БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №4**

**«Изучение устройства и функциональных особенностей**

**Шифровальной машины «Энигма»**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

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

**Ход работы**

**Задание.** Разработать приложение, которое реализует операции зашифрования сообщения с помощью алгоритма работы шифровальной машины «Энигма».

По варианту 10 левому ротору соответствует тип гамма, центральному – тип III, правому ротору – бета, используется рефлектор типа С.

В качестве сообщения используется ФИО студента (Потапейко Полина Павловна).

В результате после применения 5 вариантов случайных начальных установок роторов получаем следующие зашифрованные сообщения (рисунок 1).

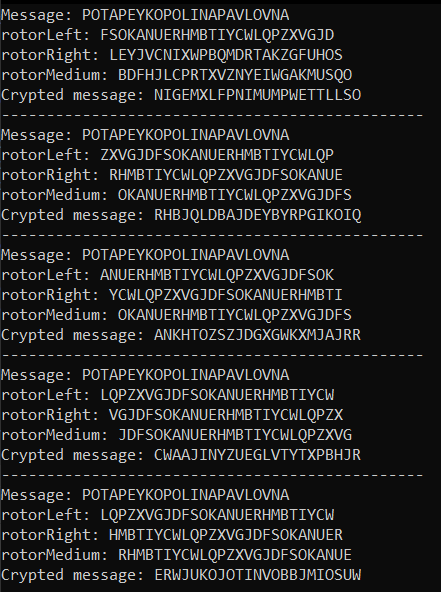


Рисунок 1 – Зашифрование сообщения

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров, изучена структура, принципы функционирования, реализация процедур зашифрования сообщений в машинах семейства «Энигма», изучены и приобретены практические навыки выполнения криптопреобразований информации на платформе «Энигма».