|  |
| --- |
| **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** |
| Федеральное государственное бюджетное образовательное учреждение высшего образования |
| **«Тихоокеанский государственный университет»** |

Институт экономики и управления

Экономическая кибернетики

Направление 09.03.03 «Прикладная информатика»

Профиль «Прикладная информатика в экономике»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

по дисциплине «Информационная безопасность»

Тема: «ИСПОЛЬЗОВАНИЕ КЛАССИЧЕСКИХ КРИПТОАЛГОРИТМОВ ПОДСТАНОВКИ И ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ».

|  |  |
| --- | --- |
| Студент: | Липихин Д.В. |
| Группа: | ПИЭ(б)з-21 |
| Преподаватель: | Салаватова Ю.А. |

Хабаровск – 2024 г.

2. Для одноалфавитного метода с фиксированным смещением определить

установленное в программе смещение.

Для этого:

* просмотреть предварительно созданный с помощью редактора свой

текстовый файл;

* выполнить для этого файла шифрование;

просмотреть в редакторе зашифрованный файл;

* просмотреть гистограммы исходного и зашифрованного текстов,
* описать гистограммы (в чем похожи, чем отличаются) и определить, с

каким смещением было выполнено шифрование;

* расшифровать зашифрованный текст:

с помощью программы, после чего проверить в редакторе правильность

расшифрования;

вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность

выполняемых действий, имена всех использованных файлов, описываются

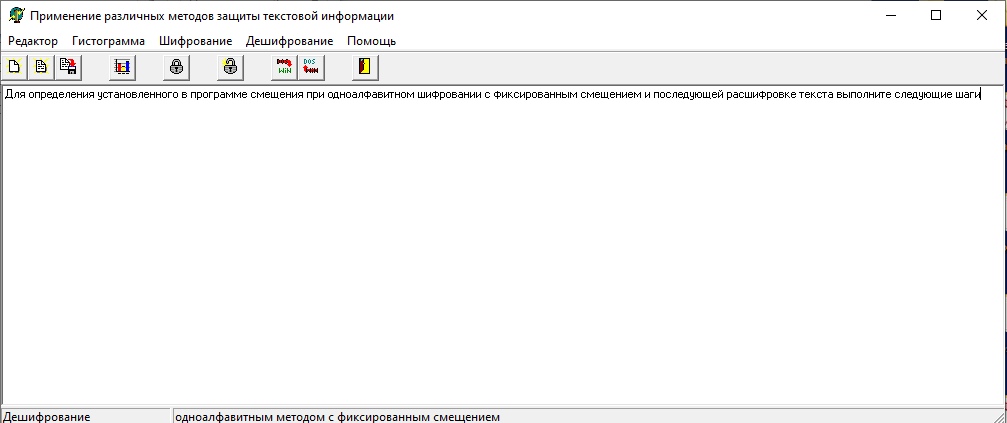
полученные гистограммы, указывается найденное смещение, описывается процесс

дешифрования.

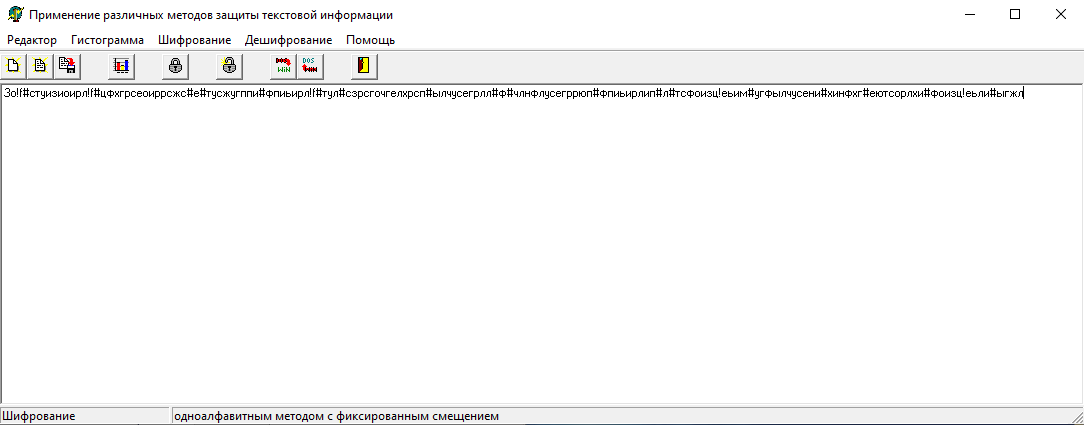
Преподавателю предоставляется отчет о проделанной работе и все использованные

и созданные файлы

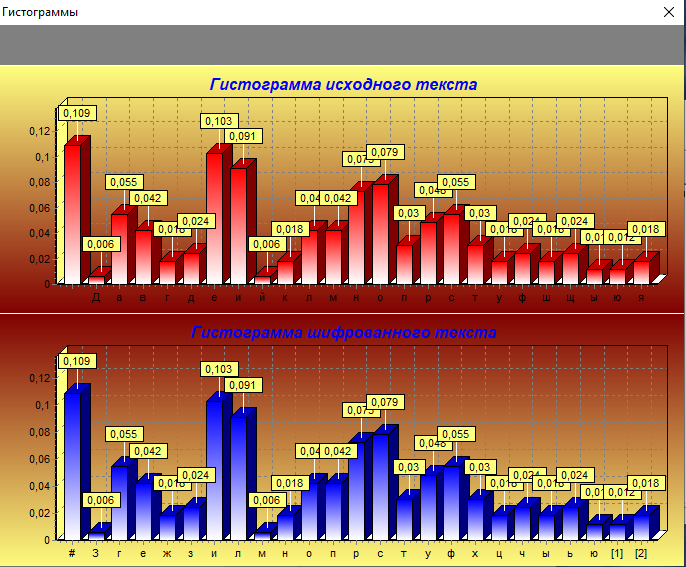
Исходный текстовый файл – Задание 2.txt



Было выполнено шифрование текста одноалфавитным методом (с фиксированным смещением).



Получены следующие результаты:



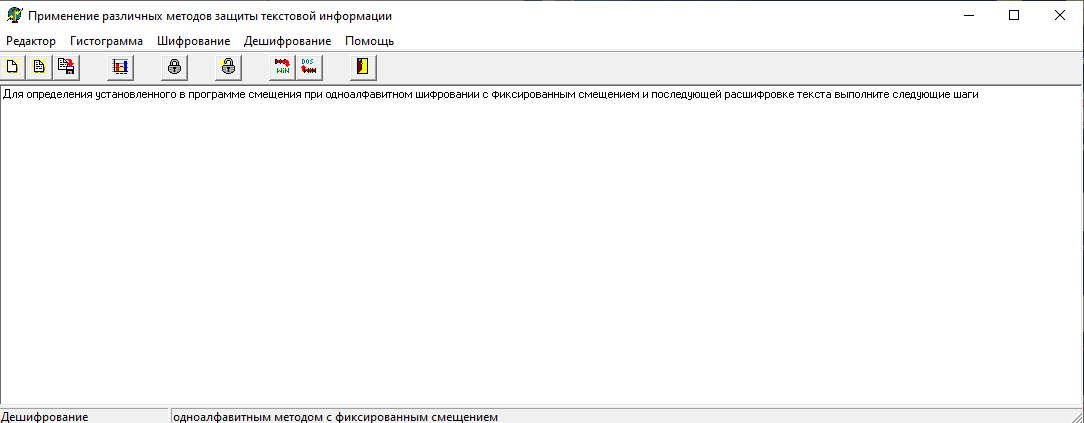
Верхняя гистограмма состоит из данных об исходном тексте. В ней указаны встречающиеся символы, и частота встречаемости каждого.

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.

***Дешифрование с помощью программы.***

Данная программа позволяет автоматически и безошибочно расшифровать текст.



*А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я*

*Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я*

Гистограмма очень упрощает задачу. Мы видим, что шифрованный символ находится прямо под исходным символом, т.е. смещение равняется 3. Это значит, что все остальные символы в шифрованном файле сдвинуты на 3 позиции.

Чтобы определить смещение, можно сравнить позиции самых частых букв в исходном и зашифрованном текстах. Предположим, что в исходном тексте самая частая буква — "Е". В зашифрованном тексте найдём самую частую букву, допустим, это "И". Теперь вычисляем разницу между этими буквами в алфавите:

Где 33 — количество букв в русском алфавите. Полученное значение и будет искомым смещением.

Например, если "Е" имеет позицию 7, а "И" — 10, то смещение равно:

10 - 7 = 3

Таким образом, шифрование было выполнено со смещением на 3 позиций.

3. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):

* для своего исходного текста выполнить шифрование с произвольным

смещением;

* просмотреть и описать гистограммы исходного и зашифрованного

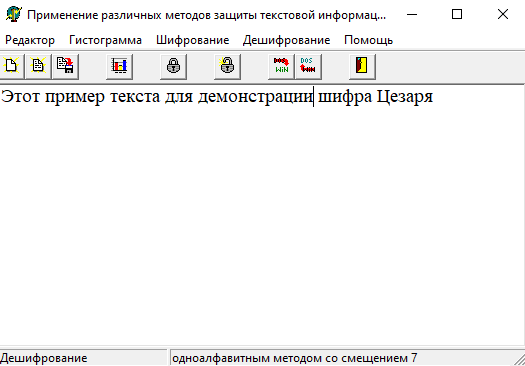
текстов, определить смещение для нескольких символов;

* расшифровать текст с помощью программы;
* имеется зашифрованный шифром Цезаря текст; дешифровать его с

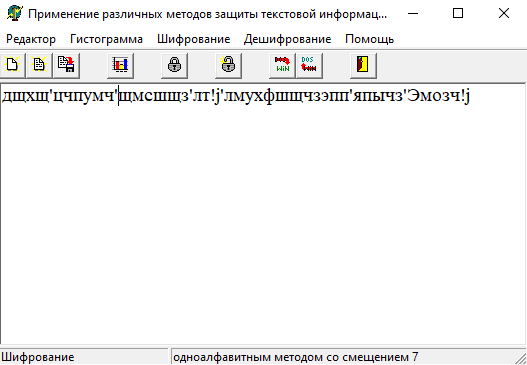
помощью программы методом подбора смещения; указать, с каким

смещением был зашифрован файл.

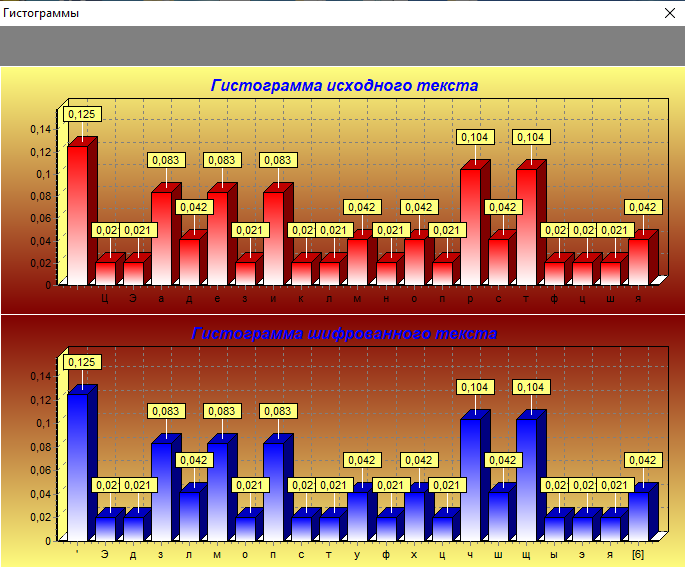
Исходный текстовый файл – Задание 3.txt



В шифровании использовалось смещение на 7 позиций



Получили следующие результаты



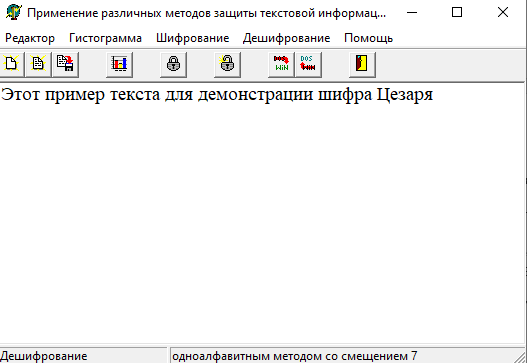
***Процесс дешифрования вручную.***

Из гистограммы шифрованного текста возьмем наиболее часто встречающийся символ ‘-’. В гистограмме исходного текста ему соответствует символ ‘ ’ (пробел), т.к. он имеет ту же частоту встречаемости 0,138. Из ASCIIтаблицы код символа ‘ ’ (пробел) равен 32, а код символа ‘ ' ’ равен 45.

Вычислим смещение: 39 – 32 = 7. Зная смещение, можно рассчитать оставшиеся символы по формуле:

ASCII-код исход. символа =ASCII-код шифр. символа – смещение;

***Дешифрование с помощью программы.***



4. Для метода перестановки символов дешифровать зашифрованный файл.

Для этого необходимо определить закон перестановки символов открытого

текста. Создайте небольшой файл длиной в несколько слов с известным вам

текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно

ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью

редактора) ваш исходный и зашифрованный тексты и определите закон

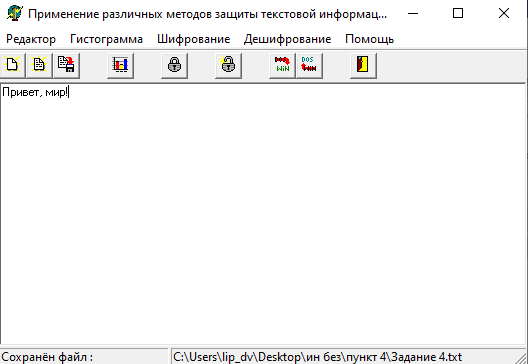
перестановки символов.

Дешифруйте файл:

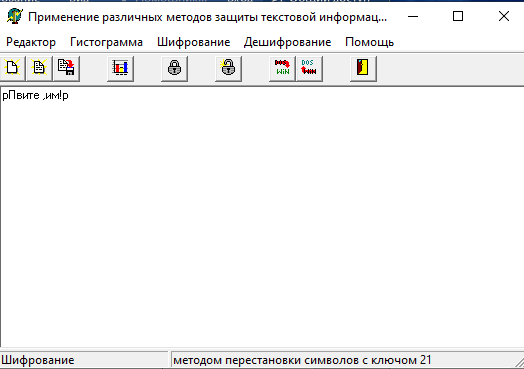
1) вручную (объясните ваши действия);

2) с помощью программы.

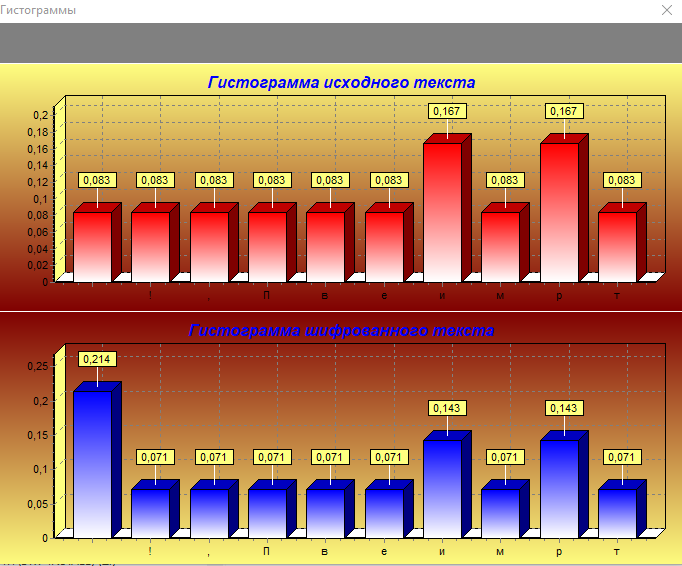
Исходный текстовый файл – Задание 4.txt



После шифрования с ключом 21, получили текстовый файл Задание 4 шифр.txt:



Гистограммы исходного и зашифрованного текстов схожи между собой:



Оба текста содержат одинаковые буквы, поэтому их гистограммы будут одинаковыми. Это означает, что из гистограмм нельзя извлечь полезной информации для дешифровки.

**Определение закона перестановки символов**

Сравнивая открытый и зашифрованный тексты, можно заметить, что каждая первая буква была перемещена на одну позицию вперед. Закон перестановки заключается в следующем:

Первая буква перемещается на одну позицию вперед.

Вторая буква остается на месте.

Третья буква перемещается на одну позицию вперед.

Четвертая буква остается на месте.

И так далее.

**Ручная дешифрация**

Чтобы расшифровать текст вручную, нужно применить обратный порядок действий:

Вернуть каждую первуб букву на одну позицию назад.

Например, для зашифрованного текста рПвите ,им!р

Вторую букву оставляем (р).

Первую букву возвращаем на одну позицию назад (П).

Четвертую букву оставляем (в).

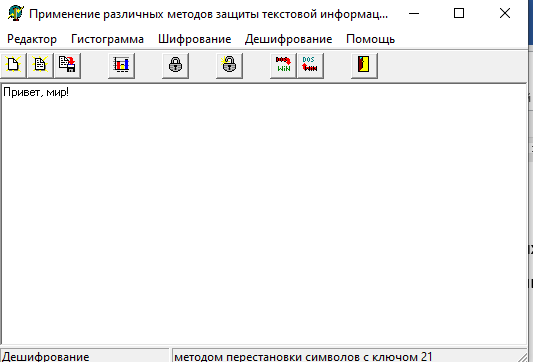
Третью букву возвращаем на одну позицию назад (и).

И так далее.

Получаем оригинальный текст: Привет, мир!

**Программная дешифрация**

Дешифрация делается так же как и шифрование, методом перестановки символов с ключом 21



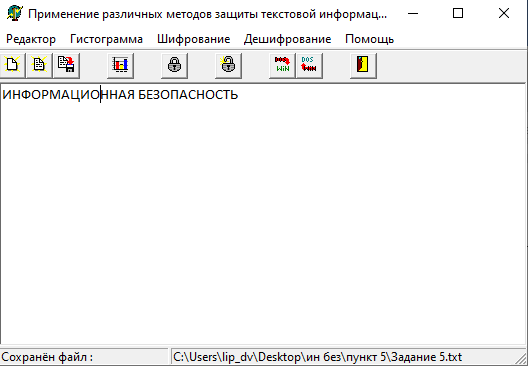
5.Для инверсного кодирования (по дополнению до 255):

* для своего произвольного файла выполните шифрование;
* просмотрите гистограммы исходного и зашифрованного текстов,

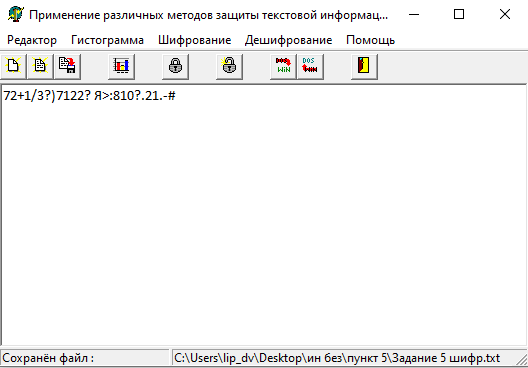
опишите гистограммы и определите смещение для нескольких

* символов;
* дешифруйте зашифрованный текст, проверьте в редакторе правильность
* дешифрования.

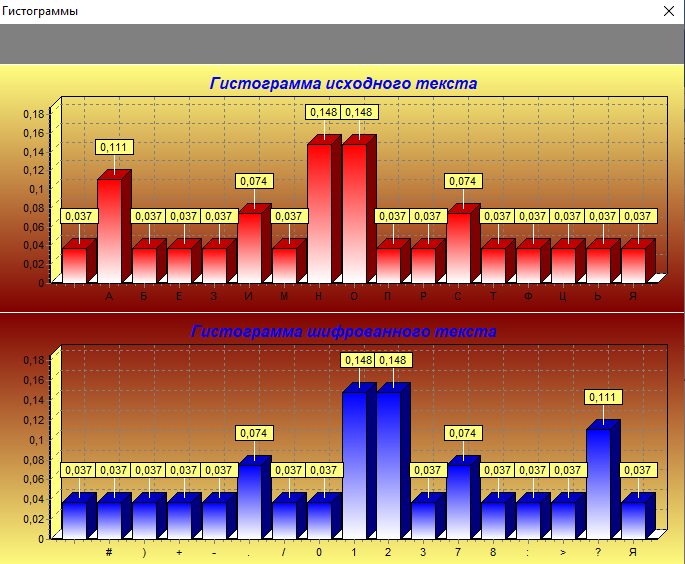
Исходный текстовый файл Задание 5.txt



Шифрованный текстовый файл Задание 5 шифр.txt



Гистограммы исходного и шифрованного текстов:



Инверсное кодирование по дополнению до 255 предполагает преобразование числа таким образом, чтобы результат был дополнением исходного числа до 255. Смещение в данном контексте — это разница между максимальным значением (255) и исходным числом.

Чтобы найти смещение, нужно вычесть исходное число из максимального значения (255). Это позволит получить число, которое является дополнением исходного числа до 255.  
  
72+1/3?)7122? Я>:810?.21.-#

**И**2+1/3?)7122? Я>:810?.21.-# - 255 – 55(«7») = 200(«И»)

**ИН**+1/3?)7122? Я>:810?.21.-# - 255 – 50(«2») = 205(«Н»)

**ИНФ**1/3?)7122? Я>:810?.21.-# - 255 – 43(«+») = 212(«Ф»)

**ИНФО**/3?)7122? Я>:810?.21.-# - 255 – 49(«1») = 206(«О»)

**ИНФОР**3?)7122? Я>:810?.21.-# 255 – 47(«/») = 208(«Р»)

Часто появляющиеся символы в гистограмме Н и О в исходном тексте, в шифрованном же тексте символы 1 и 2, чтобы определить смещение отнимем значения символов исходного текста от шифрованного

205 – 50 = 145 получившееся смещение

При расшифровке текста, получается аналогичный текст до шифрования

6. Для многоалфавитного шифрования с фиксированным ключом определите,

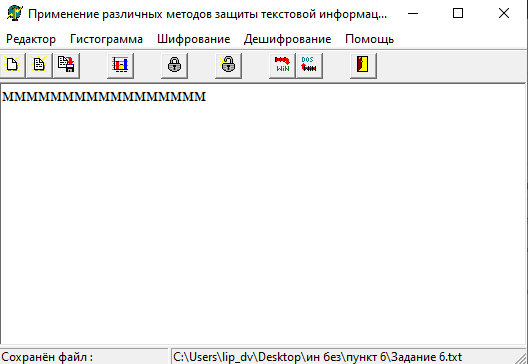
сколько одноалфавитных методов и с каким смещением используется в программе.

Для этого нужно создать свой файл, состоящий из строки одинаковых

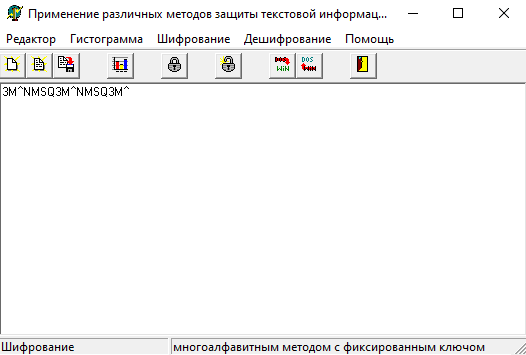
символов, выполнить для него шифрование и по гистограмме определить способ

шифрования и набор смещений.

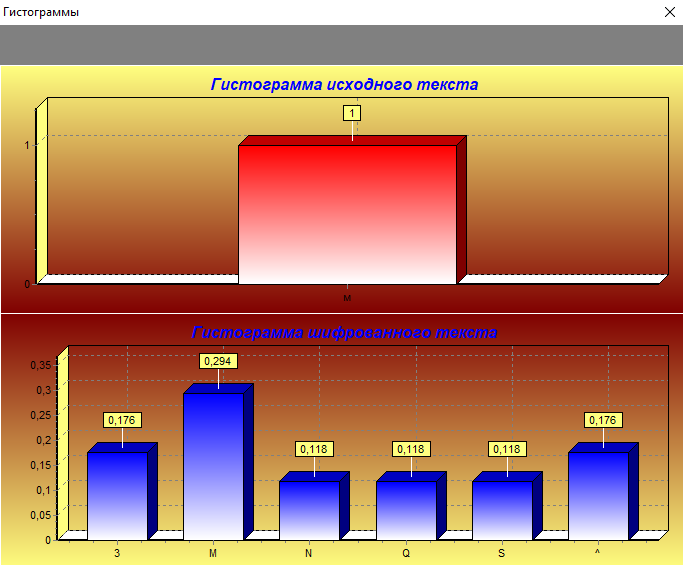
Исходный текстовый файл Задание 6.txt



Зашифрованный текстовый файл Задание 6 шифр.txt



Гистограмма исходной и зашифрованной строки:



Для шифрования последовательности из одинаковых символов используется набор из 7-и смещений.

|  |  |  |  |
| --- | --- | --- | --- |
|  | ASCII-код | Смещение | Результат |
| 1. | 3мммммммммммммммм | 236 | -185 | 51 – «3» |
| 2. | **3M**ммммммммммммммм | 236 | -159 | 77 – «M» |
| 3. | **3M^**мммммммммммммм | 236 | -142 | 94– «^» |
| 4. | **3M^N**ммммммммммммм | 236 | -158 | 78– «N» |
| 5. | **3M^NM**мммммммммммм | 236 | -159 | 77 – «M» |
| 6. | **3M^NMS**ммммммммммм | 236 | -153 | 83 – «S» |
| 7. | **3M^NMSQ**мммммммммм | 236 | -155 | 81– «Q» |
|  | … |  |  |  |
| n | 3M^NMSQ3M^NMSQ3M^ |  |  |  |

После 7-го шага набор смещений повторяется. И в конце мы получили результат шифрования.

7. Для многоалфавитного шифрования с ключом фиксированной длины:

для файла, состоящего из строки одинаковых символов выполнить

шифрование и определить по гистограмме, какое смещение получает каждый

символ;

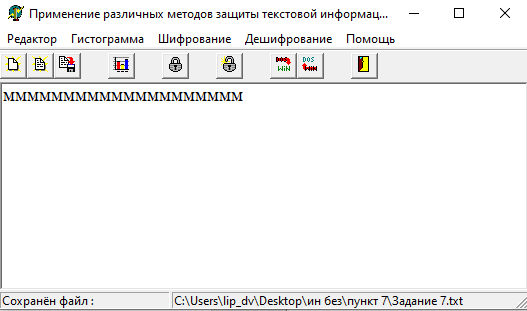
для файла произвольного текста произвести шифрование и расшифрование;

просмотреть и описать гистограммы исходного и зашифрованного текстов;

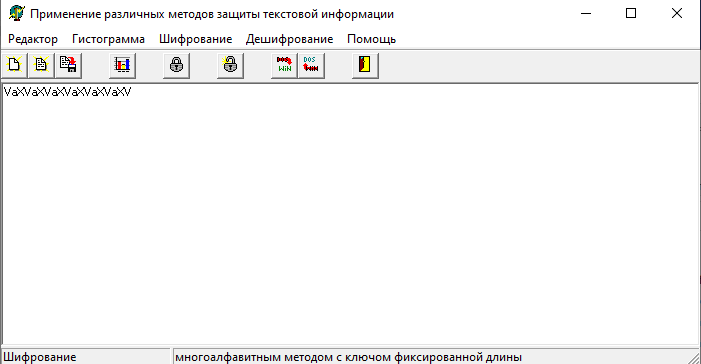
ответить, какую информацию можно получить из гистограмм.

Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п.7.

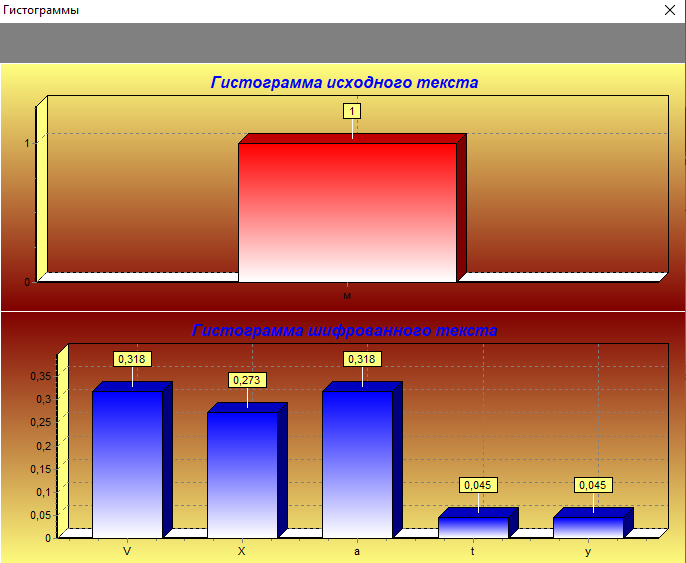
Исходный текстовый файл Задание 7.txt



Зашифрованный текстовый файл Задание 7 шифр.txt



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 ASCIIтаблицы:

Исход. символ: р – 236;

Ключ: j– 106;u– 117;l– 108;

Последовательность из повторяющихся символов «VaX» (ASCII-коды:Z– 090; \ – 092;e– 101) определим по формуле:https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-8_Nsv_.png. Гдеhttps://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-phdTeI.png– зашифрованный символ,https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-uDufvF.png– шифруемый символ (исход.),https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-cC4Hfz.png– задаваемая гамма посл-ть,https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-LuTgTq.png– кол-во символов в алфавите (255 – в нашем случ.)

Итак:

(236 + 106) – 255 = 87;

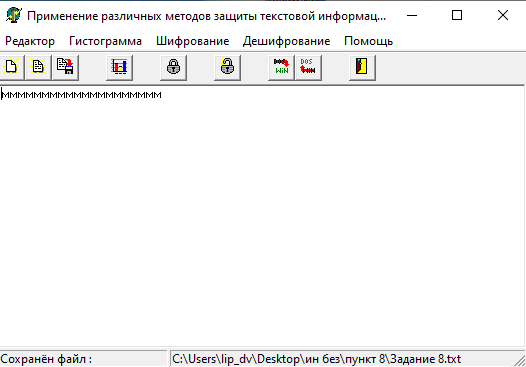
(236 + 117) – 255 = 98;

(236 + 108) – 255 = 89;

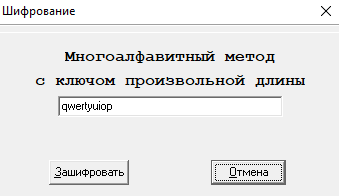
Как видим, для шифрования исход. текста используется фор-ла: https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-cshY4R.png.

7.1 Многоалфавитное шифрование с произвольным паролем

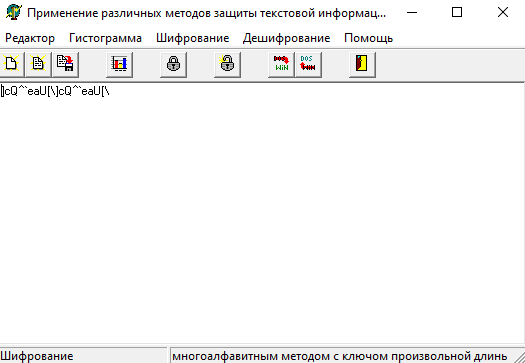
Исходный текстовый файл Задание 8.txt

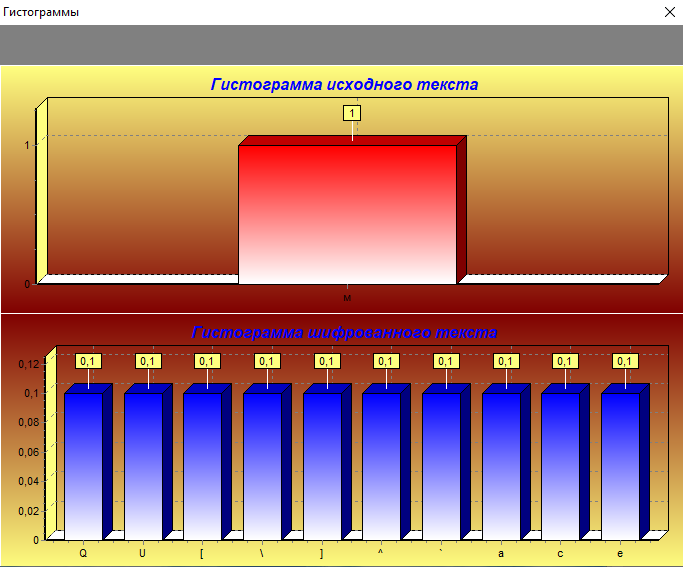


Вводим ключ шифрования



Зашифрованный текстовый файл Задание 8 шифр.txt





Перевод символов с помощью ASCIIтаблицы:

Исход. символ: р – 240;

Ключ: q– 113;w– 119;e– 099;r– 114;t– 116;y– 121;u– 117;i– 105;o– 111.

Получаем посл-ть из повторяющихся символов: «]cQ^`eaU[\]cQ^`eaU[\» (ASCII-коды:]– 093;c– 99;Q– 081; ^– 094;`– 145;e– 101;a– 097;U– 085; [ - 091; \ - 092 ). Определим метод шифрования по формуле:https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-qqlsz0.png. Гдеhttps://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-kicW8E.png– зашифрованный символ,https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-Kh4YqA.png– шифруемый символ (исход.),https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-LicwwR.png– задаваемая гамма посл-ть,https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-N0Uzpr.png– кол-во символов в алфавите (255 – в нашем случ.)

Итак:

(236 + 113) – 255 = 94;

(236 + 119) – 255 = 100;

(236 + 099) – 255 = 80;

(236 + 114) – 255 = 95;

(236 + 116) – 255 = 102;

(236 + 121) – 255 = 102;

(236 + 117) – 255 = 98;

(236 + 105) – 255 = 86;

(236 + 111) – 255 = 92;

Можем увидеть, что для шифрования исход. текста использовалась формула: https://studfile.net/html/2706/28/html_zWsgaN71L0.2Pua/img-OQtwLK.png