БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №6**

**«Исследование потоковых 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 потоковых шифров.

**Ход работы**

**Задание.** Разработать приложение, которое реализует генерацию ПСП алгоритмом BBS и алгоритм RC4.

Результат выполнения программы представлен на рисунке 1.

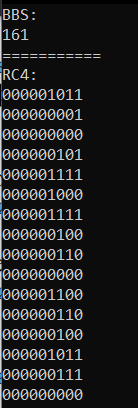


Рисунок 1 – Результат выполнения программы

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