Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Криптографические методы защиты информации**

**Лабораторная работа №8**

ИССЛЕДОВАНИЕ ПОТОКОВЫХ ШИФРОВ

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 потоковых шифров.

**Задачи**:

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

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.

3. Выполнить анализ криптостойкости потоковых шифров.

4. Оценить скорость зашифрования/расшифрования реализованных шифров.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Практическое задание**

Было разработано приложение, реализующее генераторы ПСП на основе алгоритмов RSA и RC4. Так же приложение высчитывает время выполнения генерации последовательностей.

Вывод программы представлен на рисунке 1.

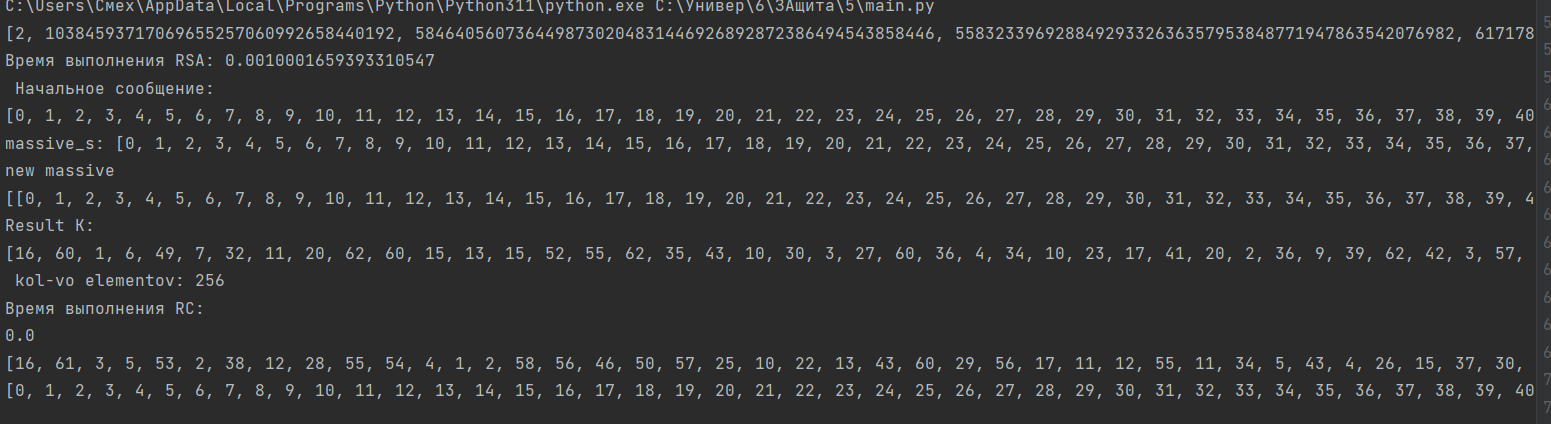


Рис. 1 – вывод консоли программы

### Для генерации ПСП в алгоритме RSA для нахождения членов последовательности используется соотношение *xt* ≡ (*xt*–1)*е* mod *n*. Из соответствия следует, что для получения ПСП нужен первый элемент, от которого надо отталкиваться, который будет не равен 1.

### В алгоритме RSA *p* и *q* были выбраны 99996615615953329556773283 и 75503096001852492674291743 соответственно, а число *e* было выбрано 133 т.к. оно взаимно простое с функцией эйлера *n*, где *n = q*×*p.*

Зависимость выполнения операций от количества этих операций в алгоритме RSA представлена на рисунке 2.



Рис. 2 – график зависимости выполнения операций от количества этих операций

**Вывод**: в ходе лабораторной работы были реализованы генераторы ПСП на основе алгоритма RSA и RC4 так же были рассмотрены другие генераторы ПСП.