Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №5**

**Тема «****Изучение устройства и функциональных особенностей шифрования машины «Энигма»»**

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

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»

**Машина “Энигма» и перестановочный шифр**

Шифрование происходит благодаря трём роторам и рефлектору. Сначала проходим от правого рефлектора до левого (прямое шифрование) смотря на входной алфавит и соотнося с символом ротора(учитывая смещение начальной позиции), далее символ проходит через рефлектор и получается новый символ. После этого совершается проход от левого ротора до правого (обратное шифрование), при котором смотрим на символ ротора и соотносим с основным алфавитом. Роторы совершают вращение после шифрования одного символа, учитывая фиксированное значение смещения(физически – выемка). При дешифровании всё тоже самое

Код для программы шифрования предоставлен на рисунке 1.1, а результат выполнения на рисунке 1.2

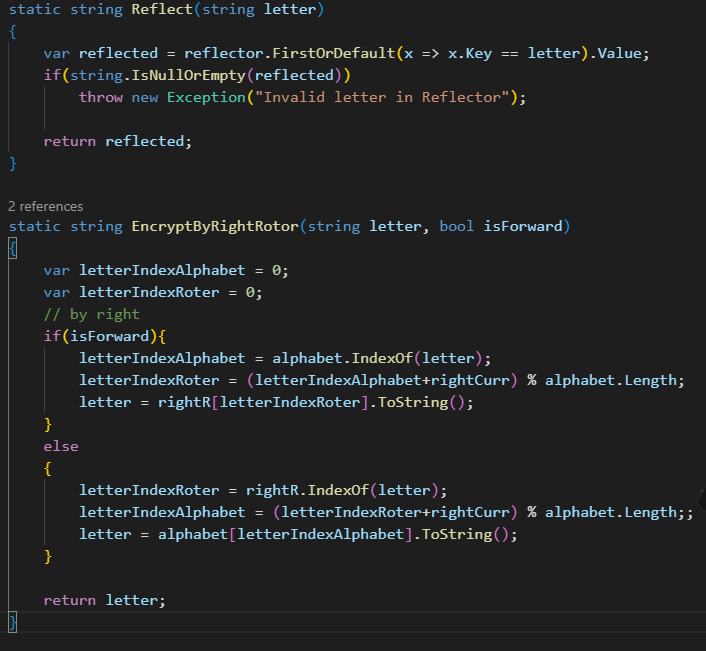


Рисунок 1.1 – Код программы для шифрования

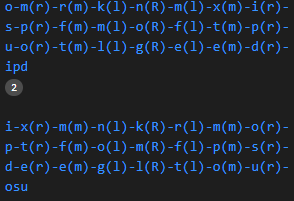


Рисунок 1.2 – Результат выполнения программы

По результатам выполнения программы можно заметить, что шифрование и дешифрование одинаковые (просто перевёрнуты).

Шифрование является криптостойким, т.к. имеет большое количество различных настроек(ротор, позиция ротора, начальное состояние роторов), при шифровании одного и того же символа каждый раз будет разный результат

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации перестановочных шифров.