МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №5**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

Содержание

[**Теоретические сведения** 3](#_Toc131362903)

[**Практические задания** 5](#_Toc131362904)

[Задание 1 5](#_Toc131362905)

[Задание 2 6](#_Toc131362906)

[Задание 3 7](#_Toc131362907)

[**Выводы** 9](#_Toc131362908)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров;
* Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров;
* Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования;
* Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях;
* Оценить скорость зашифрования/расшифрования реализованных способов шифров;
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Теоретические сведения**

**Сущность перестановочного шифрования** состоит в том, что исходный текст (из множества *М*) и зашифрованный текст (из множества *С*) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм перестановки.

В классической криптографии шифры перестановки делятся на два подкласса:

* шифры *простой*, или *одинарной*, *перестановки* – при зашифровании символы открытого текста *Мi* перемещаются с исходных позиций в новые (в шифртексте *Сi*) один раз;
* шифры *сложной*, или *множественной*, *перестановки* – при зашифровании символы открытого текста *Мi* перемещаются с исходных позиций в новые (в шифртексте *Сi*) несколько раз.

Основой современных шифров ***маршрутной перестановки*** является геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слево направо, сверху вниз или каким-либо иным образом) записывается открытый текст. Для получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т. е. по иному маршруту.

***Организация маршрутной перестановки***. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

Особенностью шифров ***множественной перестановки*** является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов, но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

# **Практические задания**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

Задание 1:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом использованы маршрутная перестановка (маршрут – по спирали, параметры таблицы – 20х30) и множественная перестановка (ключевые слова- имя и фамилия);

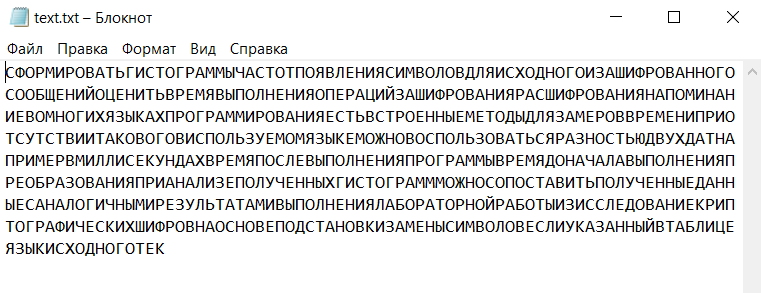
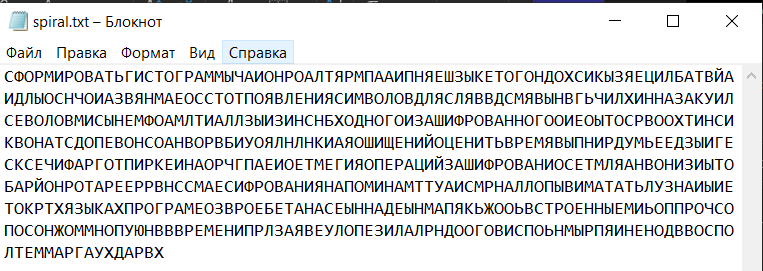


Рисунок 1 — Содержание документа с исходным текстом

Рисунок 2 — Содержание документа, содержащего зашифрованный исходный текст при помощи шифра маршрутной перестановки

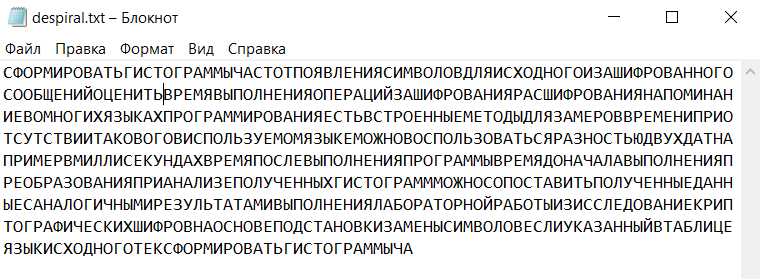


Рисунок 3 — Содержание документа, содержащего расшифрованный текст при помощи шифра маршрутной перестановки

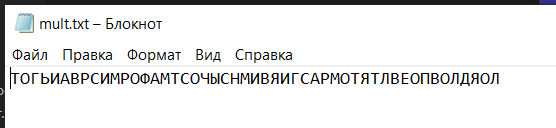


Рисунок 4 — Содержание документа, содержащего зашифрованный исходный текст при помощи шифра множественной перестановки

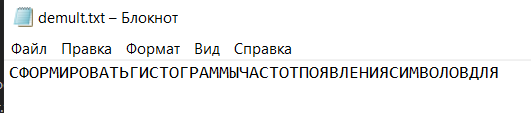


Рисунок 5 — Содержание документа, содержащего расшифрованный текст при помощи шифра множественной перестановки

Задание 2:

* сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений;

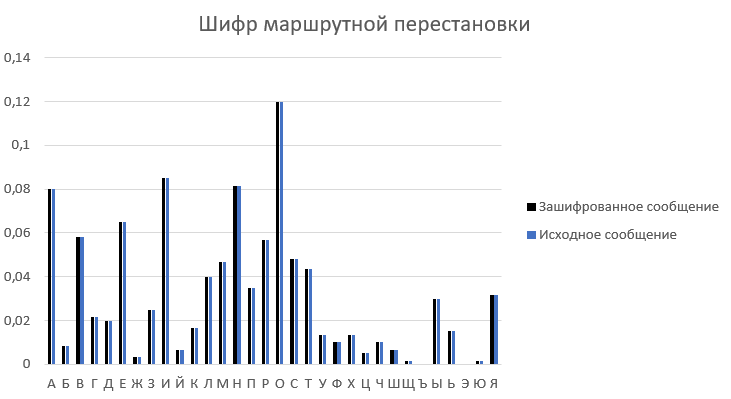


Рисунок 6 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при помощи шифра маршрутной перестановки

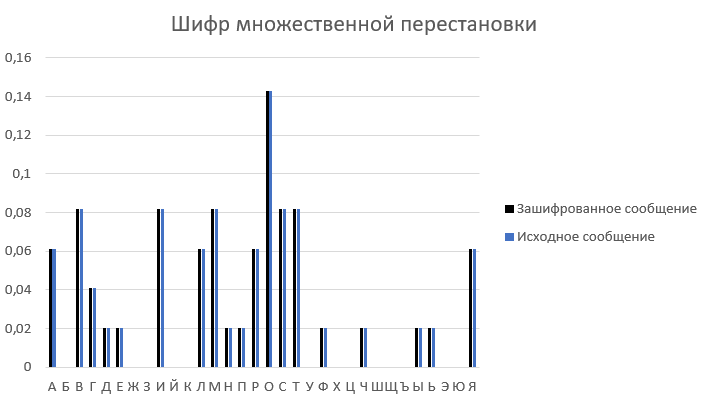


Рисунок 7 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при помощи шифра множественной перестановки

Задание 3:

* оценить время выполнения операций зашифрования/расшифрования.

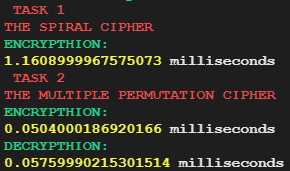


Рисунок 8 — Время выполнения операций зашифрования/расшифрования для шифров маршрутной и множественной перестановок

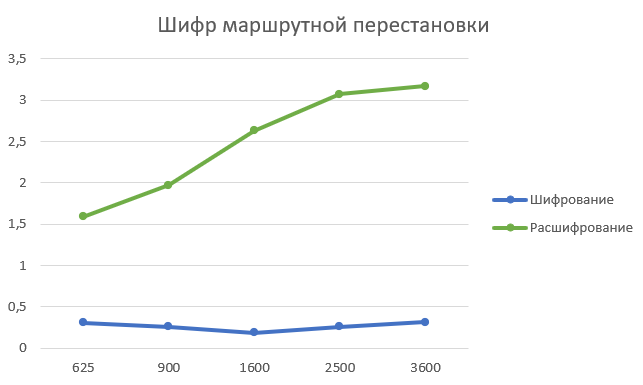


Рисунок 9 — Зависимость времени выполнения зашифрования/расшифрования от количества символов для шифра маршрутной перестановки

# **Выводы**

В ходе выполнения лабораторной работы было разработано приложение, позволяющее выполнять функции зашифрования и расшифрования при помощи шифров маршрутной и множественной перестановок. Так же были построены гистограммы частот появления символов для зашифрованного и исходного сообщений и график зависимости времени выполнения зашифрования/расшифрования от количества символов.

Гистограммы частот появления символов для зашифрованного и исходного сообщений будут одинаковыми, т.к. символы как в зашифрованном, так и в исходном сообщении одни и те же.

Графиком зависимости времени выполнения зашифрования/расшифрования от количества символов для шифра маршрутной перестановки будет являться прямая, т.к. количество символов зависит от количества символов ключей.