БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №5**

**«Исследование блочных шифров»**»

**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 блочных шифров.

**Ход работы**

**Задание.** Разработать приложение, которое реализует операции выполнения требуемых преобразований ключевой информации, операций зашифрования/расшифрования, оценки скорости выполнения операций зашифрования/расшифрования.

Для реализации выбран алгоритм AES (Advanced Encryption Standard).

В качестве сообщения используется ФИО студента (Potapeyko Polina Pavlovna).

В результате зашифрования и расшифрования получаем данные значения (рисунок 1).

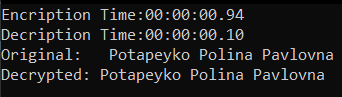


Рисунок 1 – Результат выполнения программы

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости блочных шифров, разработано приложение для реализации заданных методов блочного зашифрования/расшифрования, выполнен анализ криптостойкости блочных шифров, оценена скорость зашифрования/расшифрования реализованных шифров.