

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

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

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Отчет**

**Лабораторная работа №9 по дисциплине «Методы и средства криптографической защиты»**

Выполнил:   
обучающийся гр. ВКБ41

Ушаков М.А.

Проверила:   
 Сафарьян Ольга Александровна

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ростов-на-Дону

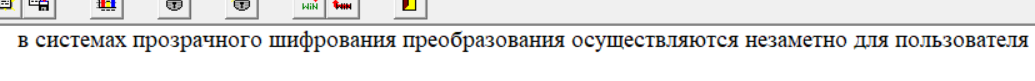
2024

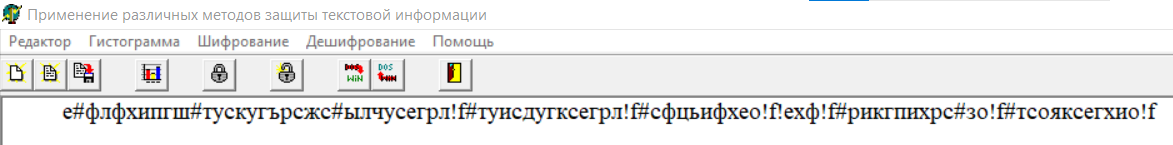
**Лабораторная работа №9**

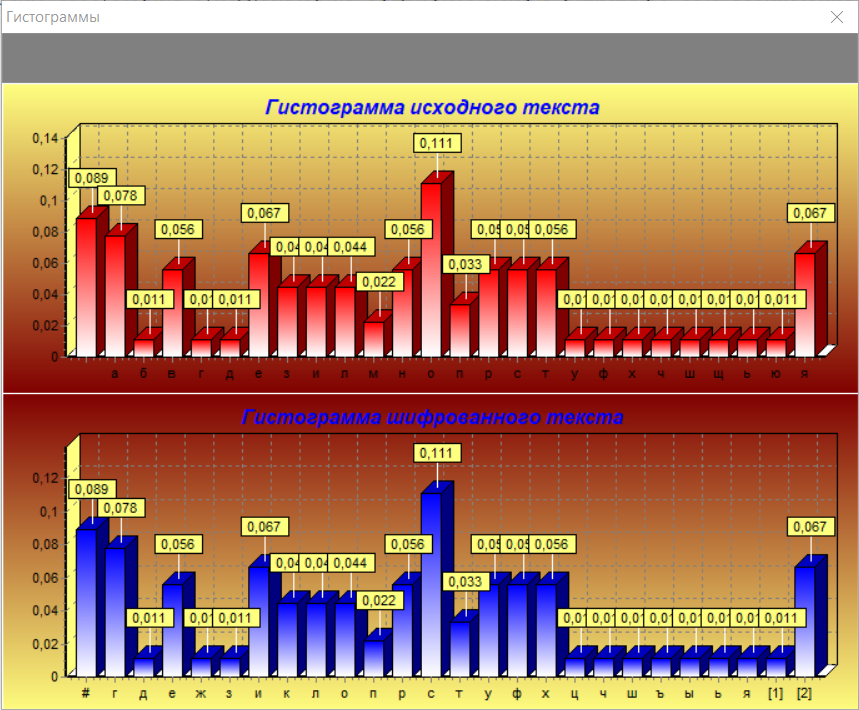
**Цель работы:** Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

**1.Одноалфавитный метод с фиксированным смещением.**

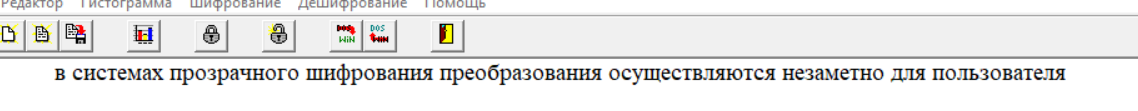
В системах прозрачного шифрования преобразования осуществляются незаметно для пользователя







Верхняя(красная) гистограмма указывает символы, встречающиеся в исходном тексте и соответствующую частоту. Аналогично построена нижняя (синяя) гистограмма по шифртексту. В данном методе частота появления символов в ОТ и соответствующих символов в ШТ будут одинаковы. Благодаря этому можно легко определить шаг смещения и расшифровать текст.



Для определения смещения выделим наиболее часто встречающийся символ шифрованного текста. Найдем символ с той же частотой встречаемости на гистограмме исходного текста. Переведем символы в ASCII-кодировку и определим смещение, посчитав разность между шифрованным символом и исходным.

Гистограмма очень упрощает задачу. Мы видим, что шифрованный символ находится прямо под исходным символом.

Чаще всего встречаемые символы

о = 0,111 а = 0,078 е = 0,067 в ОТ

с = 0,111 г = 0,078 и = 0,067 в ШТ

|  |  |  |
| --- | --- | --- |
| о | а | е |
| 238 | 224 | 229 |
| с | г | и |
| 241 | 227 | 232 |

241 – 238 = 3

227 – 224 = 3

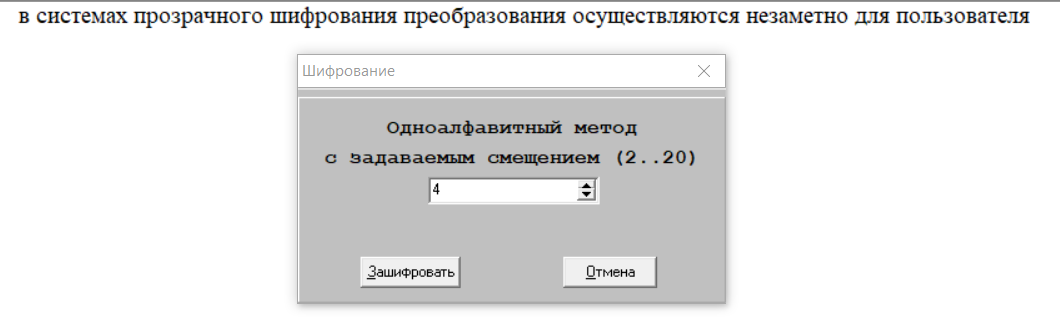
232 – 229 = 3 те– смещение на 3 символа

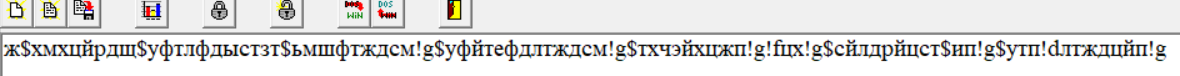
Ручная проверка

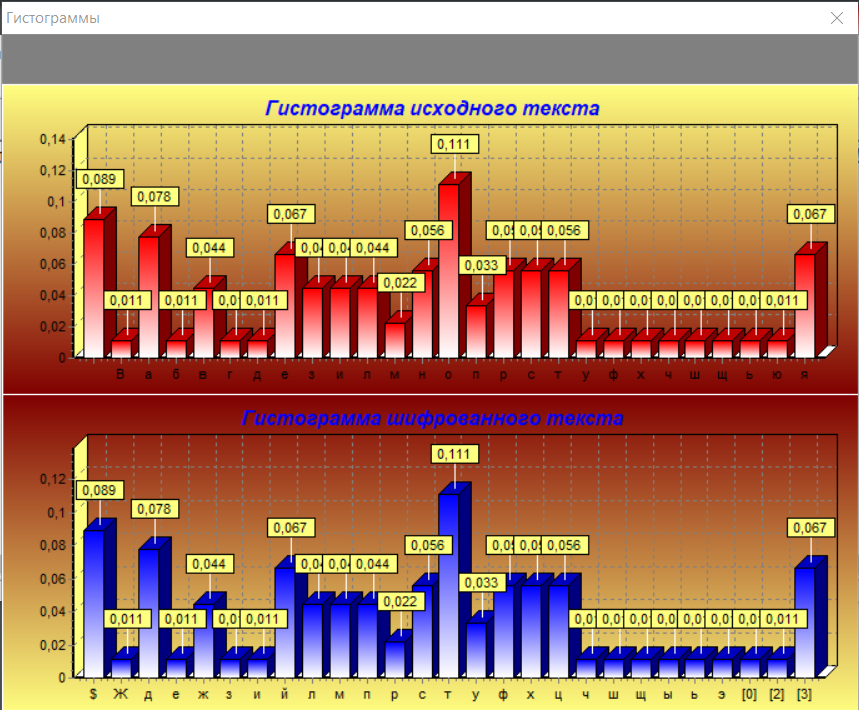
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| в | \_ | с | и | с | т | е | м | а | х | \_ | п | р | о | з | р | а | ч | н | о | г | о | \_ | ш | и | ф | р | о | в | а | н | и |
| 226 | 32 | 241 | 232 | 241 | 242 | 229 | 236 | 224 | 245 | 32 | 239 | 240 | 238 | 231 | 240 | 224 | 247 | 237 | 238 | 227 | 238 | 32 | 248 | 232 | 244 | 240 | 238 | 226 | 224 | 237 | 232 |
| е | # | ф | л | ф | х | и | п | г | ш | # | т | у | с | к | у | г | ъ | р | с | ж | с | # | ы | л | щ | у | с | е | г | р | л |
| 229 | 35 | 244 | 235 | 244 | 245 | 232 | 239 | 227 | 248 | 35 | 242 | 243 | 241 | 234 | 243 | 227 | 250 | 240 | 241 | 230 | 241 | 35 | 251 | 235 | 247 | 243 | 241 | 229 | 227 | 240 | 235 |

**2.Одноалфавитный метод с задаваемым смещением (шифр Цезаря).**

Выполним шифрования на 4 позиции.







Самые частые символы на гистограммах являются:

ОТ p(**о)** = 0,111 ; p(\_) = 0.089 ; p(а) = 0.078 ; p(е) = 0.067

ШТ p(**т) =** 0,111; p($) = 0.089 ; p(д) = 0.078 ; p(й) = 0.067

В таблице ASCII

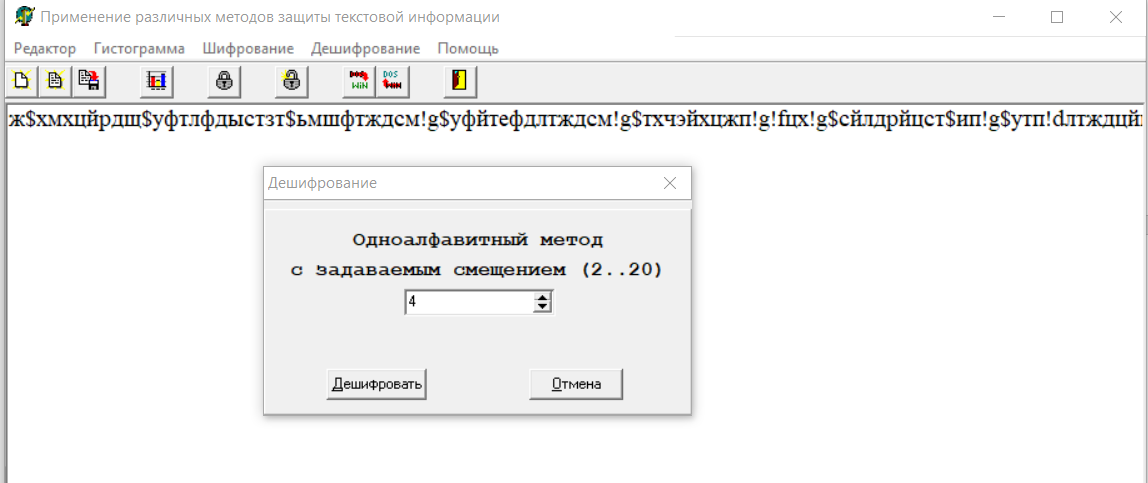
|  |  |  |  |
| --- | --- | --- | --- |
| о | а | е | \_ |
| 238 | 224 | 229 | 32 |
| т | д | й | $ |
| 242 | 228 | 233 | 36 |

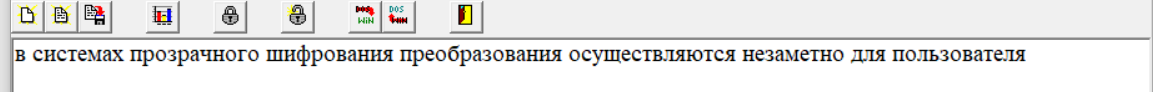
242 – 238 = 4 36 – 32 = 4

228 – 224 = 4

233 – 229 = 4  
 - Смещение было совершено на **4** шага

Дешифрование с помощью программы



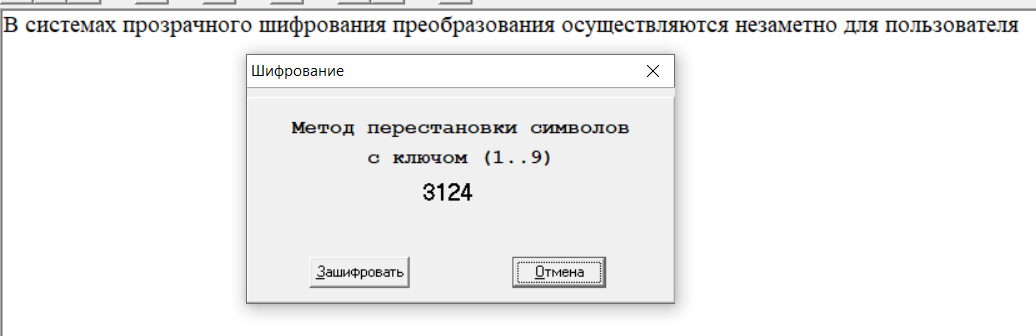


Ручная проверка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| в | \_ | с | и | с | т | е | м | а | х | \_ | п | р | о | з | р | а | ч | н | о | г | о | \_ | ш | и | ф | р | о | в | а | н | и | я |
| 226 | 32 | 241 | 232 | 241 | 242 | 229 | 236 | 224 | 245 | 32 | 239 | 240 | 238 | 231 | 240 | 224 | 247 | 237 | 238 | 227 | 238 | 32 | 248 | 232 | 244 | 240 | 238 | 226 | 224 | 237 | 232 | 255 |
| ж | $ | х | м | х | ц | й | р | д | щ | $ | у | ф | т | л | ф | д | ы | с | т | з | т | $ | ь | м | ш | ф | т | ж | д | с | м |  |
| 230 | 36 | 245 | 236 | 245 | 246 | 233 | 250 | 228 | 249 | 36 | 243 | 244 | 242 | 235 | 244 | 228 | 251 | 241 | 242 | 231 | 242 | 36 | 252 | 236 | 248 | 244 | 242 | 230 | 228 | 241 | 236 |  |

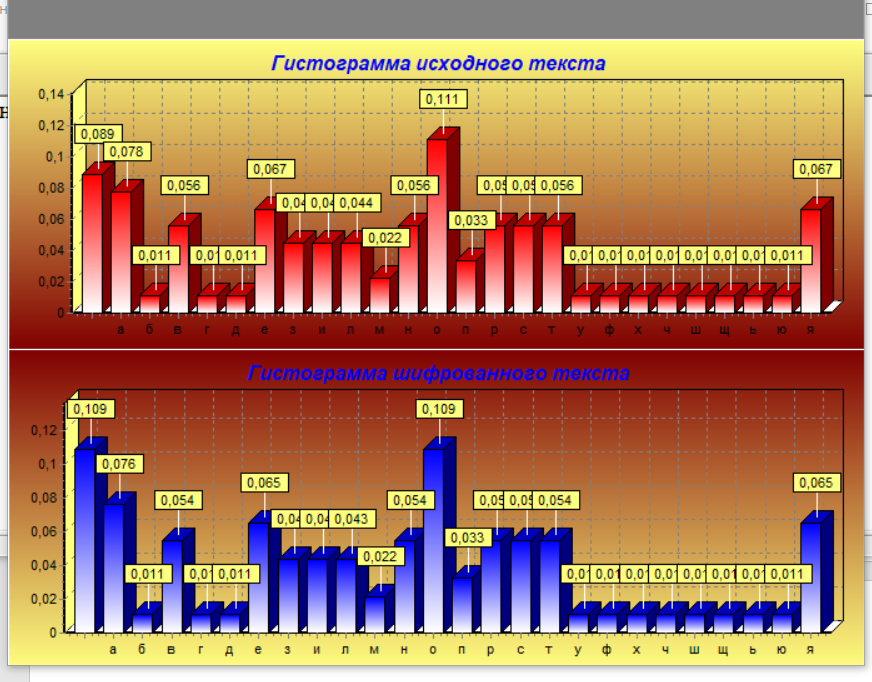
**3.Метод перестановки символов.**

Идея метода состоит в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного текста.

****

****

Гистограмма исходного и зашифрованного текста



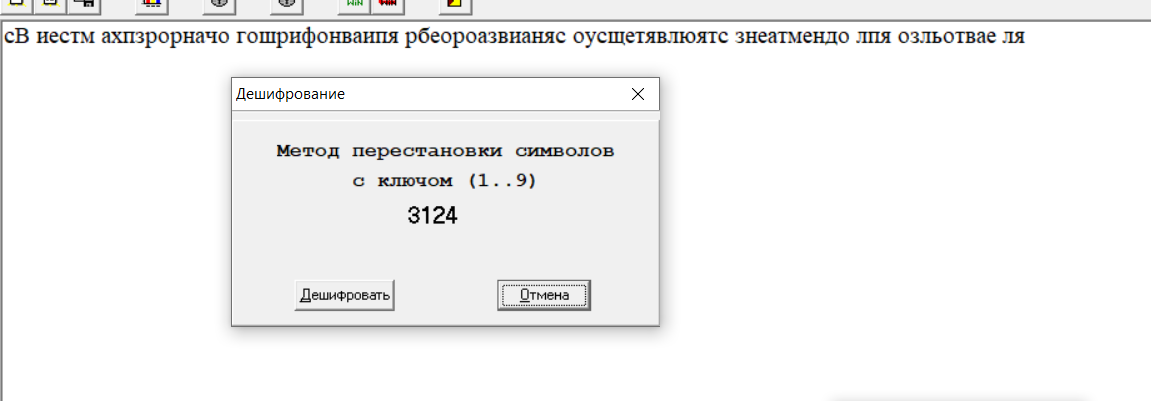
Если количество символов исходного текста кратно длине ключа, то гистограммы совпадут, иначе – не совпадут, т.к. в конце исходного текста добавляются недостающие для кратности ‘ ’ (пробелы). Гистограмма не содержит полезной информации для дешифрования, т.к. данный метод основан на перестановке символов, следовательно, частота появления отдельных символов совпадает.

Процесс дешифрования вручную. Длина ключа равна 4, значит берем из шифрованного текста блок размером в 4 символа и выполняем над ним следующие действия: берем символ с номером, соответствующим номеру первой позиции ключа (символ с номером 4), и помещаем его в первую позицию расшифрованного текста. Далее делает то же самое с символом, соответствующим номеру второй позиции, затем – третьей, после чего переходим к дешифрованию следующего блока.

В системах прозрачного шифрования преобразования осуществляются незаметно для пользователя

сВ иестм ахпзрорначо гошрифонваипя рбеороазвианяс оусщетявлюятс знеатмендо лпя озльотвае ля

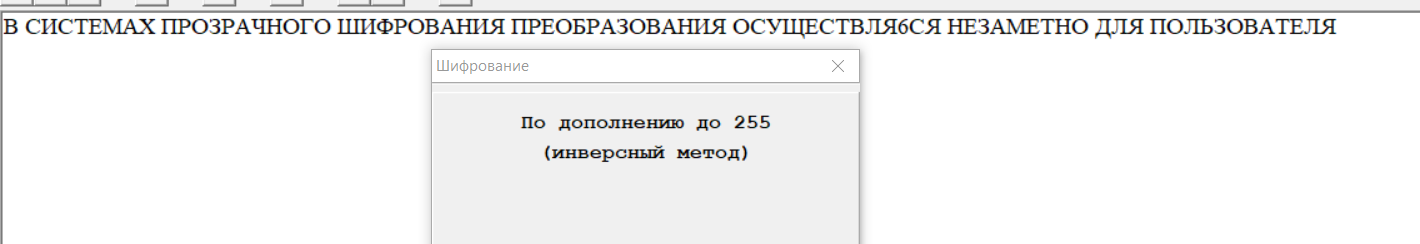
Дешифрование с помощью программы.

****

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| в | \_ | с | и | с | т | е | м | а | х | \_ | п | р | о | з | р | а | ч | н | о | г | о | \_ | ш | и | ф | р | о | в | а | н | и |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 |
| c | в |  | и | е | с | т | м |  | а | х | п | з | р | о | р | н | а | ч | о |  | г | о | н | р | и | ф | р | н | в | а | и |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| в | \_ | с | и | с | т | е | м | а | х | \_ | п | р | о | з | р | а | ч | н | о | г | о | \_ | ш | и | ф | р | о | в | а | н | и |

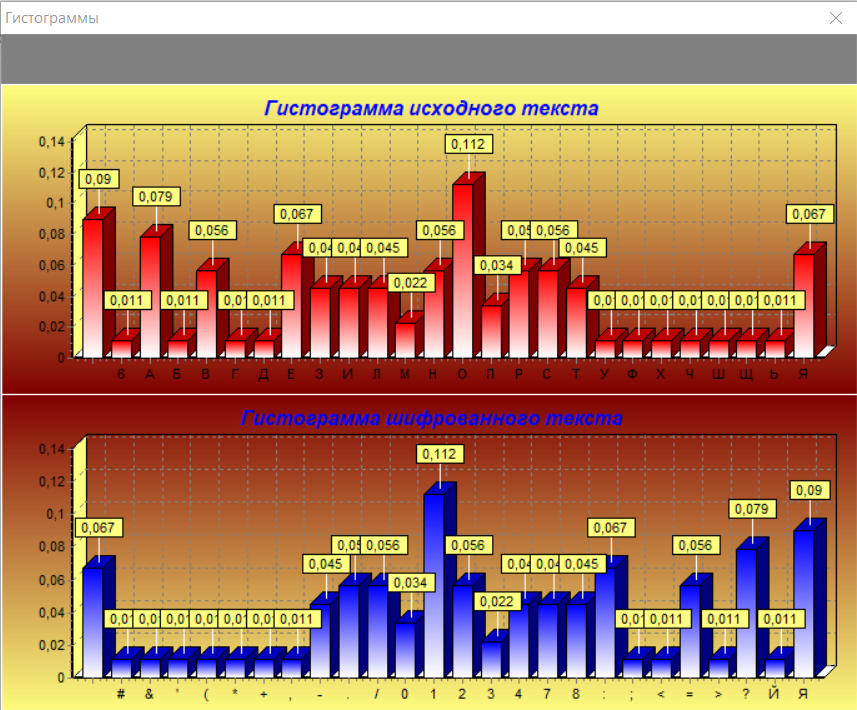
**4.Метод инверсного кодирования (по дополнению до 255).**

Данный метод шифрования является частным случаем одноалфавитной замены в алфавите мощности 256. Суть метода заключается в замене символа ASCII-кодировки с номером i на символ с номером 255 –i.





|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| в | \_ | с | и | с | т | е | м | а | х | \_ | п | р | о | з | р | а | ч | н | о | г | о | \_ | ш | и | ф | р | о | в | а | н | и | я |
| 194 | 32 | 209 | 200 | 209 | 210 | 197 | 204 | 192 | 213 | 32 | 207 | 208 | 206 | 199 | 208 | 194 | 215 | 205 | 206 | 195 | 206 | 32 | 216 | 200 | 212 | 208 | 206 | 194 | 192 | 205 | 200 | 223 |
| = | Я | . | 7 | . | - | : | 3 | ? | \* | Я | 0 | / | 1 | 8 | / | ? | ( | 2 | 1 | < | 1 | Я | ‘ | 7 | + | / | 1 | = | ? | 2 | 7 |  |
| 61 | 223 | 46 | 55 | 46 | 45 | 58 | 51 | 63 | 42 | 223 | 48 | 47 | 49 | 56 | 47 | 63 | 40 | 50 | 49 | 60 | 49 | 223 | 44 | 55 | 43 | 47 | 49 | 61 | 63 | 50 | 55 | 32 |





Расшифруем несколько символом вручную:

=Я.7.-:3?\*

1 =Я.7.-:3?\*(255 – 61) = 194 В

2 ВЯ.7.-:3?\* **(**255-223)=32 « »

3 В .7.-:3?\*(255 - 46) = 209 С

4 В С7.-:3?\* (255 - 55) = 200 И

5 В СИ.-:3?\* (255-46) = 209 С

6 В СИС-:3?\* (255 – 45) = 210 Т

7 В СИСТ:3?\* (255 - 58) = 197 Е

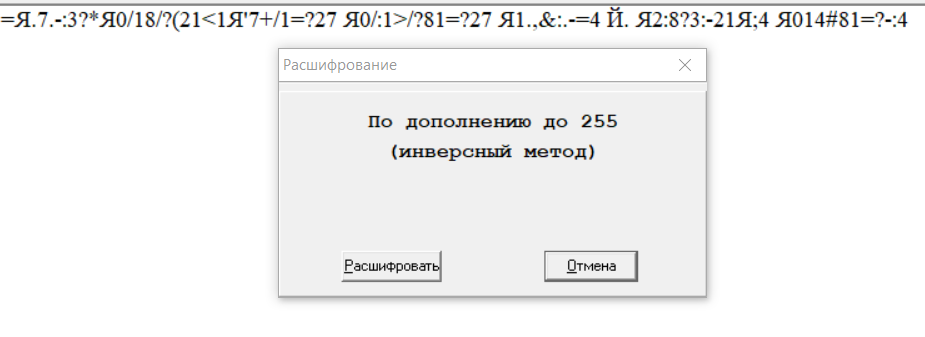
8 В СИСТЕ3?\* (255 - 51) = 204 М

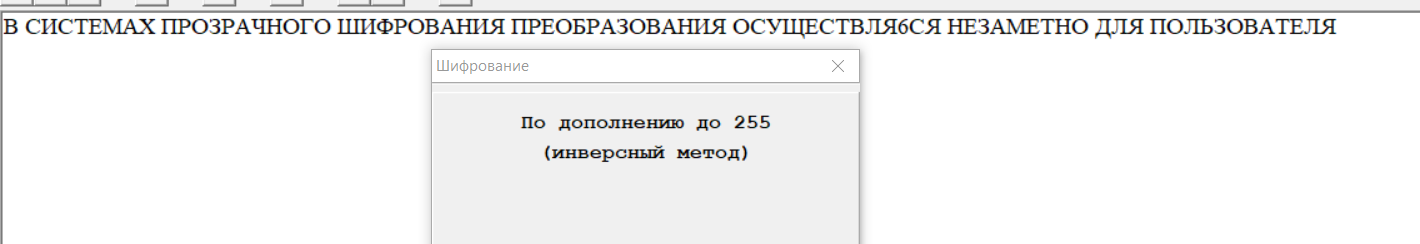
9 В СИСТЕМ?\* (255 - 63) = 192 А

10 В СИСТЕМА\* (255 - 42) = 213 Х

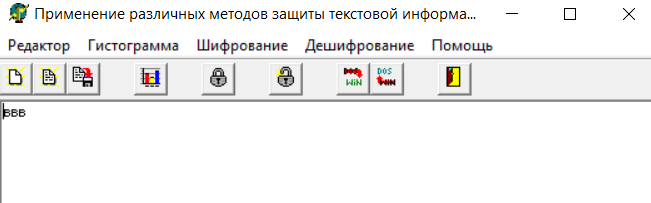
… … …

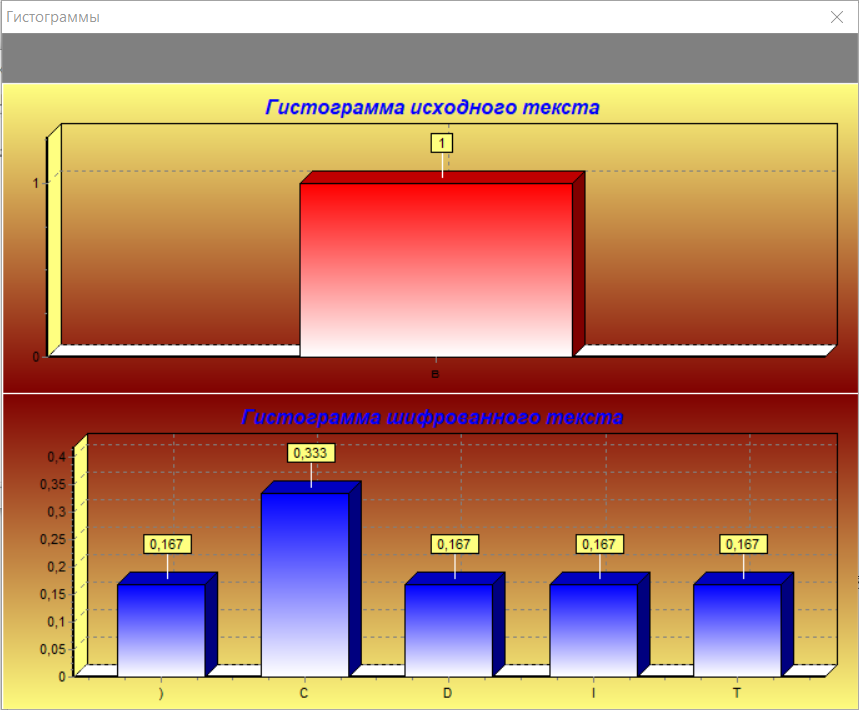
n В СИСТЕМАХ ПРОЗРАЧНОГО ШИФРОВАНИЯ ПРЕОБРАЗОВАНИЯ ОСУЩЕСТВЛЯЮТСЯ НЕЗАМЕТНО ДЛЯ ПОЛЬЗОВАТЕЛЯ





**5.Метод многоалфавитного шифрования с фиксированным ключом.**

****



|  |  |  |
| --- | --- | --- |
| в | в | в |
| 226 | 226 | 226 |
| ) | C | T |
| 41 | 67 | 84 |
|  |  |  |

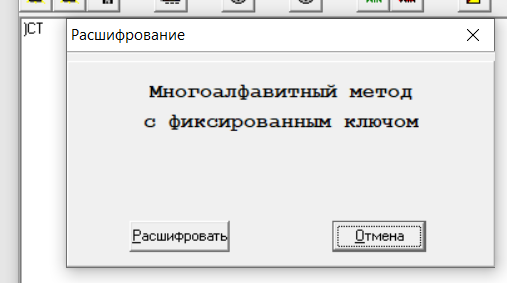
)CT; ) = 41 C = 67 T = 84 **в** =226

226 – 41=185

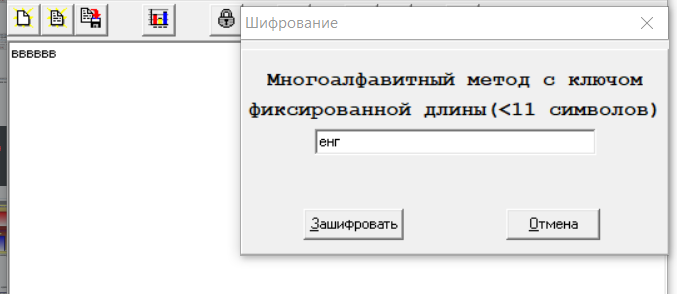
226 – 67= 159

226 – 84 = 142

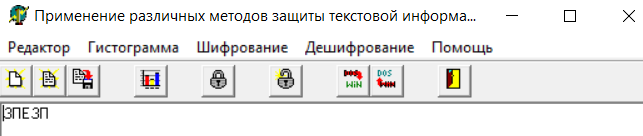
Для шифрования последовательности из одинаковых символов используется набор из 3-х смещений, те отдельное смещение для каждого символа

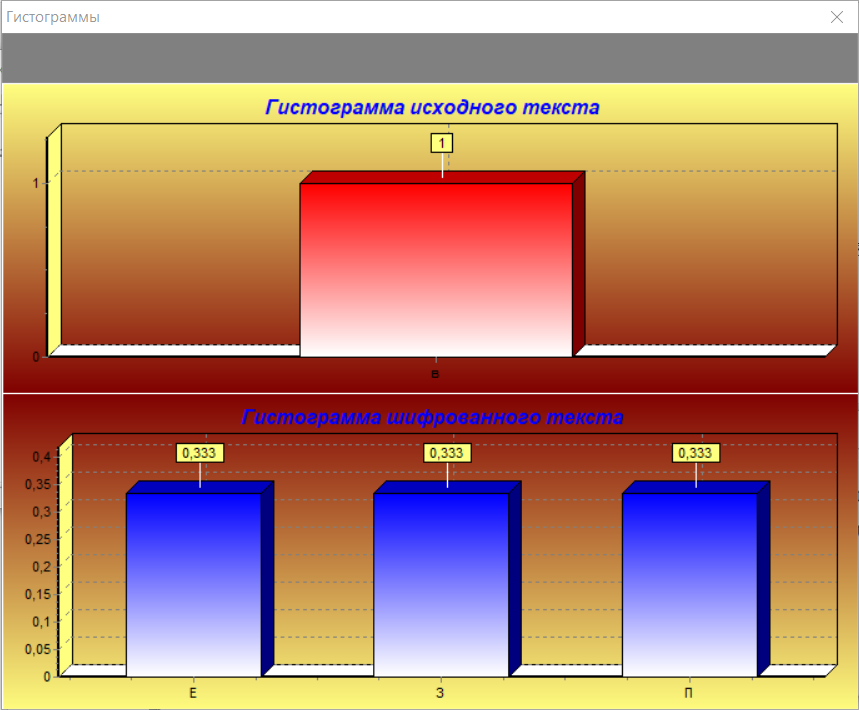
****

**6.Метод многоалфавитного шифрования с ключом фиксированной длины.**



до 11 элементов





Гистограмма исходного и зашифрованного текстов. 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 3 символа.

Перевод символов с помощью ASCII таблицы

|  |  |  |
| --- | --- | --- |
| в | в | в |
| 226 | 226 | 226 |
| е | н | г |
| 229 | 237 | 227 |
| З | П | Е |
| 199 | 207 | 197 |

Исход. символ: в=226;

Ключ:

е=229

н=237

г=227;

Символы ШТ:

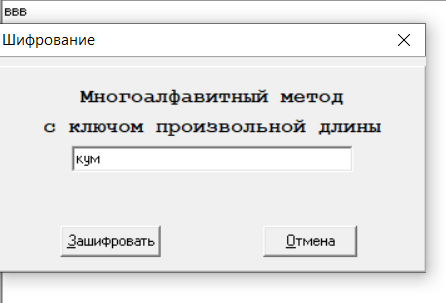
Е = 197 З = 199 П = 207

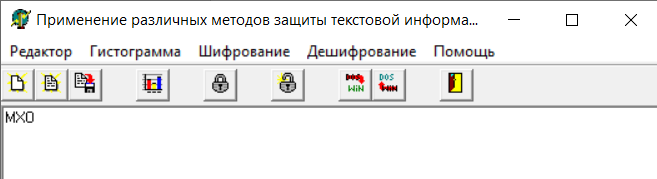
(226 + 229)mod 256 = 455 mod 256=199

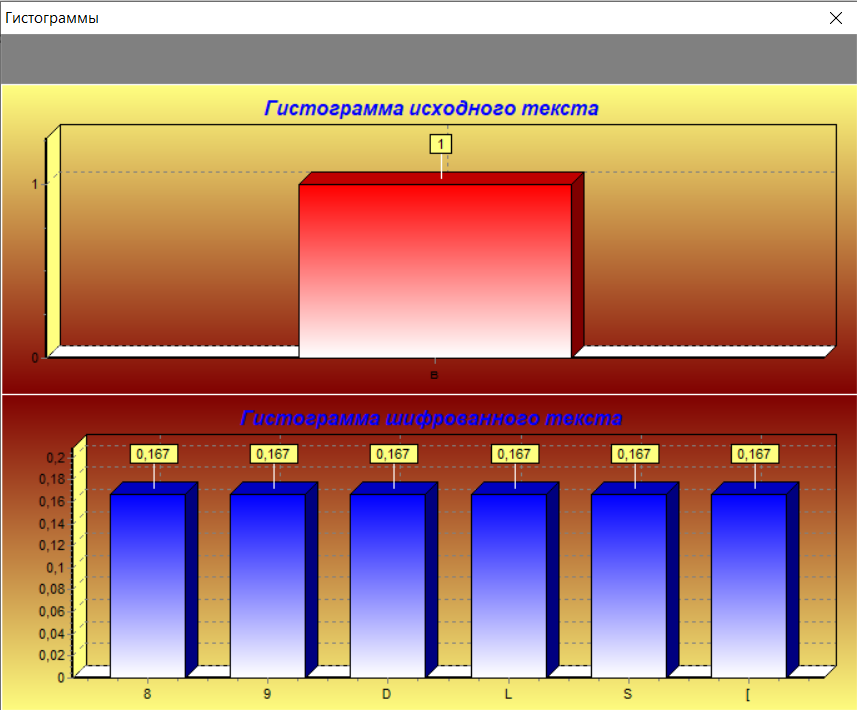
(226 + 237)mod 256 = 463 mod 256=207

(226 + 227)mod 256 = 453 mod 256=197

**7. Многоалфавитное шифрование с произвольным паролем.**







Исход. символ: в=226

Тш=(Т₀+Тг)mod K, где Тш – зашифрованный символ, Т₀ – шифруемый символ (исход.), Тг – задаваемая гамма посл-ть, K– кол-во символов в алфавите(256)

|  |  |  |
| --- | --- | --- |
| в | в | в |
| 226 | 226 | 226 |
| к | у | м |
| 234 | 243 | 236 |
| М | Х | О |
| 204 | 213 | 206 |

Ключ: к = 234 у = 243 м = 236

Получаем МХО

М = 204

Х = 213

О = 206

(226 + 234)mod 256=460 mod 256 =204 M

(226 + 243)mod 256= 469 mod 256 =213 X

(226 + 236)mod 256= 462 mod 256 =206 O

**Вывод:** в ходе выполнения данной лабораторной работы были изучены простые классические криптографические алгоритмы моноалфавитной подстановки и перестановки для защиты текстовой информации. К ним относятся: одноалфавитный метод с фиксированным смещением, одноалфавитный метод с задаваемым смещением, метод перестановки символов, метод инверсного кодирования (по дополнению до 255). Зашифровать и расшифровать текст, а также гистограммы (их делала программа),отображающие частоту встречаемости символов в тексте, удалось с помощью программы “L\_lux”.