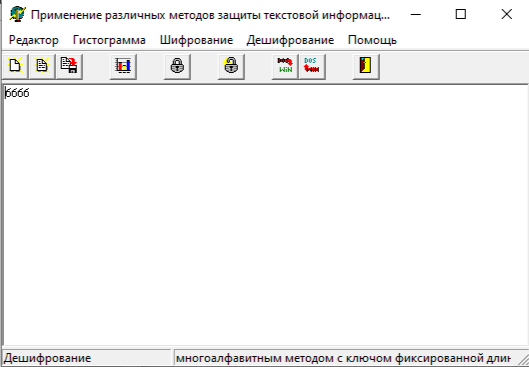


Рисунок 22 – Расшифрованный текст

1. Метод многоалфавитного шифрования с произвольным паролем

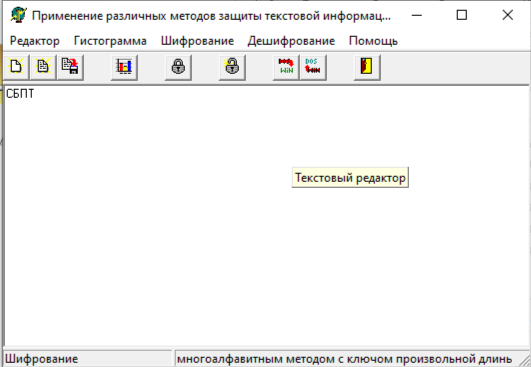


Рисунок 23 – Зашифрованный текст

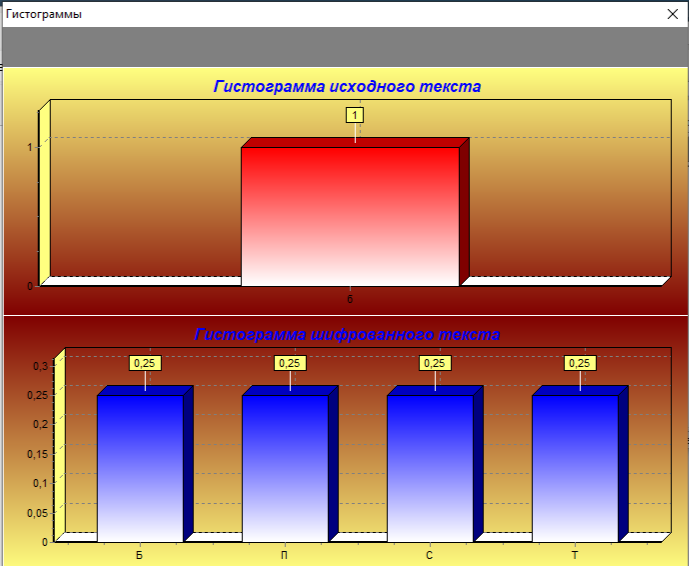


Рисунок 24 – Гистограмма исходного и шифрованного текста

б = 225

р = 240, а = 224, о = 238, с = 241

С = 209, Б = 193, П = 207, Т = 210

(225 + 240) mod 256 = 209

(225 + 224) mod 256 = 193

(225 + 238) mod 256 = 207

(225 + 241) mod 256 = 210

Для расшифрования:

(209 - 240) mod 256 = 225

(193 - 224) mod 256 = 225

(207 - 238) mod 256 = 225

(210 - 241) mod 256 = 225

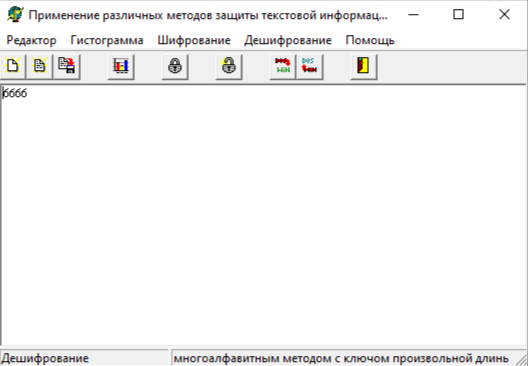


Рисунок 25 – Расшифрованный текст