

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. ВКБ43

Ковалев Д. П.

Проверил:

Доцент к.т.н Сафарьян О.А.

Ростов-на-Дону

2025

**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.

**Вариант 11.** Шифр-текст: “Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитикам противника”.

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

Для выполнения данного задания нужно создать документ вставить наш исходный текст: “Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитикам противника”.

Изображение выглядит как снимок экрана, текст, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 1 – Исходный текст

Теперь зашифруем наш исходный текст, для этого нужно нажать на “Замок”, который означает зашифровать информацию. Результат представлен на рисунке 2.

Изображение выглядит как текст, Шрифт, линия, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 2 – Зашифрованный текст

После этого воспользуемся действием построением гистограмм, для этого сверху нажимаем “Гистограмма”, а после этого выбираем “Исходные и шифрованные файлы”. В результате должно получиться то, что представлено на рисунке 3.

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Содержимое, созданное искусственным интеллектом, может быть неверным.

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: 0,105 = “и” и самый часто встречающийся символ из гистограммы исходного текста: 0,105 = “л”. Возьмём коды символов из ASCII таблицы. “и” = 232, “л” = 235. Вычислим смещение символов с помощью вычитания кодов: 235–232 = 3. Смещение равно 3 это значит, что все остальные символы в шифрованном файле сдвинуты на 3 позиции. Таблица представлена на рисунке 4.

Изображение выглядит как текст, снимок экрана, черно-белый, шов

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4 – расширенная таблица ASCII

**Задание 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.

Очистим полностью наш редактор от старого текста и теперь введем снова данные – “Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитикам противника”. Теперь нам нужно выбрать шифрование с названием: “Одноалфавитное шифрование с задаваемым смещением”. После этого зашифруем наш исходный текст, выбрав смещение на 5 символов. В результате должно получиться то, что представлено на рисунке 5.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 5 – Зашифрованный текст

Построим теперь гистограмму, чтобы провести частотный анализ символов исходного текста и шифр-текста. В результате должно получиться то, что представлено на рисунке 6.

Изображение выглядит как текст, снимок экрана, Шрифт, графический дизайн

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 6 – Гистограмма исходного и шифрованного текста

Берём самый часто встречающийся символ из гистограммы шифрованного текста: 0,105 = “и” и самый часто встречающийся символ из гистограммы исходного текста: 0,105 = “н”. Возьмём коды символов из ASCII таблицы. “и” = 232, “н” = 237. Вычислим смещение символов с помощью вычитания кодов: 237 – 232 = 5. Смещение равно 5 это значит, что все остальные символы в шифрованном файле сдвинуты на 5 позиции.

Указав данное смещение при дешифровании в программе, как на рисунке 7 получим то, что представлено на рисунке 8.

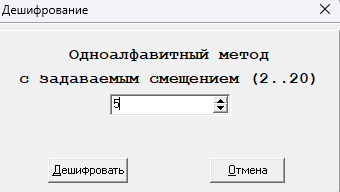


Рисунок 7 – Задание смещения

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 8 - Дешифрованное сообщение

**Задание 3.** Перестановка 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.

Очистим содержимое файла и напишем заново наш исходный текст, после выбора режима шифрования с помощью перестановки символов придумаем ключ. В нашем случае был выбран ключ – 2134, как представлено на рисунке 9.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 9 – создание ключа для метода перестановки

Произведём шифрование исходного текста нашим ключом. В результате получилось то, что представлено на рисунке 10.

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 10 - Зашифрованный текст

Теперь построим гистограмму, как это требуется по условию задания. В нашем случае получилось то, что представлено на рисунке 11.

Изображение выглядит как текст, снимок экрана, Шрифт, диаграмма

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 11 – 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, так как 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 “еВсь”. Сравнив с первыми 4 символа исходного текста определим правило смещения: е – 2 находится на первой позиции, В – 1 находится на второй позиции, с – 3 находится на третьей позиции и ь – 4 находится на четвёртой позиции. Следовательно, можем составить правило перестановки равное 2134. Применим это правила перестановки к остальным частям текста получим исходное сообщение. На рисунке 12 представлено задание правила перестановки.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 12 – Установка правила перестановок

Теперь попробуем расшифровать наш исходный текст, в результате получим то, что представлено на рисунке 13.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 13 – Расшифрованный текст

**Задание 4.** Метод инверсивного кодирования (по дополнению до 255).

Исходный текст для задания 4 представлен на рисунке 14.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 14 – Исходный текст

Теперь нажмем на “Шифрование” и выберем “По дополнению до 255 (инверсионный метод)”. В результате должно получиться то, что представлено на рисунке 15.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 15 – Зашифрованный текст

Теперь построим гистограмму исходного текста и шифрованного текста. Результат представлен на рисунке 16.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 16 – 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.

Расшифруем пару символов с помощью данного алгоритма:

1. =!~ -> В!~ (255 – 61 = 194)
2. В!~ -> Ве~ (255 – 33 = 222)
3. Ве~ -> Вес (255 – 14 = 241)

….

В результате должно получиться то, что представлено на рисунке 17.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 17 – Расшифрованный текст

**Задание 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.

Вставим наш любой произвольный текст для анализа. В нашем случае для примера вставим текст, который состоит из одинаковых символов “б”. Результат представлен на рисунке 18.

Изображение выглядит как снимок экрана, текст, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 18 – Исходный текст

Теперь зашифруем наш исходный текст, в результате получим то, что представлено на рисунке 19. Если выдает ошибку, то была найдена инструкция, которая показывает, как решить проблему: https://yandex.ru/q/question/vydaet\_oshibku\_kogda\_v\_programme\_l\_lux\_d12a5e4a/

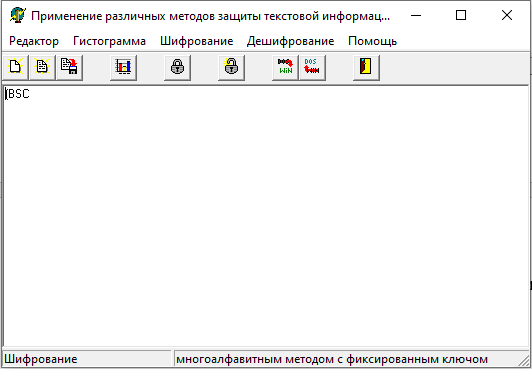


Рисунок 19 – Зашифрованный текст

На рисунке 20 представлена гистограмма для исходного текста и шифрованного.

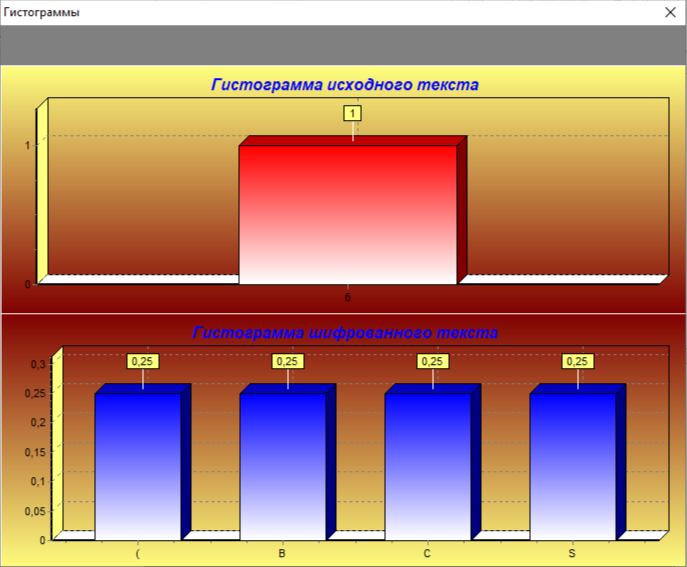


Рисунок 20 – Гистограмма исходного и зашифрованного текста

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 смещений: 225– 40 = 185; 225 – 66 = 159; 225 – 67 = 158; 255 – 83 = 142.

В нашем понимании скорее всего в программе заготовлен исходный ключ, в ином случае не особо становится как понятно, как находится сдвиг.

На рисунке 21 представлен расшифрованный текст.

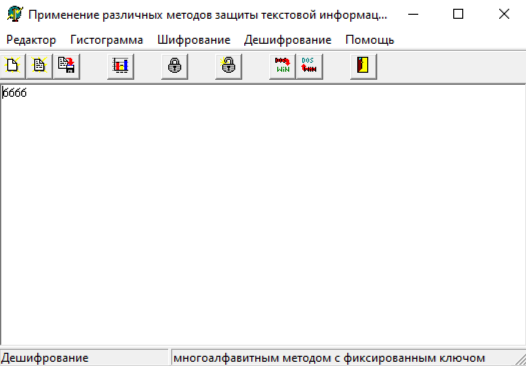


Рисунок 21 – Расшифрованный текст

**Задание 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 текст для шифрования будет использоваться – “бббб”, ключ – “фома”. Зашифрованный текст представлен на рисунке 22. Гистограмма символов исходного текста и шифрованного представлено на рисунке 23.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 22 – Зашифрованный текст

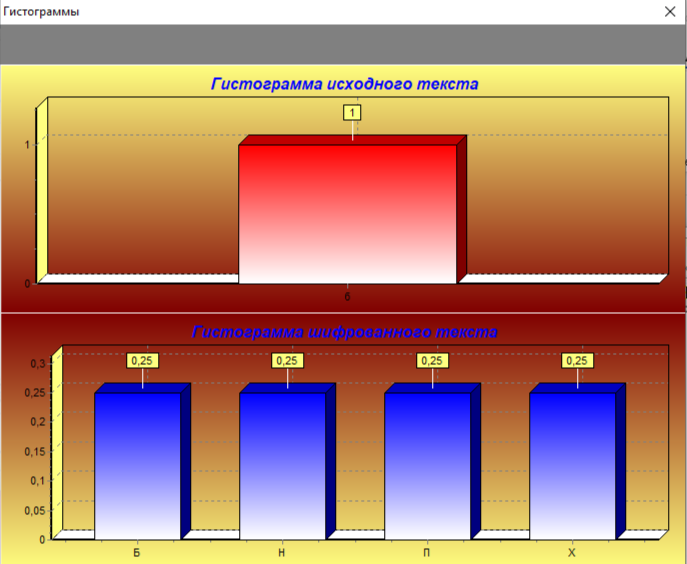


Рисунок 23 – Гистограмма исходного и шифрованного текста

По гистограмме можно определить длину ключа, которым зашифровывался исходный текст. Она соответствует количеству 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. На рисунке 24 представлен расшифрованный текст.

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

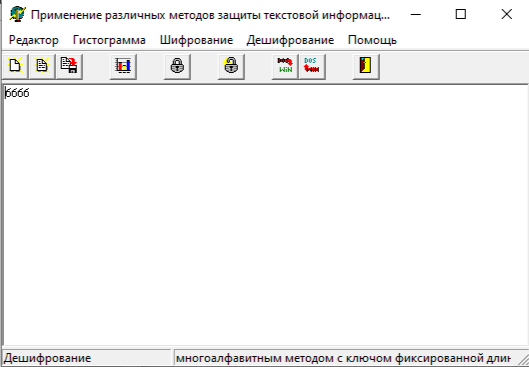


Рисунок 24 – Расшифрованный текст

**Задание 7.** Метод многоалфавитного шифрования с произвольным паролем (с ключом произвольной 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.

Для данного метода будет использоваться исходный текст – “бббб”, как в прошлых заданиях. В качестве ключа будет выступать слово “раос”. В результате получился зашифрованный текст, который представлен на рисунке 25. На рисунке 26 представлена гистограмма исходного текста и зашифрованного.

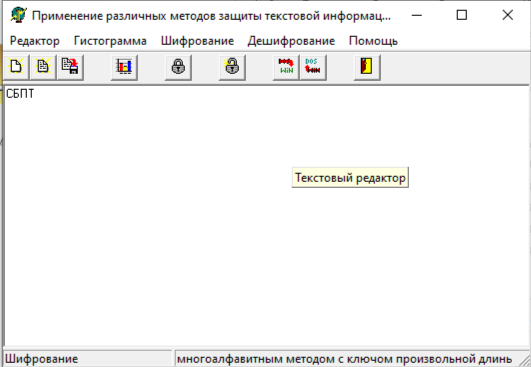


Рисунок 25 – Зашифрованный текст

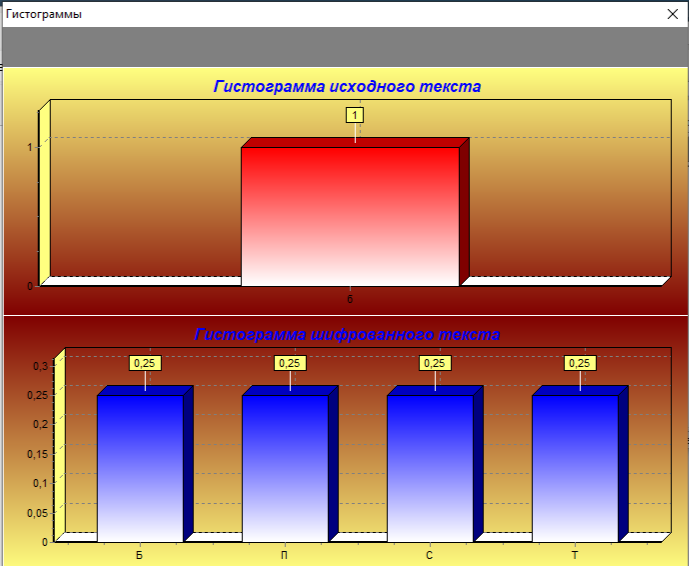


Рисунок 26 – Гистограмма исходного и шифрованного текста

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

Попробуем теперь расшифровать с помощью программы, в результате получим то, что представлено на рисунке 27.

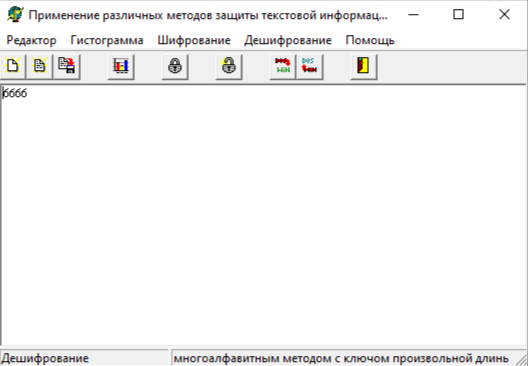


Рисунок 27 – Расшифрованный текст

**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”.