**ЛАБОРАТОРНАЯ РАБОТА 1**

**ИСПОЛЬЗОВАНИЕ КЛАССИЧЕСКИХ КРИПТОАЛГОРИТМОВ**

**ПОДСТАНОВКИ И ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ**

**ТЕКСТОВОЙ ИНФОРМАЦИИ**

**Выполнил Студент группы БИВТ-23-6**

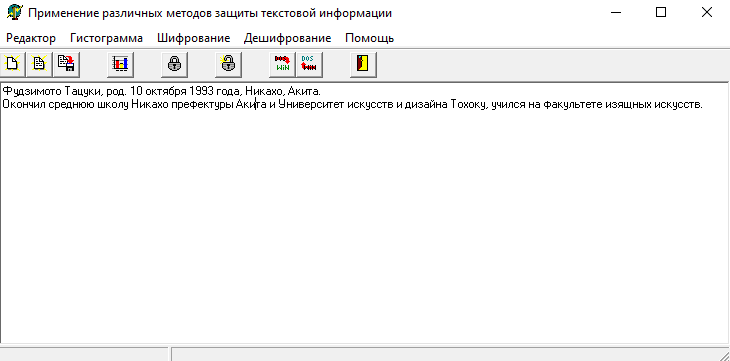
**Малютин Александр**

Задание 2

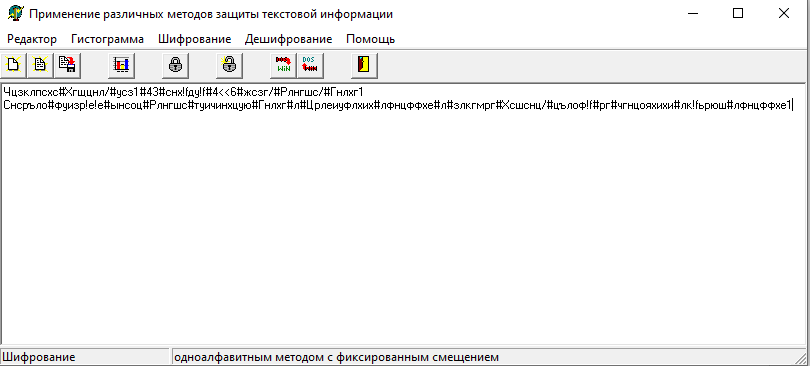
Пункт 1. Шифрование файла

Используем файл «2.txt» и зашифруем его используя одноалфавитный метод с фиксированным смещением (результат находится в файле «шифры.txt»).

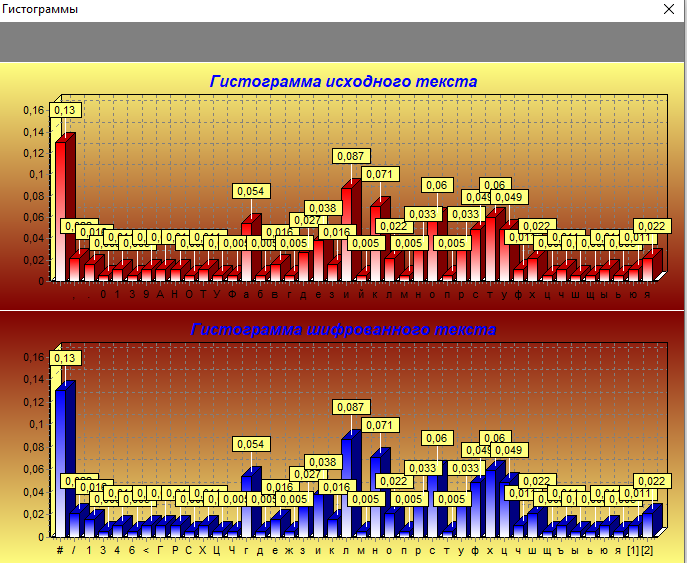
Исходный текст:



Результат:



Пункт 2. Описание гистограмм:



На гистограммах показана частота используемых символов. Частота остается неизменной, однако сами символы заменяются на другие.

Пункт 3. Определение смещения:

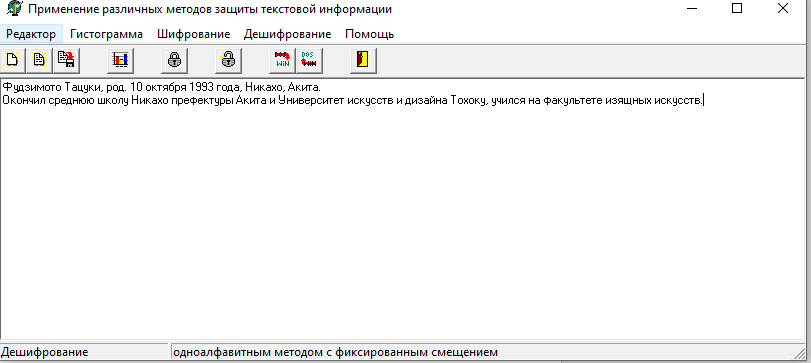
Переведем символы с одинаковой частотой использования в ASCII-код и найдем разность между ними.

Пример: А = 128, Г = 131, следовательно, смещение равно 131 – 128 = 3.

Пункт 4. Дешифровка:

1. Расшифровка с помощью программы:

С помощью программы расшифруем содержимое файла «(2)`.txt», используя одноалфовитный метод с фиксированным смещением.



1. Расшифровка вручную

Так как, из гистограмм видно, что смещение равно 3, то при ручной расшифровке переписывается каждый символ с учетом этого смещения, например: Ч Ф,

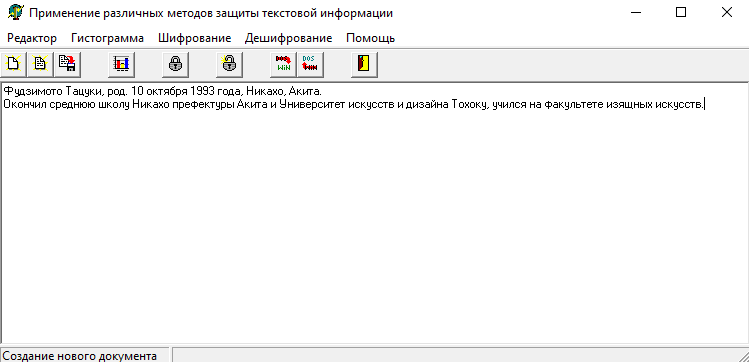
ц у.

Задание 3

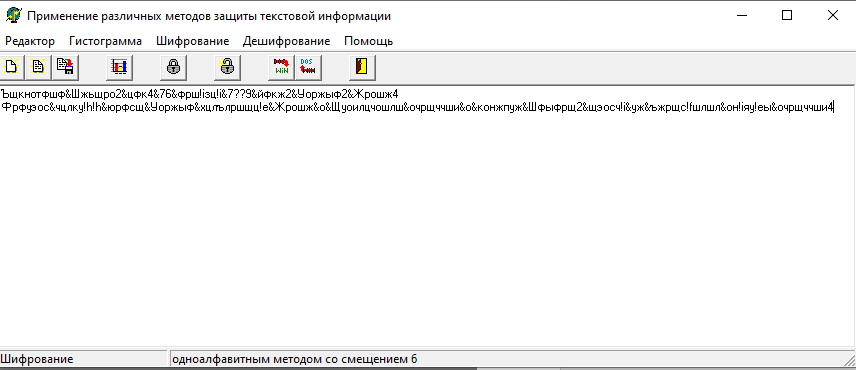
Пункт 1.

Зашифруем файл «2.txt» используя одноалфавитный метод

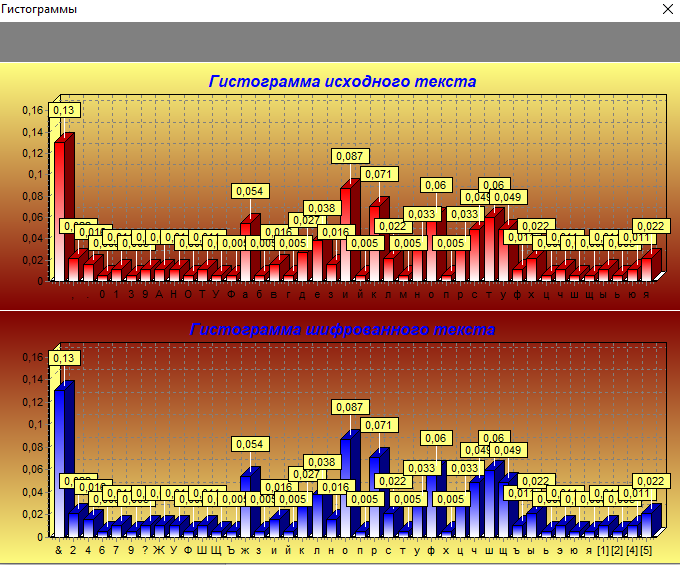
С заданным смещением



Результат (записан в файл «шифры.txt»):



Пункт 2.



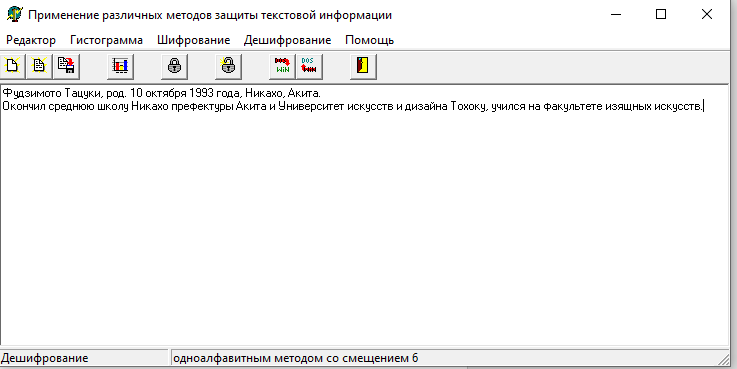
Из гистограмм видно, что при шифровке значение смещения установлено на 6 (0 6, к р)

Пункт 3.

Зная смещение можно легко дешифровать текст.

Используем одноалфавитное дешифрование со значением смещения = 6

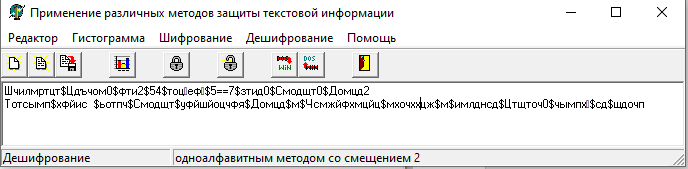
Результат:



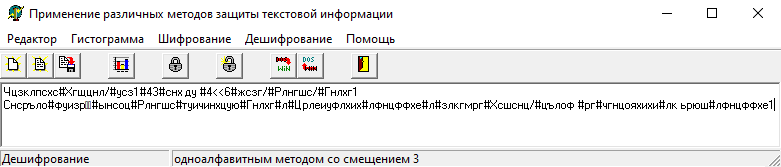
Пункт 4.

Расшифровка методом подбора смещения:

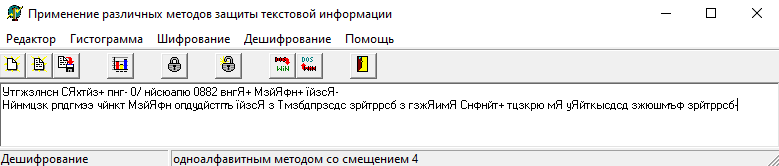
Смещение = 2



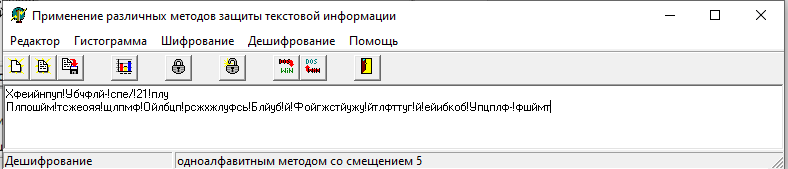
Смещение = 3



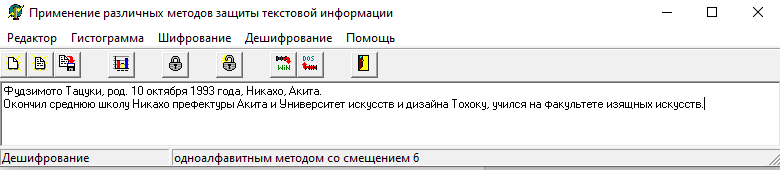
Смещение = 4



Смещение = 5



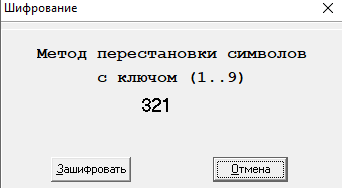
Смещение = 6



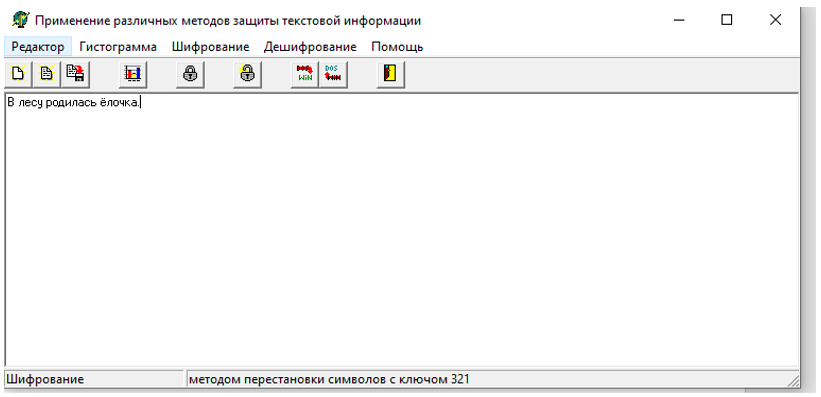
Задание 4

Зашифруем текст из файла «4.txt»

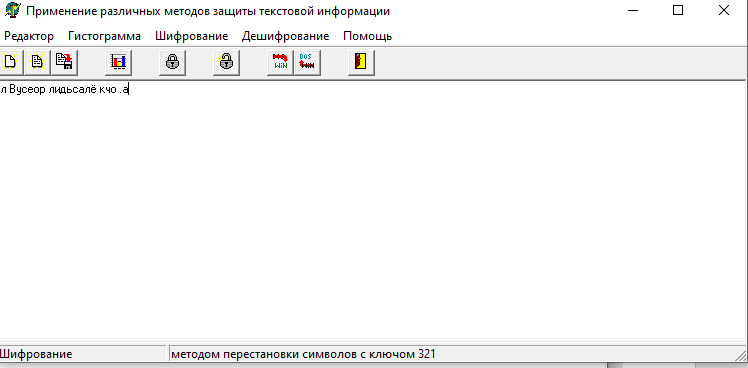
Используем ключ 321

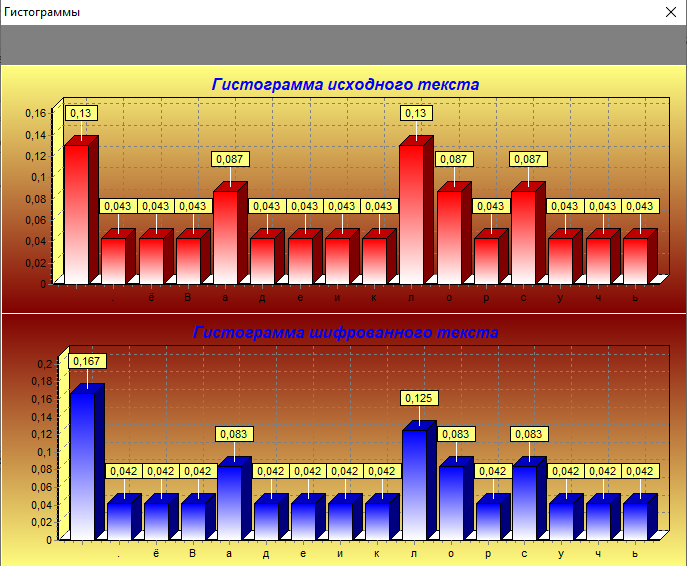


Исходный текст:



Результат:





Из гистограмм видно, что частота использования символов изменилась.

Сравним исходный текст и полученный шифр

В лесу родилась ёлочка.

л Вусеор лидьсалё кчо .а

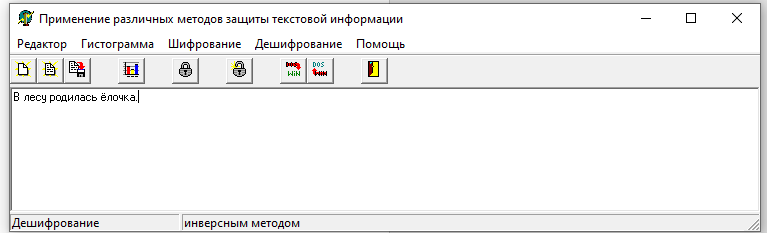
Стрелками указано, как происходит перестановка символов.

Поняв эту логику можно легко расшифровать этот текст как с помощью программы, так и вручную.

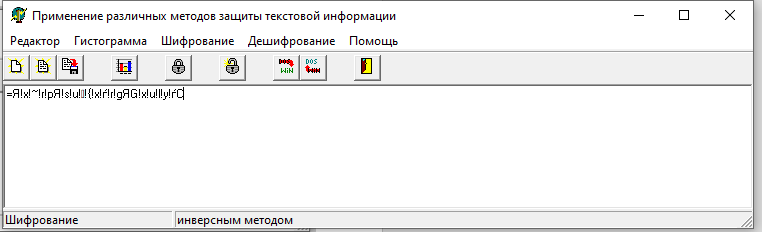
Задание 5

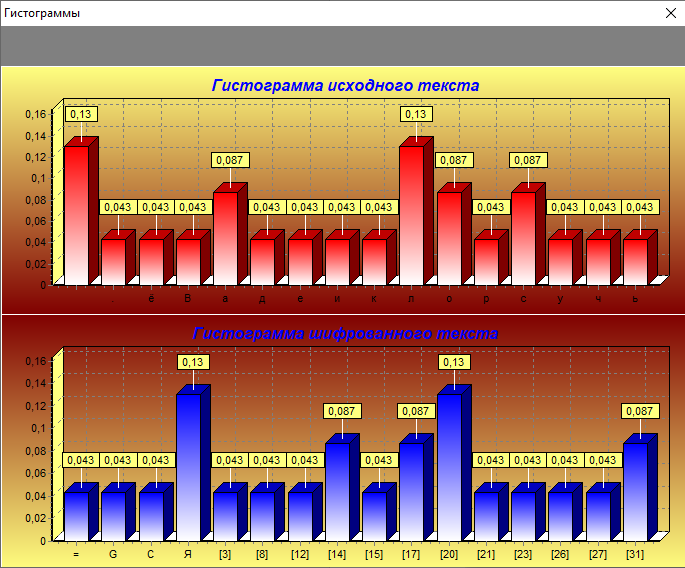
Зашифруем тот же текст (файл «4.txt»).

Исходный текст:



Результат:





Из гистограмм видно, что изменились символы и частота их использования.

Определим смещение для символов «В» и «ё»

|  |  |
| --- | --- |
| Символ | ASCII-код |
| В (до шифровки) | 130 |
| Я (после шифровки) | 159 |

255 - 130 = 125

159 – 125 = 34

Искомое смещение = 34

|  |  |
| --- | --- |
| Символ | ASCII-код |
| ё (до шифровки) | 241 |
| C (после шифровки) | 43 |

255 - 241 = 14

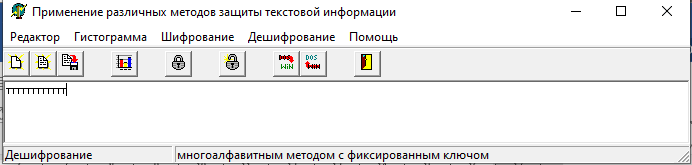
43 – 14 = 29

Искомое смещение = 29

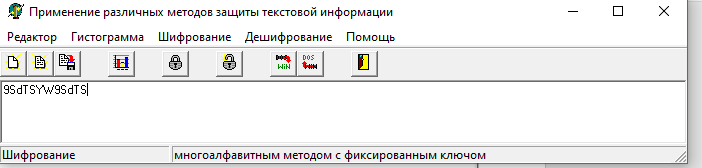
Задание 6

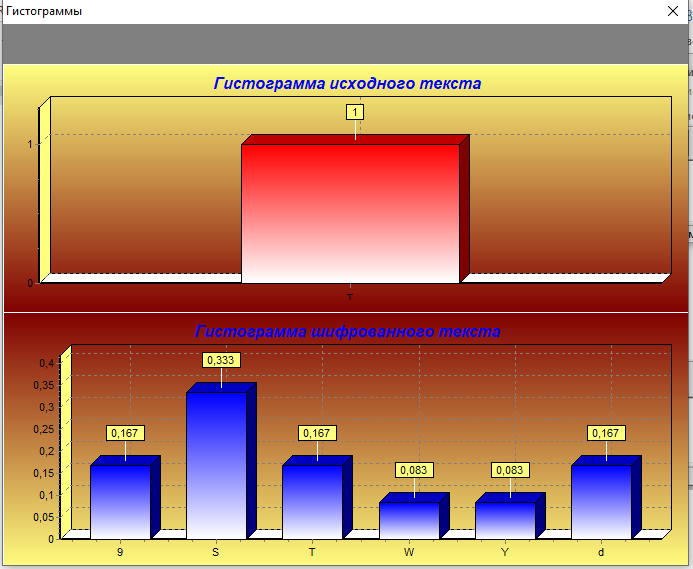
Зашифруем файл «6.txt» с помощью многоалфавитного метода с фиксированным ключом

Исходный текст:



Результат:



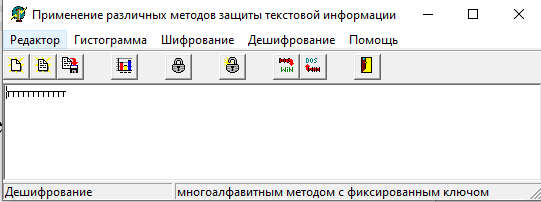


|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | тттттттттттт | ASCII-код | Смещение | Результат |
| 1 | **9**ттттттттттт | 226 | -169 | 57 — «9» |
| 2 | **9S**тттттттттт | 226 | -143 | 83 — «S» |
| 3 | **9Sd**ттттттттт | 226 | -116 | 100 — «d» |
| 4 | **9SdT**тттттттт | 226 | -142 | 84 — «T» |
| 5 | **9SdTS**ттттттт | 226 | -143 | 83 — «S» |
| 6 | **9SdTSY**тттттт | 226 | -137 | 89 — «Y» |
| 7 | **9SdTSYW**ттттт | 226 | -139 | 87 — «W» |
|  | ……… |  |  |  |

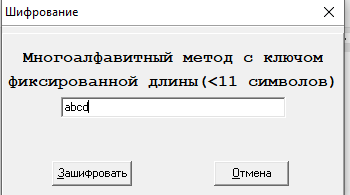
После 7-ого шага набор смещений повторяется.

Задание 7

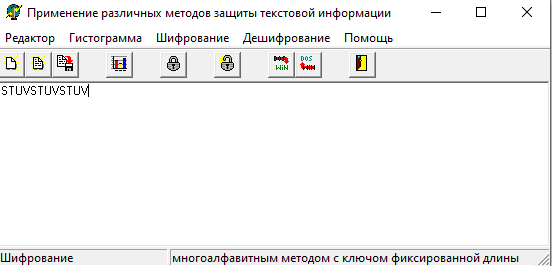
Зашифруем тот же файл (6.txt)

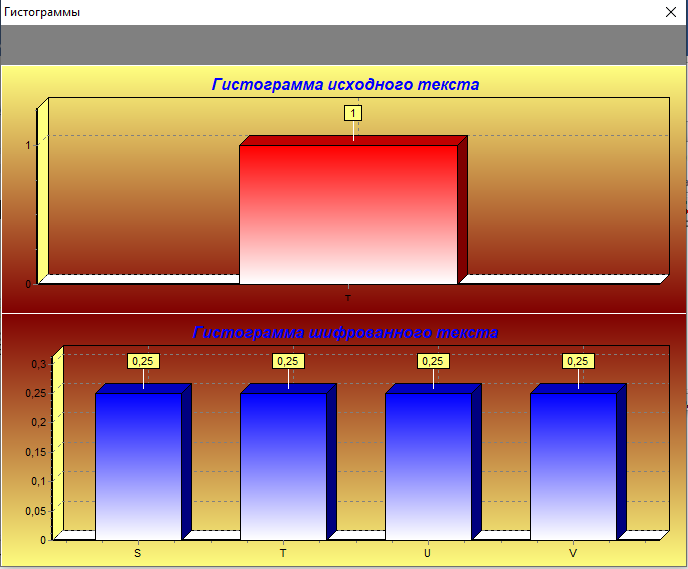


Используем ключ abcd



Результат:





Из данной гистограммы можно понять, длину ключа, которым зашифрован текст.

Исходный символ т – 226.

Ключ: a – 97, b – 98, c – 99, d –100.

Полученные символы: S – 83 T – 84 U – 85 V – 86

Воспользуемся формулой 

(226 + 97)mod(255) = 68

(226 + 98)mod(255) = 69

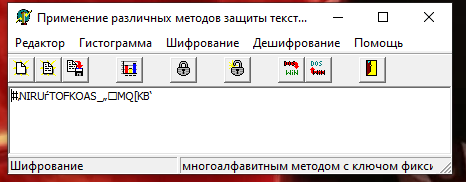
(226 + 99)mod(255) = 70

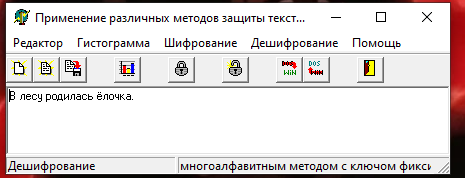
(226 + 100)mod(255) = 71

|  |  |  |  |
| --- | --- | --- | --- |
|  | ASCII-код | Зашифрованный символ | смещение |
| S | 83 | 68 | 15 |
| T | 84 | 69 | 15 |
| U | 85 | 70 | 15 |
| V | 86 | 71 | 15 |

Каждый символ получает смещение 15.

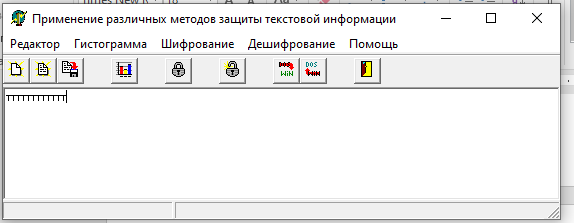
Шифрование и разшифрование для файла с произвольным текстом (используется файл «4.txt»)

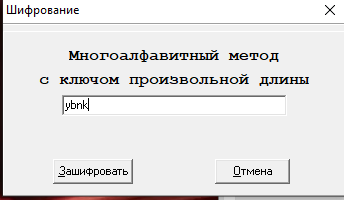




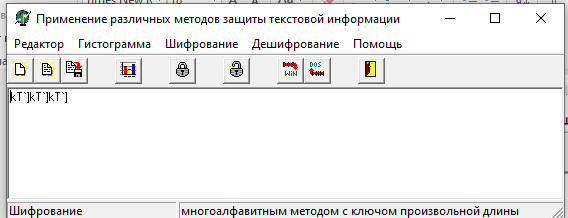
Задание 8

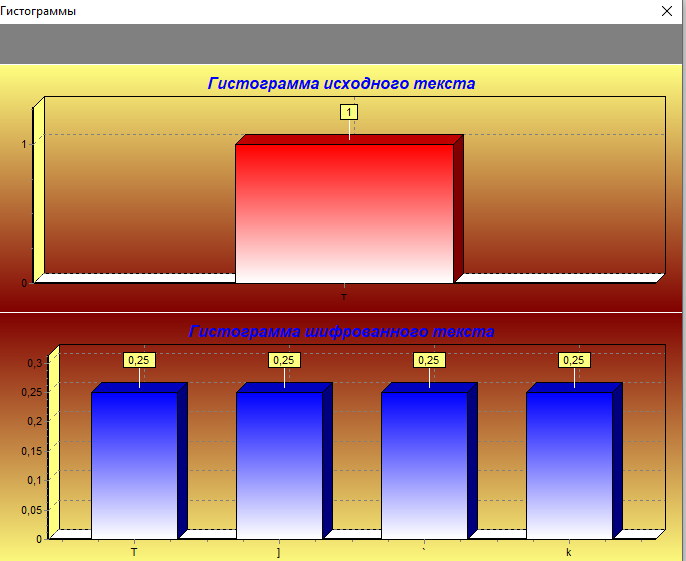
Зашифруем файл «6.txt»





Результат:





Исходный символ т – 226.

Ключ: y – 121, b – 98, n – 110, k – 107

Полученные символы: k – 107, T – 84, ` – 96, ] – 93

Воспользуемся формулой 

(226 + 121)mod(255) = 92

(226 + 98)mod(255) = 69

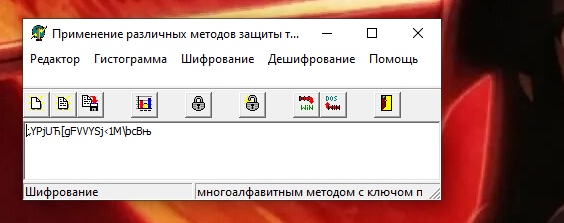
(226 + 110)mod(255) = 81

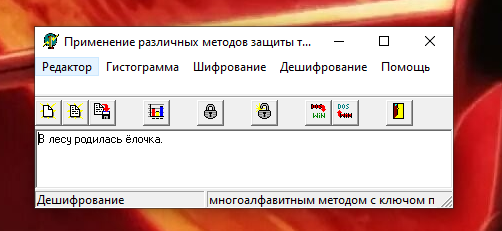
(226 + 107)mod(255) = 78

|  |  |  |  |
| --- | --- | --- | --- |
|  | ASCII-код | Зашифрованный символ | смещение |
| k | 107 | 92 | 15 |
| T | 84 | 69 | 15 |
| ` | 96 | 81 | 15 |
| ] | 93 | 78 | 15 |

Каждый символ получает смещение 15.

Шифрование и разшифрование для файла с произвольным текстом (используется файл «4.txt»)





Контрольные вопросы

Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод, из рассмотренных, вы выберете? Обоснуйте свой выбор.

— Для шифрования важных данных лучше всего использовать многоалфавитный метод с произвольным паролем т.к. он предоставляет наивысший уровень безопасности. Этот подход использует ключ, чтобы определить, какой алфавит будет использоваться для шифрования каждого символа в исходном тексте. В отличие от одноалфавитных методов, многоалфавитные шифры значительно затрудняют проведение частотного анализа, поскольку каждый символ может заменяться различными другими символами в зависимости от позиций ключа.