Лабораторная работа №12

Тема: Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации.

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.

Описание лабораторной работы

Для выполнения лабораторной работы необходимо запустить программу L_LUX.EXE. На экране дисплея появляется окно с размещенным в его центре текстовым редактором (для отображения зашифрованных и расшифрованных текста), в верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие. Чуть ниже основного меню размещена панель инструментов (для управления быстрыми командными кнопками и другими ≪горячими≫ элементами управления), а в самом низу окна, под текстовым редактором, находится строка состояния. в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов для удобства снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу ENTER, вернуться в главное меню или вовсе выйти из него — ESC.

Рассмотрим более подробно каждый из пунктов главного меню.

Редактор. Данный пункт основного меню содержит подпункты: создать документ, открыть файл, сохранить файл, выход из программы.

Предварительно, сразу после запуска программы, текстовый редактор недоступен, также недоступными являются почти все пункты главного меню, кроме создания документа, открытия файла, выхода из программы, информации о программе, и большая часть клавиш панели управления, за исключением создания документа, открытия файла и выхода из программы.

Создать документ (Ctrl+N) – при выборе данного подпункта становится доступна работа с текстовым редактором, также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Создать документ (Ctrl+N) - данный подпункт делает доступным для работы тестовый редактор (пользователь получает право создать свой текстовый файл , который впоследствии можно будет использовать при работе с программой) , также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Открыть файл (Ctrl+L) - при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файлабудет отображено в окне редактора текстов.

Аналогично пункту **"Создать документ"** доступным для работы становится текстовый редактор с отображаемым текстом , а также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Сохранить файл (Ctrl+S) - при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое редактора текстов.

Выход из программы (Ctrl+X) - при выборе этого пункта появляется диалоговое окно, позволяющее выйти из программы.

Гистограмма

Вывод на экран двух гистограмм , отображающих частоту встречаемости символов в тексте.

Внимание ! До выполнения шифрования и дешифрования вызывать гистограмму не имеет смысла , так как ещё не сформированы тексты , для которых будет просматриваться гистограмма.

Имеется возможность просмотра следующих сочетаний гистограмм :

- гистограммы исходного и шифрованного файла ,

- гистограммы шифрованного и расшифрованного файла ,

- гистограммы стандартного распределения и шифрованного текста ,

- гистограммы стандартного распределения и расшифрованного текста .

В гистограммах с целью масштабирования используются левая и правая клавиши мыши.

Например , после шифрования текста большого объёма пользователь хочет посмотреть гистограммы исходного и шифрованного файла. Поскольку размеры текста достаточно большие , то на экран будут выведены две гистограммы с большим количеством столбиков в каждой (столбик соответ-

ствует одному символу текста) , однако трудно будет сказать , какой из этих столбцов соответствует тому или иному символу текста , и какова частота встречаемости данного символа. Поэтому у пользователя есть возможность увеличить масштаб любой из двух гистограмм с целью более точного определения требуемого значения частоты встречаемости конкретного символа.

Для этого необходимо навести указатель мыши на левую границу того участка гистограммы, который требуется увеличить, затем нажать левую клавишу мыши, и не отпуская её растянуть прямоугольник так , чтобы его нижний правый угол совпал с правой границей увеличиваемого участка гистограммы. После этого следует отпустить левую клавишу мыши и на экране появится увеличенное изображение нужного участка.

Причём, нажав и не отпуская правую клавишу мыши можно двигать гистограмму в любом направлении с целью изучения всего полученного распределения в увеличенном масштабе.

Для того, чтобы от увеличенного масштаба вернуться к исходному виду,нужно навести указатель мыши на гистограмму , затем нажать левую клавишу мыши , и не отпуская её снизу вверх растянуть небольшой по размерам прямоугольник , после этого следует отпустить левую клавишу мыши и на экране появится исходное изображение гистограммы .

Шифрование

Выполнение шифрования текстового файла одним из семи методов , рассматриваемых в лабораторной работе :

1) Одноалфавитный метод (с фиксированным смещением).

2) Одноалфавитный с задаваемым смещением (от 2 до 20).

3) Перестановка символов.

4) По дополнению до 255 (инверсный метод).

5) Многоалфавитный метод (с фиксированным ключом).

6) Многоалфавитный метод с ключом фиксированной длины.

7) Многоалфавитный метод с ключом произвольной длины.

Выбор метода шифрования производится как мышкой, так и клавишами перемещения курсора и клавишей "ENTER" . Затем появляется окно в котором в зависимости от метода шифрования требуется указать те или иные параметры , и либо подтвердить процесс кодировки , либо отказаться от него.

После этого в окно редактора будет выдан зашифрованный текст.

Дешифрование

"Дешифрование" - выполнение расшифрования зашифрованного текста.

П р и м е ч а н и е : Обычно термин ДЕШИФРОВАНИЕ применяют , когда известен ключ , а термин РАСШИФРОВАНИЕ - когда ключ не известен .

Аналогично предыдущему пункту выбирается метод расшифрования (должен соответствовать методу , которым был зашифрован файл).

Снова появляется окно, в котором в зависимости от метода расшифрования требуется указать те или иные параметры, и либо подтвердить процесс раскодировки, либо отказаться от него.

После этого в окно редактора будет выдан расшифрованный текст.

При правильном дешифровании полученный текст совпадает с исходным. Если какой либо задаваемый параметр не точен , то исходный и дешифрованный текст не совпадают , то есть расшифрование проведено неверно .

Помощь

Имеется возможность посмотреть данный текст (Помощь Ctrl+F9), справочную информацию об используемых методах шифрования (О методах Ctrl+F10), сведения о программе ('О программе Ctrl+F11').

Пример работы с программой

В качестве примера рассмотрим одноалфавитное шифрование с фиксированным ключом.

Нажав клавиши Ctrl+L , либо выбрав в меню пункт "Открыть файл" , загрузите в окно редактора исходный текст .

Затем вызовите пункт меню "Шифрование" , выберите одноалфавитный метод (с фиксированным смещением). В появившемся окне нажмите клавишу "Зашифровать" .

После того, как шифрование выполнено , можно также просмотреть в редакторе зашифрованный текст .

Затем перейдите к пункту меню "Гистограмма" . Выберите тип гистограмм , отображающий гистограммы исходного и шифрованного файлов. Проанализируйте гистограммы.

Они должны иметь примерно одинаковый вид.

Чтобы узнать ключ шифра, (смещение второго алфавита относительно первого), необходимо найти по гистограммам символы , имеющие одинаковую частоту встречаемости . Например , самый частый символ в первой гистограмме при шифровании должен перейти в самый частый символ во второй гистограмме .

Таким образом, найдя два самых часто встречаемых символа в обеих гистограммах, можно по стандартной таблице кодов IBM PC вычислить смещение .

Зная смещение и таблицу кодировки символов, текст можно легко расшифровать. Вызвав пункт меню "Дешифрование" , можно провести те же действия в автоматическом режиме .

П р и м е ч а н и е : при шифровании и дешифровании из таблицы кодировки не используются символы с кодами : 176 - 223 и 240 - 255 . То есть при ручной расшифровке эти символы следует пропускать , и считать , что , например , символ " Я " имеет код не 159 , а - 223 , аналогично " п " не 175 , а - 239 .

Иногда в гистограммах под столбиками, показывающими частоту встречаемости символов, изображены не сами символы, а их табличные коды в квадратных скобках .

Дополнительные сведения

1) Так как для всех выше перечисленных методов ключи шифрования представляют собой совершенно разные , даже несовместимые типы данных (оноалфавитные методы длина сдвига , перестановка -- массив неповторяющихся цифр , многоалфавитные методы -- строки), а для их отображения используется один и тот же элемент окна , то все они(ключи) на интерфейсном уровне общения с пользователем представляются строками, оставаясь внутри программы соответствующими своему изначальному виду.

2) При запуске утилит шифрования и расшифрования у пользователя спрашивается подтверждение на правильность выбранного метода для работы .

3) Во время работы длительных по исполнению процедур запускается прогресс процесса и гасится окно текстового редактора.По полоске прогресса можно наблюдать и оценивать примерную скорость работы алгоритма и время окончания текущего процесса.

4) Операционная среда : WIN' 95, WIN' 98 и WIN NT .

5) Минимальная конфигурация : На которой запускается WINDOWS .

6) Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся .

7) Конвертация DOS - текстов. При запуске этой опции сразу (без подтверждения со стороны пользователя) происходит прокрутка окна текстового редактора. После окончания конвертации происходит отображение в окне текстового редактора нового (конвертированного) текста.

Примечание :

Не пытайтесь конвертировать файлы с win-кодировкой , так как последствия будут непредсказуемые. Если при открытии файла на экране были псевдографические сим волы, а после конвертации вид файла не улучшился (не приблизился к русскоязыч ному варианту) , то скорее всего это был не Dos-овский файл, а какой-нибудь ещё системы .

8) Выгрузка системы .

1. У пользователя запрашивается подтверждение на выход из программы .

2. При утвердительном ответе закрываются все открытые файлы, запросом о сохранении любых изменений ; останавливаются все текущие процессы .

3. Происходит полный выход из системы .

9) Описание "горячих клавиш" :

Shift+F10 - 'О программе'

Ctrl+X - 'Выход из программы'

Ctrl+N - New - 'Файл\Создать'

Ctrl+L - Load - 'Файл\Открыть'

Ctrl+S - Save - 'Файл\Сохранить'

Шифрование :

Ctrl+F1 - 'Одноалфавитный метод (с фиксированным смещением)'

Ctrl+F2 - 'Одноалфавитный с задаваемым смещением (от 2 до 20)'

Ctrl+F3 - 'Перестановка символов'

Ctrl+F4 - 'По дополнению до 255 (инверсный метод)'

Ctrl+F5 - 'Многоалфавитный метод с фиксированным ключом'

Ctrl+F6 - 'Многоалфавитный метод с ключом фиксированной длины '

Ctrl+F7 - 'Многоалфавитный метод с ключом произвольной длины '

Дешифрование :

Shift+F1 - 'Одноалфавитный метод (с фиксированным смещением)'

Shift+F2 - 'Одноалфавитный с задаваемым смещением (от 2 до 20)'

Shift+F3 - 'Перестановка символов'

Shift+F4 - 'По дополнению до 255 (инверсный метод)'

Shift+F5 - 'Многоалфавитный метод с фиксированным ключом'

Shift+F6 - 'Многоалфавитный метод с ключом фиксированной длины '

Shift+F7 - 'Многоалфавитный метод с ключом произвольной длины '

Гистограммы :

Shift+Ctrl+F1 - 'Исходного и шифрованного файла'

Shift+Ctrl+F2 - 'Шифрованного и расшифрованного файла'

Shift+Ctrl+F3 - 'Стандартного распределения и шифрованного текста'

Shift+Ctrl+F4 - 'Стандартного распределения и расшифрованного текста'

Помощь:

Ctrl+F9 - 'Помощь'

Ctrl+F10 - 'О методах'

Ctrl+F11 - 'О программе'

Теоретический материал.

Гистограмма текста. Одним из наиболее известных методов криптоанализа является изучение статистических характеристик шифрованных текстов. Графическое отображение совокупности частот встречаемости символов в тексте называют ***гистограммой этого текста***.

Следует иметь в виду, что вид гистограммы для стандартного распределения зависит от вида исходного текста следующим образом если исходный текст содержит символы кириллицы и латинского алфавита, то выводится статистическое распределение для кириллицы; и латиницы, если только кириллицы (латиницы), то выводится статистическое распределение для кириллицы (латиницы).

Задание

1 Ознакомиться с описанием лабораторной работы и заданием.

2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:

■ просмотреть предварительно созданный с помощью редактора свой текстовый файл;

■ выполнить для этого файла шифрование;

■ просмотреть в редакторе зашифрованный файл;

■ просмотреть гистограммы исходного и зашифрованного текста;

■ 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, полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

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

■ выполнить шифрование с произвольным смещением для своего исходного текста;

■ просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
■ расшифровать текст с помощью программы;
■ дешифровать зашифрованный шифром Цезаря текст с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.
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:
■ вручную (объясните ваши действия);
■ с помощью программы.
5. Для инверсного кодирования (по дополнению до 255):
■ выполните шифрование для своего произвольного файла;
■ просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
■ дешифруйте зашифрованный текст; проверьте в редакторе правильность дешифрования.
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 смешений.
7. Для многоалфавитного шифрования с ключом фиксированной длины:
■ выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;
■ выполните шифрование и расшифрование для файла произвольного текста;
■ просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.
8 . Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 7.
9. Привести в отчете ответы на контрольные вопросы.

Вопросы

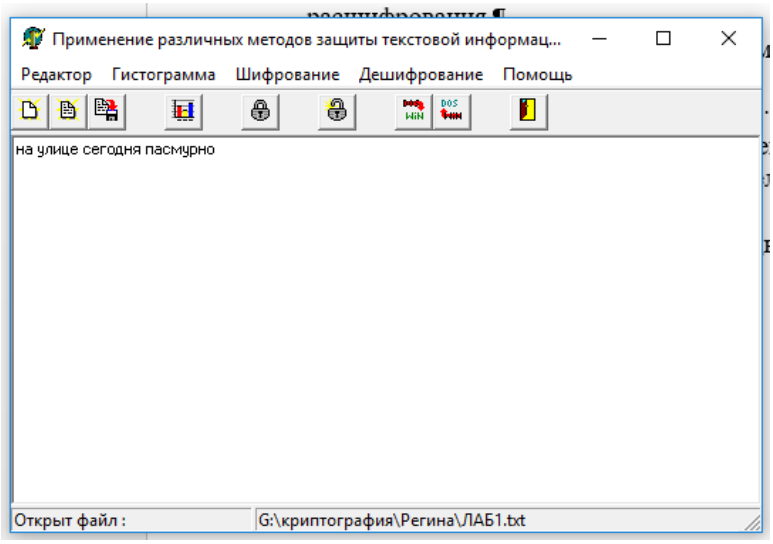
1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?
3. Если необходимо зашифровать текст, содержащий важную информацию, какой метод из рассмотренных вы выберете? Обоснуйте свой выбор.
4. Целесообразно ли повторно применять для уже зашифрованного текста:
а) метод многоалфавитного шифрования;

б) метод Цезаря?
5. Суть одноалфавитный метод.
6. Суть шифрование методом перестановки символов.
7. Суть шифрование инверсными символами (по дополнению до 255).
8. Суть многоалфавитные методы.
9. Определение гистограмма текста.

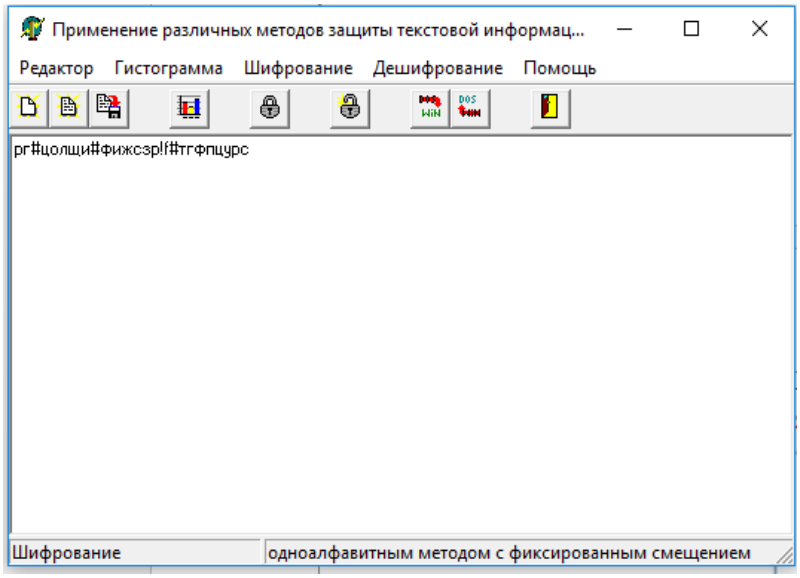
Образец оформления

1. Одноалфавитный метод с фиксированным смещением
2. Одноалфавитный метод с задаваемым смещением (шифр Цезаря)
3. Метод перестановки символов
4. Метод инверсного кодирования (по дополнению до 255)
5. Метод многоалфавитного шифрования с фиксированным ключом
6. Метод многоалфавитного шифрования с ключом фиксированной длины
7. Многоалфавитное шифрование с произвольным паролем

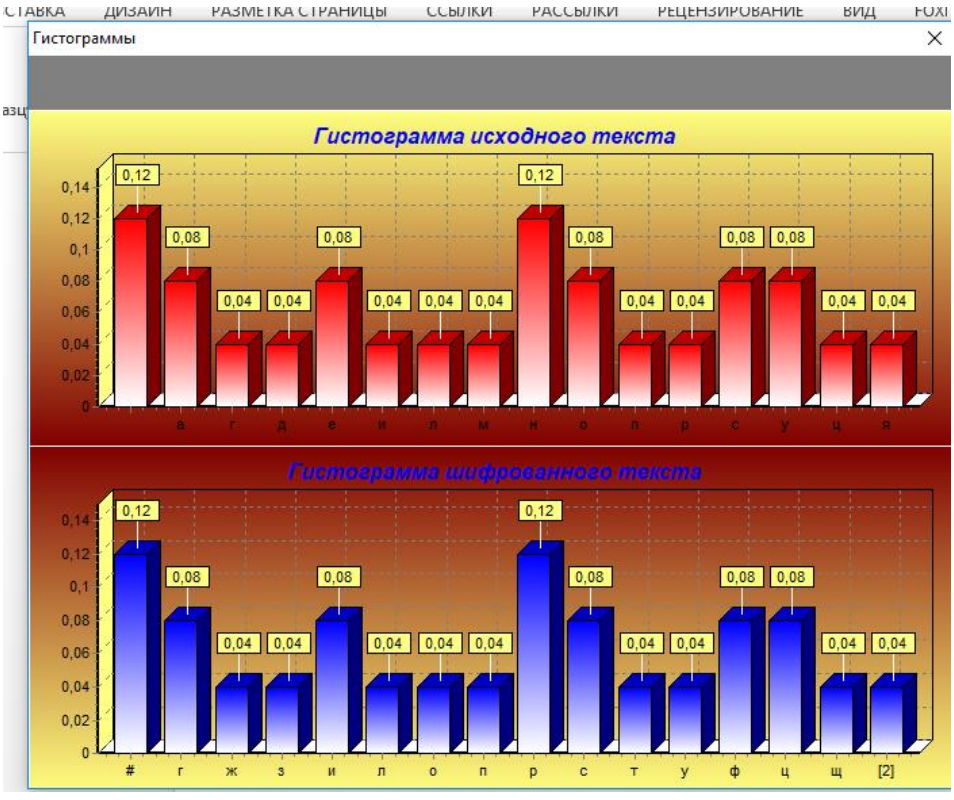
1.Одноалфавитный метод с фиксированным смещением.
Требуется: определить установленное в программе смещение. Для этого следует сделать следующие действия:
Просмотреть предварительно созданный с помощью редактора свой текстовый файл;
Выполнить для этого файла шифрование;
Просмотреть в редакторе зашифрованный файл;
Просмотреть гистограммы исходного и зашифрованного текстов;
Описать гистограммы (схожесть\различия) 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 расшифрования.
В основе этого метода лежит простой способ шифрования: отправитель и получатель зашифрованного документа заранее договариваются об определенном смещении букв относительно их обычного местоположения в алфавите.



Исходный текстовый файл

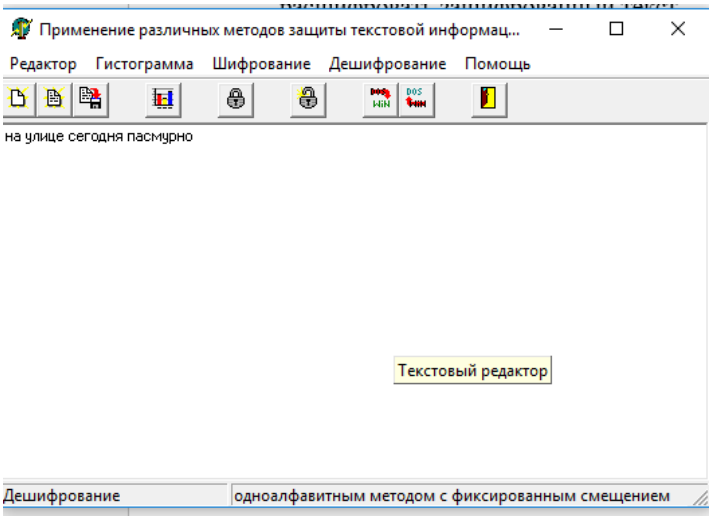


Было выполнено шифрование текста одноалфавитным методом (с фиксированным смещением).



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.

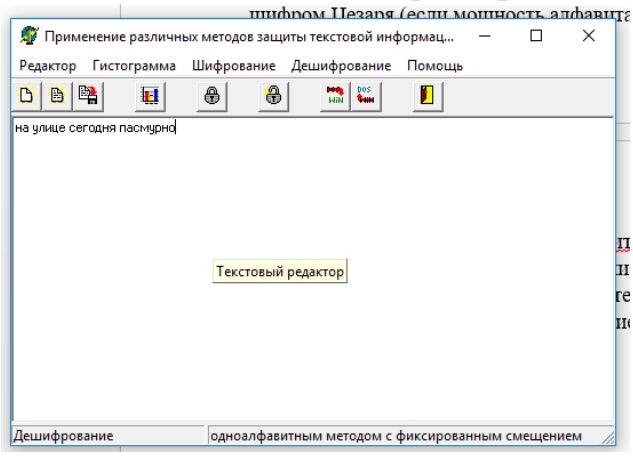


Процесс дешифрования вручную.

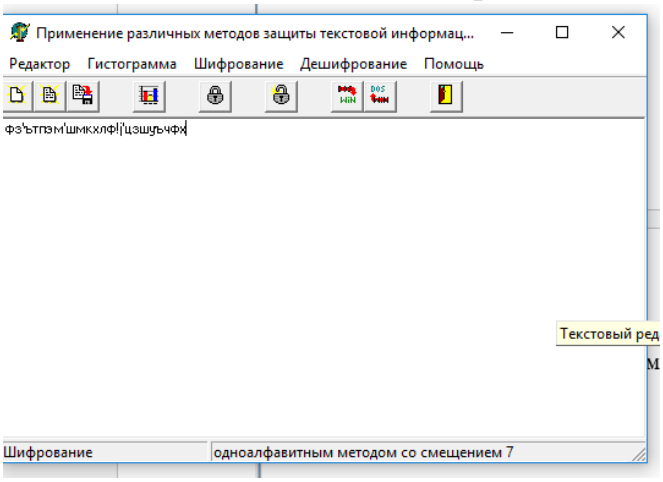
Для определения смещения выделим наиболее часто встречающийся символ шифрованного текста. Найдем символ с той же частотой встречаемости на гистограмме исходного текста. Переведем символы в ASCII-кодировку и определим смещение, посчитав разность между шифрованным символом и исходным.
Гистограмма очень упрощает задачу. Мы видим, что шифрованный символ находится прямо под исходным символом.
Из гистограммы шифрованного текста возьмем наиболее часто встречающийся символ ‘р’. В гистограмме исходного текста ему соответствует символ ‘н’, т.к. он имеет ту же частоту встречаемости 0,12. Из ASCII таблицы код символа ‘р’ равен 144, а код символа ‘н’ равен 141. Вычислим смещение: 144 – 141 = 3.
Т.Е. смещение равняется 3. Это значит, что все остальные символы в шифрованном файле сдвинуты на 3 позиции.

2.Одноалфавитный метод с задаваемым смещением (шифр Цезаря).
Требуется выполнить следующие действия:

Выполнить шифрование с произвольным смещением для своего исходного текста;
Просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
Расшифровать текст с помощью программы;
Дешифровать зашифрованный шифром Цезаря текст с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.
Произвольный шифр из класса одноалфавитных методов не является шифром Цезаря (если мощность алфавита текста равна N, то число шифров Цезаря равноN, а число всех одноалфавитных шифров –N!). Но и для таких методов легко предложить способы дешифрования, основанные на статистических свойствах шифрования текстов, т.к. открытый и закрытый тексты имеют одинаковые статистические характеристики.

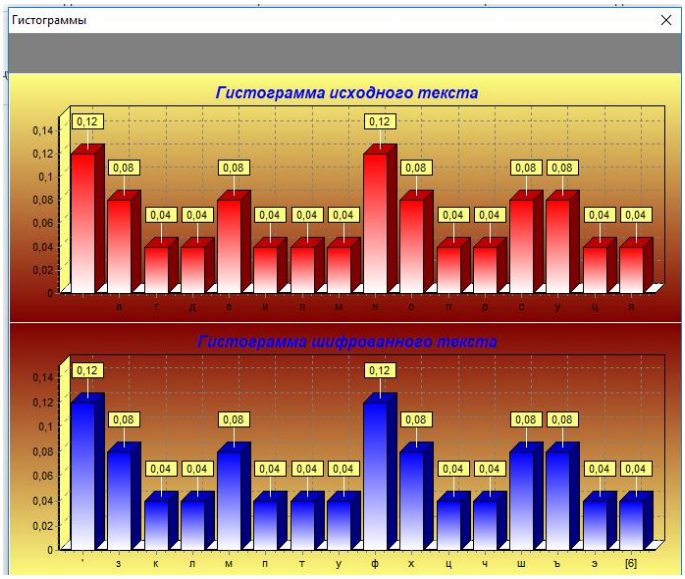


Исходный текстовый файл



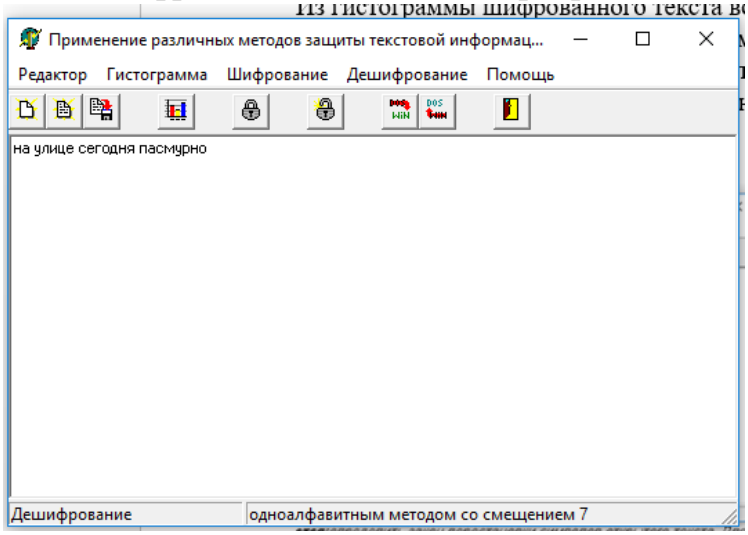
В шифровании использовалось смещение на 7 позиций.

Получены следующие результаты:



Из гистограммы шифрованного текста возьмем наиболее часто встречающийся символ ‘ф’. В гистограмме исходного текста ему соответствует символ ‘н’, т.к. он имеет ту же частоту встречаемости 0,12. Из ASCII таблицы код символа ‘ф’ равен 148, а код символа ‘н’ равен 141. Вычислим смещение: 148 – 141 = 7

Дешифрование с помощью программы.



Как мы видим, дешифрование текста выполнено без ошибок.

3.Метод перестановки символов.

Требуется: определить закон перестановки символов открытого текста. Для этого необходимо:

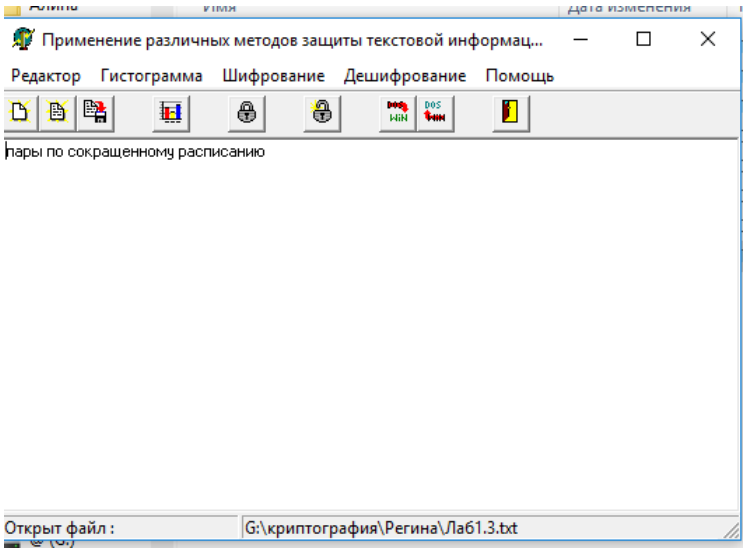
Создать небольшой файл длинной в несколько слов;

Зашифровать его;

Просмотреть гистограммы(описать их и определить, несут ли они в себе полезную информацию или нет);

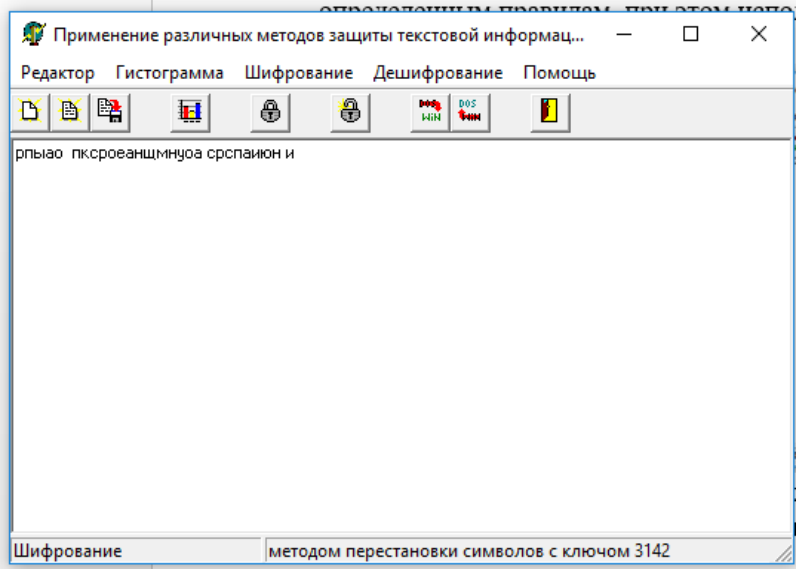
Сравнить результаты дешифровки вручную и с помощью программы.

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

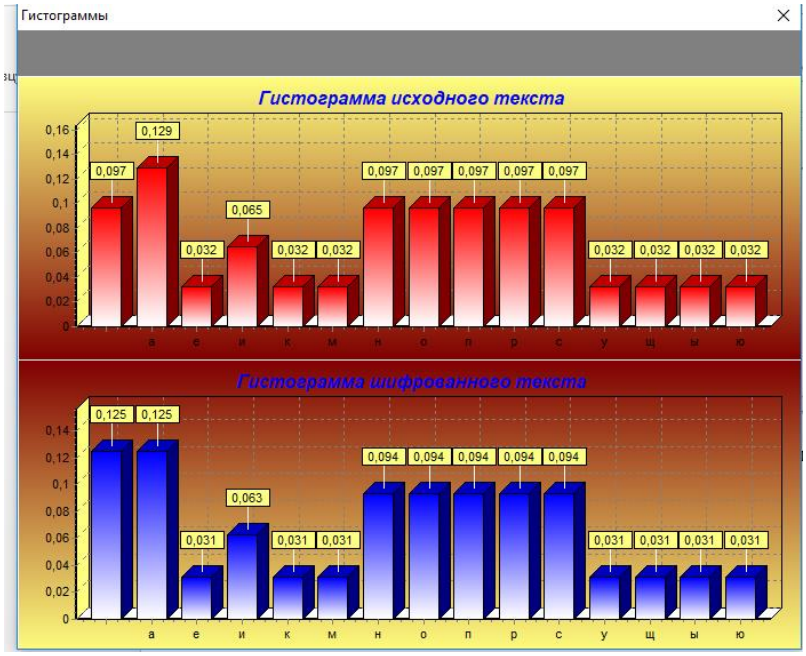


Исходный текстовый файл

После шифрования с ключом 3142, получили:



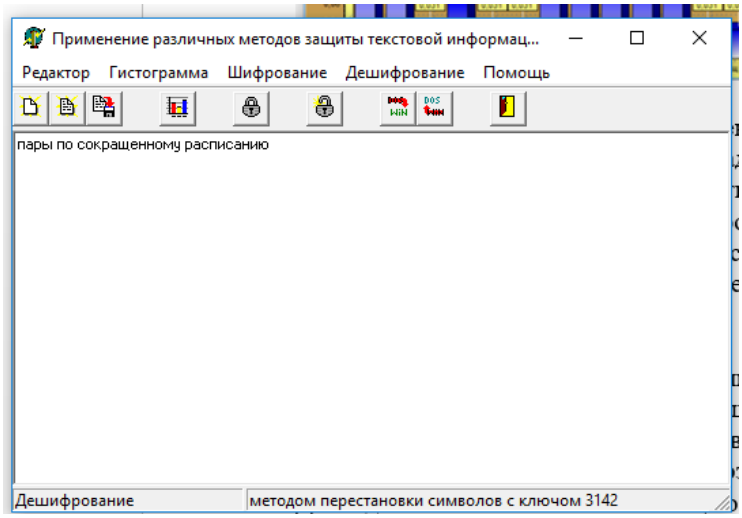
Гистограммы исходного и зашифрованного текстов схожи между собой:



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.

пары по сокращенному расписанию
рпыао_пк**строе**анщм**нуоа**_срс**паию**н_и
пары по сокращенному расписанию
Дешифрование с помощью программы.
Для расшифровки текста, нужно задать тот же ключ, что и при шифровании, т.е. в нашем случае – 3142.

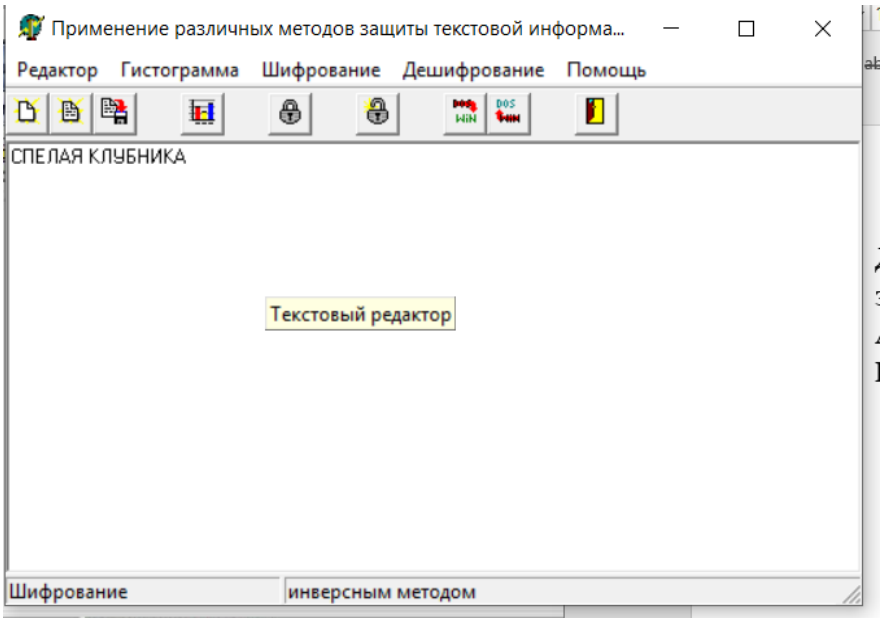


4.Метод инверсного кодирования (по дополнению до 255).

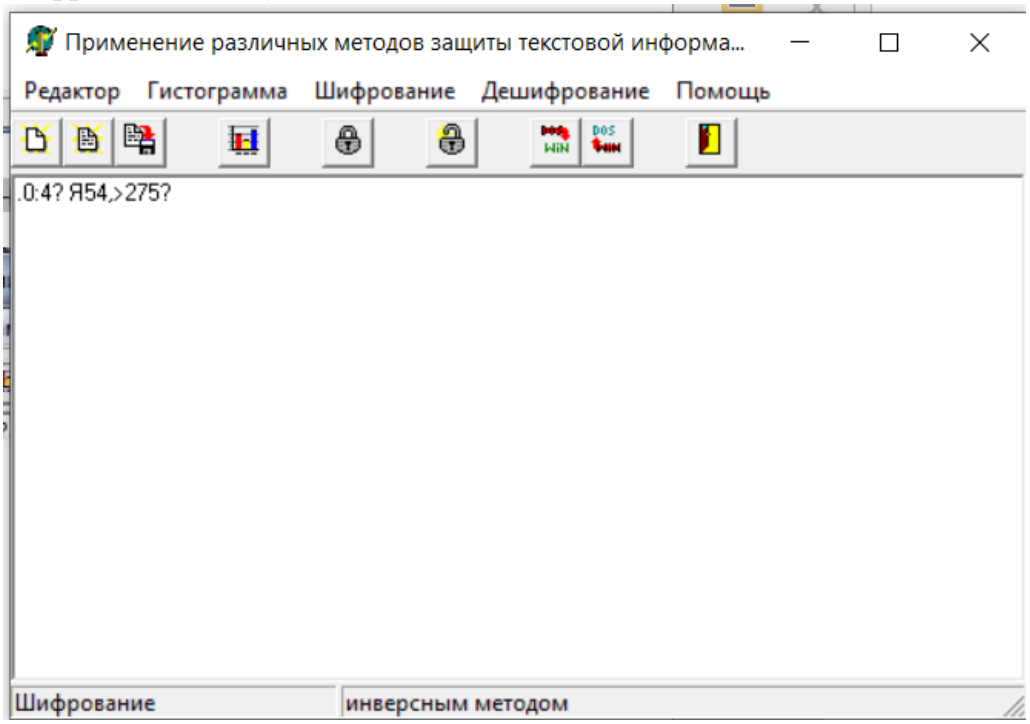
Требуется выполнить след. действия:

- выполнить шифрование для своего произвольного файла;
- просмотреть гистограммы исходного и зашифрованного текстов, описать гистограммы и определить смещение для нескольких символов;
- дешифровать зашифрованный текст, проверить в редакторе правильность дешифрования.

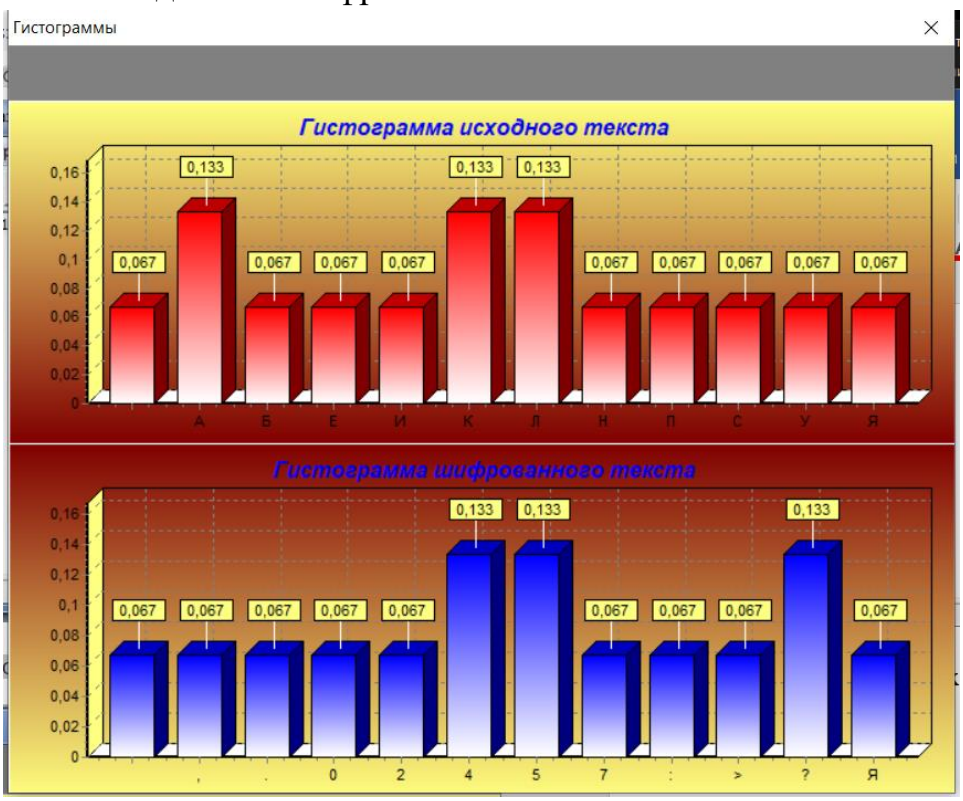
Данный метод шифрования является частным случаем одноалфавитной замены в алфавите мощности 256. Суть метода заключается в замене символа ASCII-кодировки с номером i на символ с номером 255 –i.
Исходный текст:



После шифрования получим:



Гистограммы исходного и шифрованного текстов:



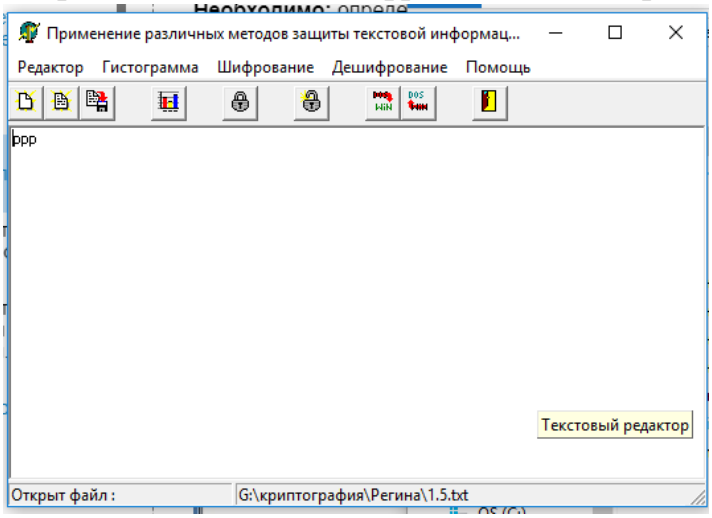
Расшифруем несколько символом вручную:

.0:4? Я54,>275?	Расшифровка символа
1 С0:4? Я54,>275?	255-46(.)=209(С)
2 СП:4? Я54,>275?	255-48(0)=207(П)
3 СПЕ4? Я54,>275?	255-58(:)=197(Е)

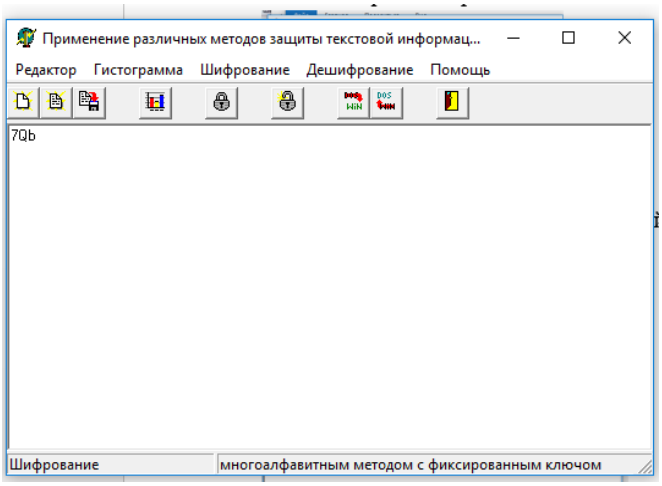
4 СПЕЛ? Я54,>275? 255-52=203(Л)
5 СПЕЛА Я54,>275? 255-63=192(А)
… … …
n Спелая клубника

5.Метод многоалфавитного шифрования с фиксированным ключом.

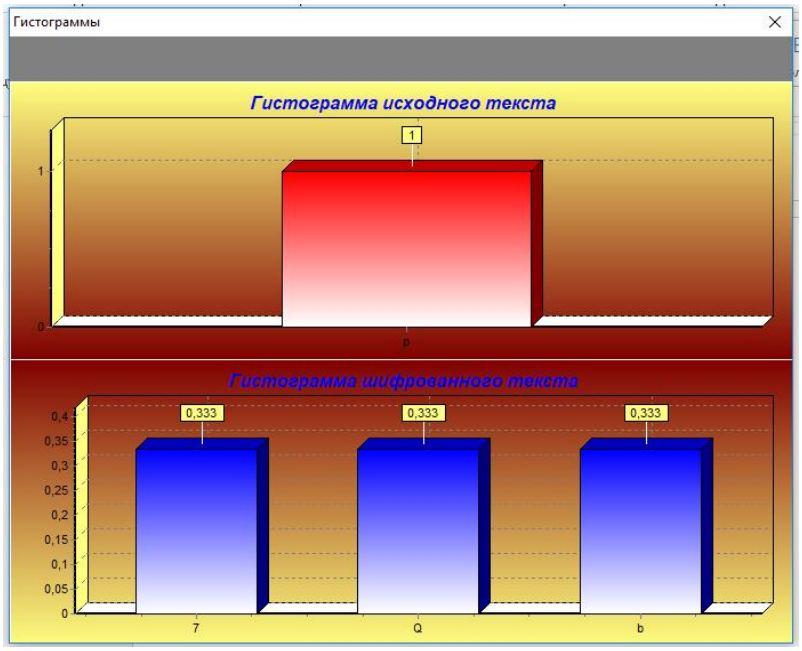
Необходимо: определить сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещения.



Исходный файл



После шифрования получили



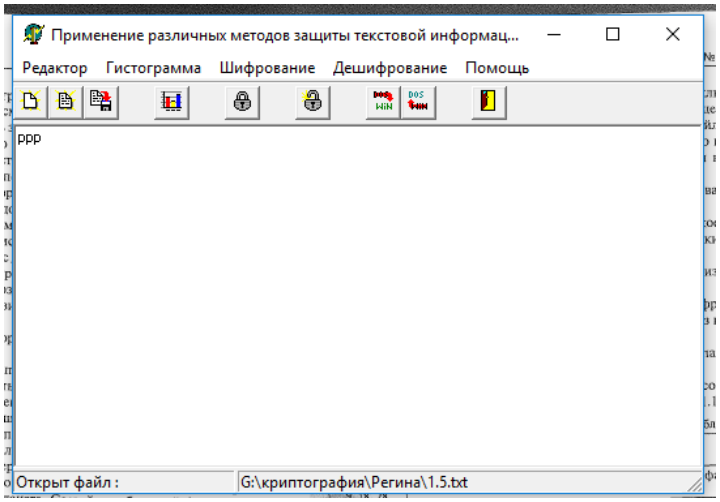
Гистограммы исходной и зашифрованной строки

7=55, Q = 81, b =98
p=240
240 – 55=189
240 – 81= 159
240 – 98 = 142
Для шифрования последовательности из одинаковых символов используется набор из 3-х смещений.

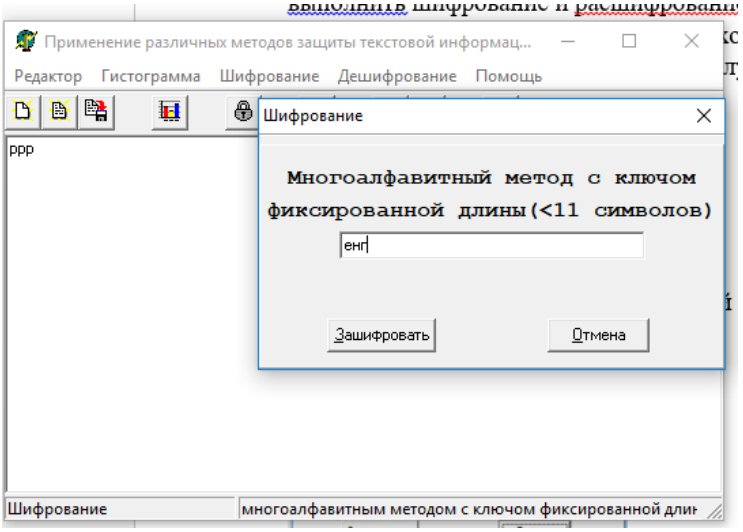
символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код
	32	00100000	8	56	00111000	P	80	01010000	h	104	01101000
!	33	00100001	9	57	00111001	Q	81	01010001	i	105	01101001
"	34	00100010	:	58	00111010	R	82	01010010	j	106	01101010
#	35	00100011	;	59	00111011	S	83	01010011	k	107	01101011
$	36	00100100	<	60	00111100	T	84	01010100	l	108	01101100
%	37	00100101	=	61	00111101	U	85	01010101	m	109	01101101
&	38	00100110	>	62	00111110	V	86	01010110	n	110	01101110
'	39	00100111	?	63	00111111	W	87	01010111	o	111	01101111
(	40	00101000	@	64	01000000	X	88	01011000	p	112	01110000
)	41	00101001	A	65	01000001	Y	89	01011001	q	113	01110001
*	42	00101010	B	66	01000010	Z	90	01011010	r	114	01110010
+	43	00101011	C	67	01000011	[	91	01011011	s	115	01110011
,	44	00101100	D	68	01000100	\	92	01011100	t	116	01110100
-	45	00101101	E	69	01000101	]	93	01011101	u	117	01110101
.	46	00101110	F	70	01000110	^	94	01011110	v	118	01110110
/	47	00101111	G	71	01000111	_	95	01011111	w	119	01110111
0	48	00110000	H	72	01001000	`	96	01100000	x	120	01111000
1	49	00110001	I	73	01001001	a	97	01100001	y	121	01111001
2	50	00110010	J	74	01001010	b	98	01100010	z	122	01111010
3	51	00110011	K	75	01001011	c	99	01100011	{	123	01111011
4	52	00110100	L	76	01001100	d	100	01100100	|	124	01111100
5	53	00110101	M	77	01001101	e	101	01100101	}	125	01111101
6	54	00110110	N	78	01001110	f	102	01100110	~	126	01111110
7	55	00110111	O	79	01001111	g	103	01100111	□	127	01111111

6.Метод многоалфавитного шифрования с ключом фиксированной длины.

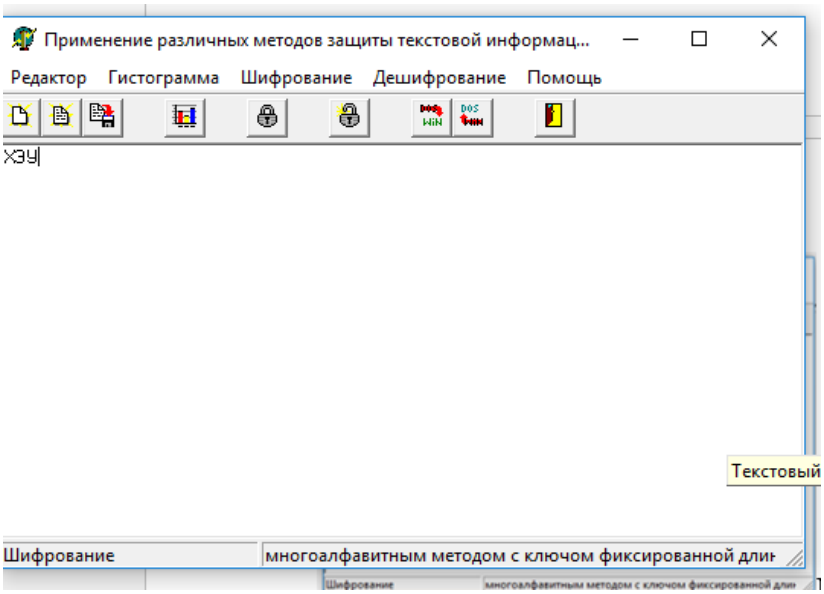
Требуется выполнить след. действия:
выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ;
выполнить шифрование и расшифрование для файла произвольного текста;
просмотреть и описать гистограммы исходного и зашифрованного текстов;
ответить, какую информацию можно получить из гистограмм.



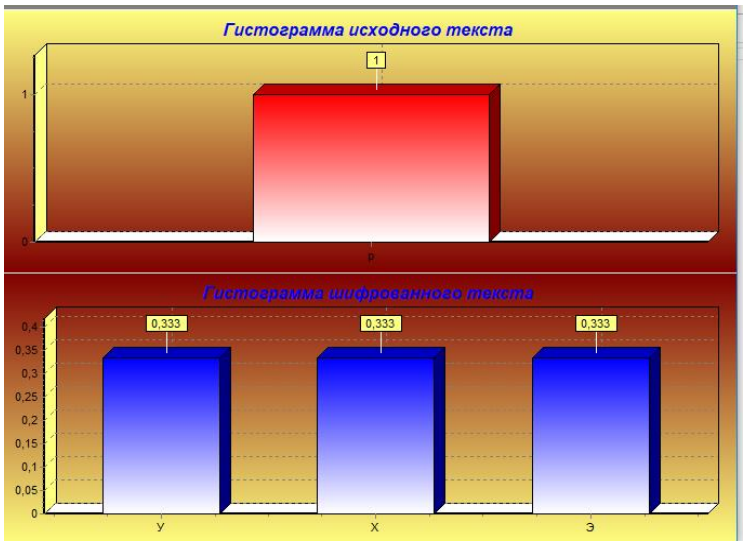
Исходный файл



Вводим ключ шифрования(енг)



Получаем



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

Исход. символ: р – 240;

Ключ:е=229; н=237; г=227;

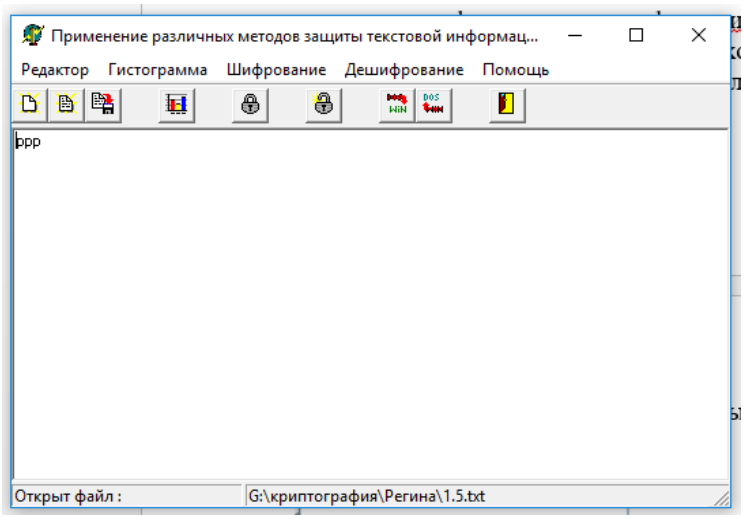
Х = 213 Э = 221 У = 211

7. Многоалфавитное шифрование с произвольным паролем.

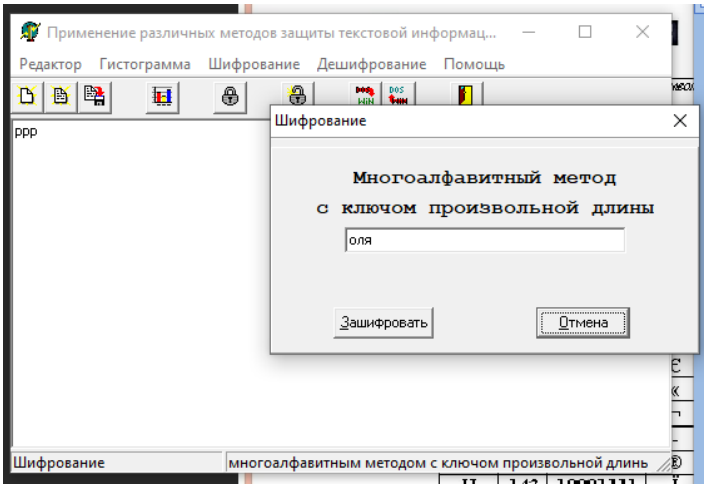
Требуется выполнить след. действия:

выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ;

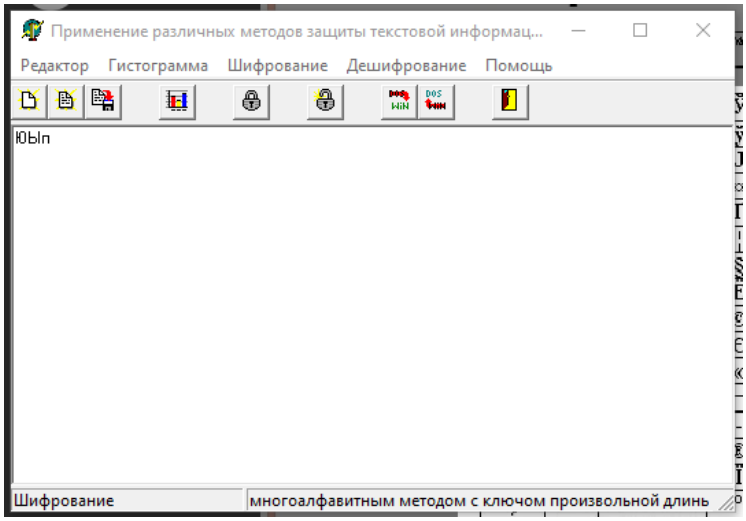
выполнить шифрование и расшифрование для файла произвольного текста; просмотреть и описать гистограммы исходного и зашифрованного текстов; ответить, какую информацию можно получить из гистограмм.



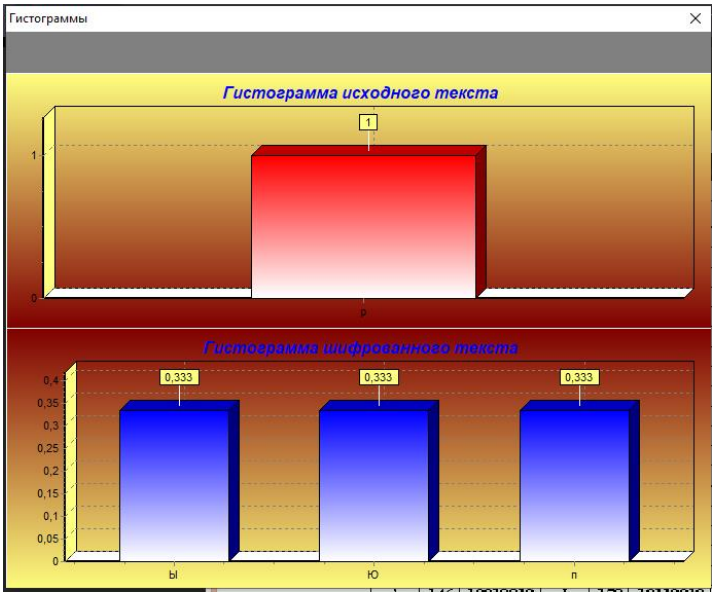
Исходный файл



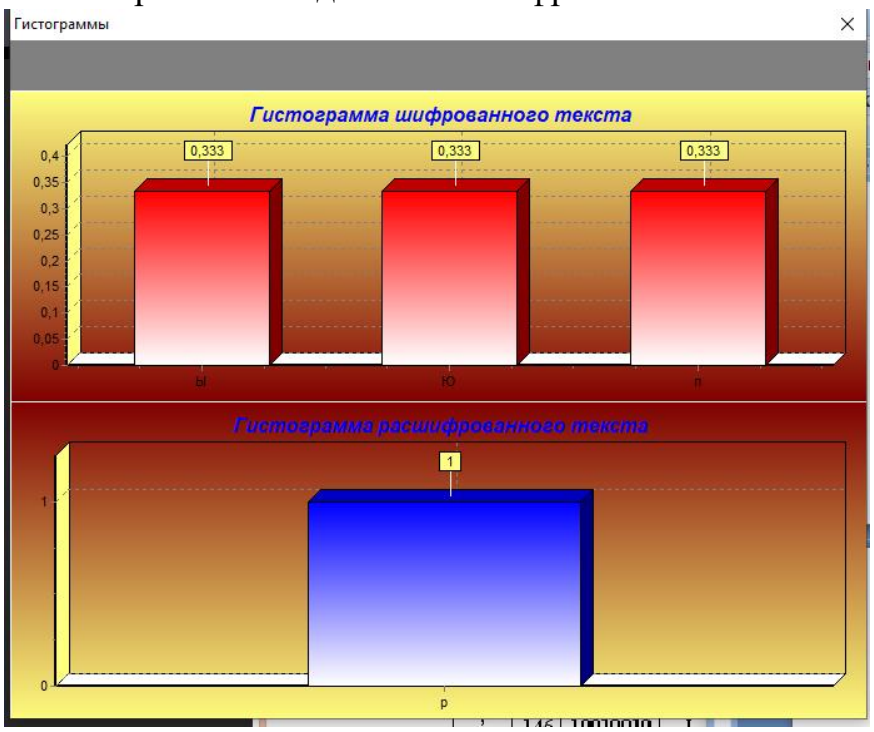
Вводим ключ шифрования (оля)



Получаем



Гистограмма исходного и зашифрованного текстов



Гистограмма зашифрованного и расшифрованного текстов

Перевод символов с помощью ASCIIтаблицы:
Исход. символ: р=240
Ключ:о = 238; л = 235; я = 255
Получаем «ЮЫп» (ASCII-коды: Ю = 222; Ы = 219; п = 239)

Тш=($Т_0$+Тг)mod К, где Тш – зашифрованный символ, $Т_0$ – шифруемый символ (исход.), Тг – задаваемая гамма посл-ть, К– кол-во символов в алфавите(256)

Итак:
(240 + 227)mod 256=478 mod 256=222

(240 + 170)mod 256=454 mod 256=219
(240 + 165)mod 256=495 mod 256=239

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 (с использованием ключа 321), 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”

Варианты
Текст сообщения должны соответствовать варианту задания лабораторной работы 3.

Расширенная таблица ASCII (кириллица)

символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код
Ђ	128	10000000		160	10100000	А	192	11000000	а	224	11100000
Ѓ	129	10000001	Ў	161	10100001	Б	193	11000001	б	225	11100001
‚	130	10000010	ў	162	10100010	В	194	11000010	в	226	11100010
ѓ	131	10000011	Ј	163	10100011	Г	195	11000011	г	227	11100011
„	132	10000100	¤	164	10100100	Д	196	11000100	д	228	11100100
…	133	10000101	Ґ	165	10100101	Е	197	11000101	е	229	11100101
†	134	10000110	¦	166	10100110	Ж	198	11000110	ж	230	11100110
‡	135	10000111	§	167	10100111	З	199	11000111	з	231	11100111
€	136	10001000	Ё	168	10101000	И	200	11001000	и	232	11101000
‰	137	10001001	©	169	10101001	Й	201	11001001	й	233	11101001
Љ	138	10001010	Є	170	10101010	К	202	11001010	к	234	11101010
‹	139	10001011	«	171	10101011	Л	203	11001011	л	235	11101011
Њ	140	10001100	¬	172	10101100	М	204	11001100	м	236	11101100
Ќ	141	10001101	-	173	10101101	Н	205	11001101	н	237	11101101
Ћ	142	10001110	®	174	10101110	О	206	11001110	о	238	11101110
Џ	143	10001111	Ї	175	10101111	П	207	11001111	п	239	11101111
ђ	144	10010000	°	176	10110000	Р	208	11010000	р	240	11110000
‘	145	10010001	±	177	10110001	С	209	11010001	с	241	11110001
’	146	10010010	І	178	10110010	Т	210	11010010	т	242	11110010
“	147	10010011	і	179	10110011	У	211	11010011	у	243	11110011
”	148	10010100	ґ	180	10110100	Ф	212	11010100	ф	244	11110100
•	149	10010101	µ	181	10110101	Х	213	11010101	х	245	11110101
–	150	10010110	¶	182	10110110	Ц	214	11010110	ц	246	11110110
—	151	10010111	·	183	10110111	Ч	215	11010111	ч	247	11110111
	152	10011000	ё	184	10111000	Ш	216	11011000	ш	248	11111000
™	153	10011001	№	185	10111001	Щ	217	11011001	щ	249	11111001
љ	154	10011010	є	186	10111010	Ъ	218	11011010	ъ	250	11111010
›	155	10011011	»	187	10111011	Ы	219	11011011	ы	251	11111011
њ	156	10011100	ј	188	10111100	Ь	220	11011100	ь	252	11111100
ќ	157	10011101	Ѕ	189	10111101	Э	221	11011101	э	253	11111101
ћ	158	10011110	ѕ	190	10111110	Ю	222	11011110	ю	254	11111110
џ	159	10011111	ї	191	10111111	Я	223	11011111	я	255	11111111