МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №6**

по дисциплине «Криптографические методы защиты информации»

на тему: ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»

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](#_Toc132661794)

[**Практические задания** 5](#_Toc132661795)

[Задание 1: 5](#_Toc132661797)

[Задание 2: 5](#_Toc132661798)

[Задание 3: 7](#_Toc132661799)

[**Выводы** 8](#_Toc132661800)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.;
* Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма»;
* Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма»;
* Результаты выполнения лабораторной работы оформить в виде отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

# **Теоретические сведения**

Машина «Энигма» – это электромеханическое устройство.

Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем. Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Изучение устройства и функциональных особенностей шифровальной машины «Энигма». Электрическая часть, в свою очередь, состоит из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).



Рисунок 1 — Спецификация на роторы «Энигмы»

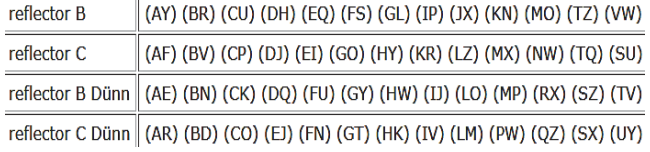


Рисунок 2 — Спецификация на рефлекторы «Энигмы»

# **Практические задания**

Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя (L — II, M — III, R — V, Re — C, Li-Mi-Ri — 1-2-2).

Задание 1:

С помощью разработанного приложения зашифровать сообщение, применив не менее 5 вариантов начальных установок роторов.

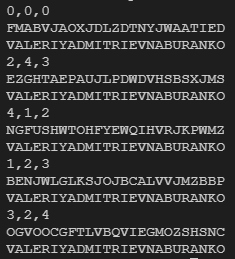


Рисунок 3 — Зашифрование/расшифрование сообщения при различных начальных установках роторов

Задание 2:

Оценить частотные свойства символов в шифртекстах и сравнить этот параметр с частотными свойствами символов для исходного текста.

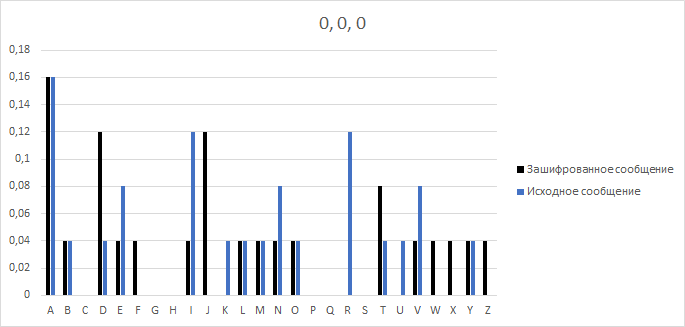


Рисунок 4 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при начальных установках роторов 0-0-0

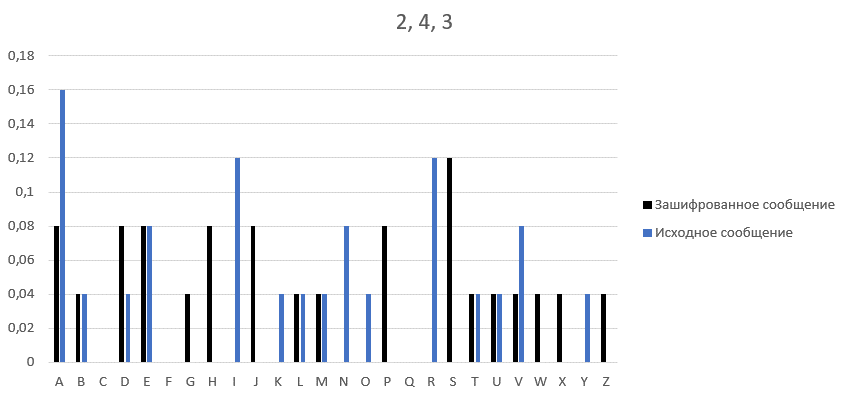


Рисунок 5 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при начальных установках роторов 2-4-3

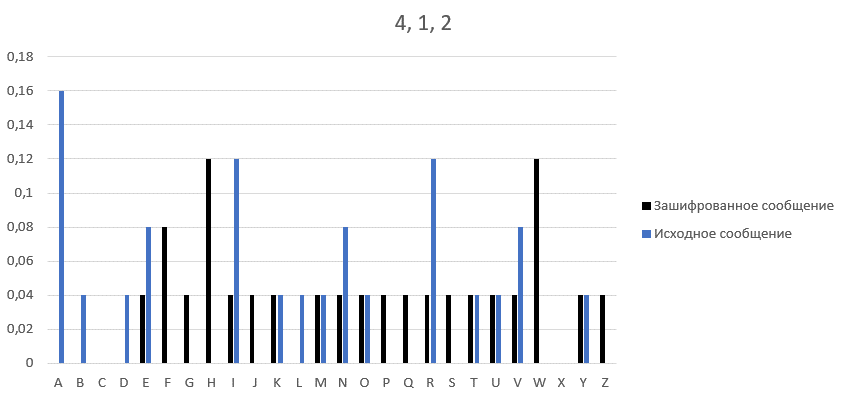


Рисунок 6 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при начальных установках роторов 4-1-2

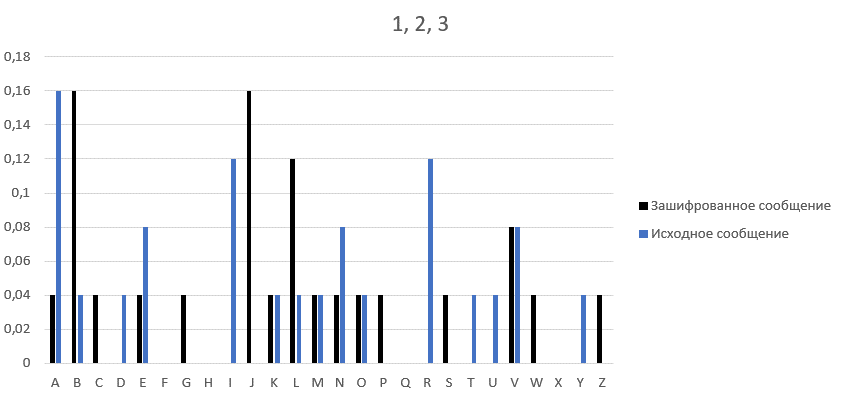


Рисунок 7 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при начальных установках роторов 1-2-3

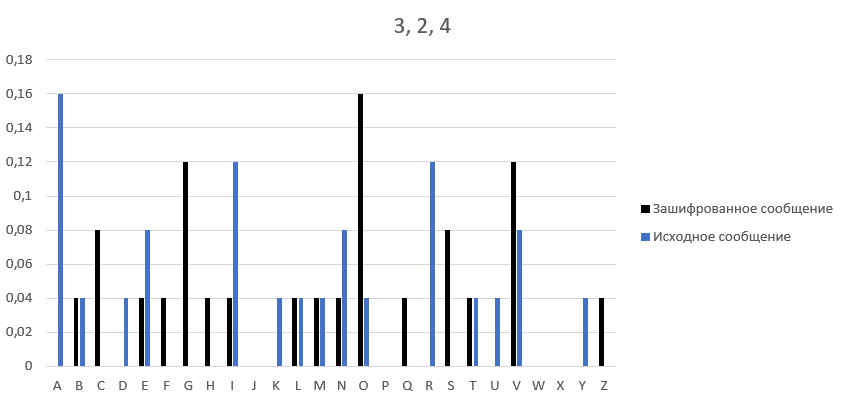


Рисунок 8 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при начальных установках роторов 3-2-4

Задание 3:

Оценить криптостойкость машины.

Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17 576 различных положений ротора (26 · 26 · 26).

Таким образом, практически рассматриваемая версия «Энигмы» может быть настроена на 17 576 различных состояний.

# **Выводы**

В ходе выполнения лабораторной работы было разработано приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Так же были построены гистограммы частот появления символов для зашифрованного и исходного сообщений.

Рассматриваемая версия «Энигмы» может быть настроена на 17 576 различных состояний.