Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №8**

Исследование потоковых шифров

Выполнил:

Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

1. **Потоковые шифры**

Потоковый шифр это – симметричный шифр, преобразующий каждый символ *mi* открытого текста в символ шифрованного *ci*, зависящий от ключа и расположения символа в текст98е.

Основной задачей потоковых шифров является выработка некоторой последовательности (гаммы) для зашифрования, то есть выходная гамма является ключевым потоком (ключом) для сообщения.

Потоковый шифр максимально должен имитировать одноразовый блокнот. В соответствии с этим ключ должен по своим свойствам максимально походить на случайную числовую последовательность. Ключевые последовательности (случайные последовательности (СП), либо псевдослучайные последовательности (ПСП)) вырабатываются специальными блоками систем потокового шифрования – генераторами.

**Задание 1:** Генерация ПСП используя алгоритм RSA.

Алгоритм RSA разработан для асимметричного зашифрования/расшифрования. Генерация ПСП происходит на основе соотношения, в котором начальными параметрами служат n, большие простые числа *p* и *q* (причём *n = pq*), целое число e, взаимно простое с произведением (*p-1*) (*q-1*), а также некоторое случайное начальное значение *x0*.

Для генерации ПСП используя алгоритм генерации RSA было разработано приложение используя язык Python. Результат выполнения представлен на рисунке 1.1:

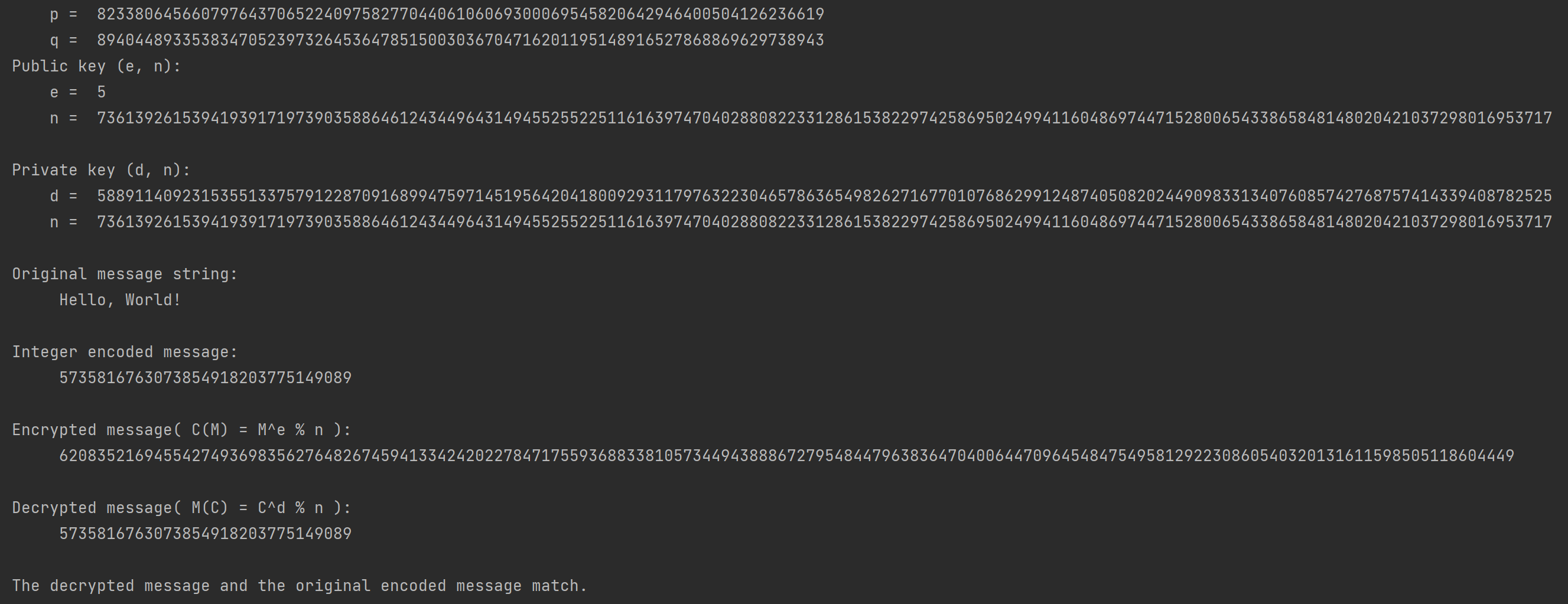


Рисунок 1.1 – Результат генерации ПСП с помощью RSA

**Задание 2:** Шифрование алгоритмом RC4

Алгоритм RC4, как и любой потоковый шифр, строится на основе генератора псевдослучайных битов (генератора ПСП). На вход генератора записывается ключ, а на выходе читаются псевдослучайные биты. Длина ключа может составлять от 40 до 2048 битов.

Ядро алгоритма состоит из функции генерации ключевого потока. Другая часть алгоритма – функция инициализации, которая использует ключ переменной длины *Ki* для создания начального состояния генератора ключевого потока.

Для реализации алгоритма была разработана программа на Python. Результат выполнения шифрования и дешифрования показан на рисунке 2.1 и 2.2 соответственно.

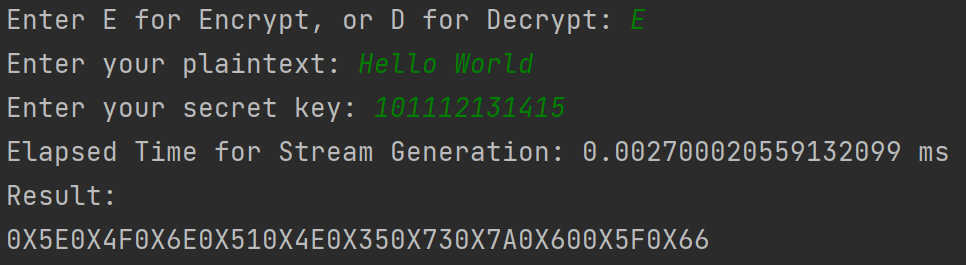


Рисунок 2.1 – Результат шифрования текста используя алгоритм RC4

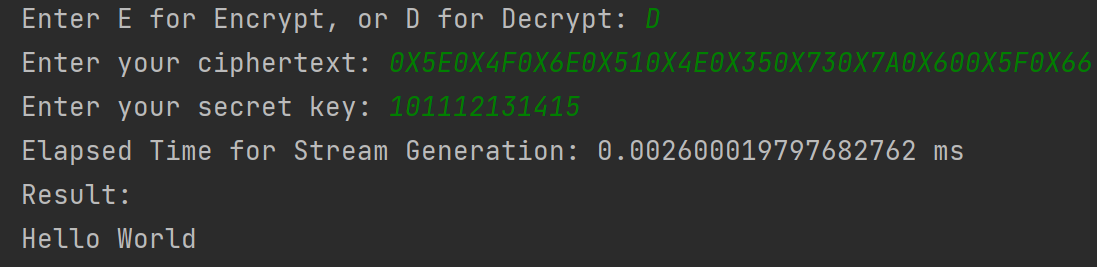


Рисунок 2.2 – Результат дешифрования текста используя алгоритм RC4

Для оценки времени выполнения операций генерации ПСП были проведены измерения. Результат приведен на рисунке 2.3.

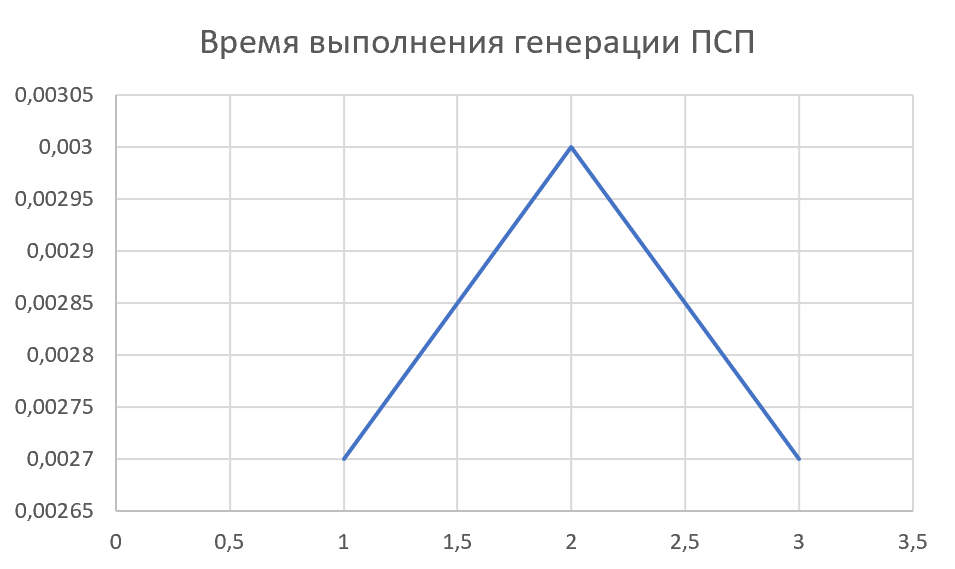


Рисунок 2.3 – Время выполнения генерации ПСП

**Вывод:** В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования потоковых шифров. А также произведена оценка скорости генерации ПСП различной длины.