Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Криптографические методы защиты информации**

**Лабораторная работа №6**

ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»

Вариант №6

Выполнил:

Студент 3 курса 4 группы ФИТ

Левша Марк Сергеевич

Минск 2023

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

**Задачи**:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.

2. Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма».

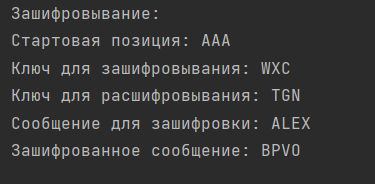
3. Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе «Энигма», реализованной в виде симуляторов.

4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».

5. Результаты выполнения лабораторной работы оформить в виде отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

**Практическое задание**

Было разработано приложение для шифрования текста посимвольно водимого с клавиатуры выводящее входные символы, шаги и результат шифрования символов и полученное сообщение с спользлованием машины “Энигама”, а так же аналогичные шаги расшифрования зашированного сообщения в соответствии с вариантом лабараторной работы.

На рисунках 1 и 2 представлен консольный вывод программы с начальными ключами на роторах *L*, *F*, *V*.

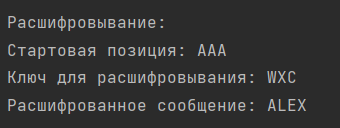
Рис. 1 – Консольный вывод зашифрования символом, используя машину «Энигма»

Рис. 2 – Консольный вывод расшифрованного сообщения, зашифрованного с помощью машины «Энигма»

Чтобы оценить криптостойкость шифра, нужно учитывать все возможные настройки машины. Для этого необходимо рассмотреть следующие свойства «Энигмы»:

• выбор и порядок роторов;

• разводку (коммутацию) роторов;

• настройку колец на каждом из роторов;

• начальное положение роторов в начале сообщения;

• отражатель;

• настройки коммутационной панели.

Мы знаем машину, роторы и внутреннюю развертку этих роторов. Поэтому для оценки криптостойкости можно учитывать только возможные настройки машины «Энигма». Мы можем указать только 3 начальные положения роторов, поэтому существует всего 26^3 = 17 576 вариантов начальных позиций, что является не большим числом вариантов для взлома современными компьютерами.

Если бы можно было бы ещё выбирать 3 ротора из 9 возможных, то количество вариантов выросло в 9! / 3! = 60 480 раз. А если бы был выбор 1 из 3 рефлекторов, то количество вариантов выросло бы ещё в 3 раза.

**Вывод**: в ходе лабораторной работы были изучены примеры машин «Энигма» и была создана приложение-симулятор этой шифровальной машины с определёнными параметрами.