МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №8**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ ПОТОКОВЫХ ШИФРОВ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

**Содержание**

[Практические задания 4](#_Toc136180293)

[Задание 1 4](#_Toc136180295)

[Задание 2 4](#_Toc136180296)

[Выводы 5](#_Toc136180297)

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

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости потоковых шифров;
* Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования;
* Выполнить анализ криптостойкости потоковых шифров;
* Оценить скорость зашифрования/расшифрования реализованных шифров;
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Практические задания**

Разработать авторское приложение в соответствии с целью лабораторной работы.

Задание 1:

С помощью разработанного приложения зашифровать сообщение «Buranko Valeria» при помощи алгоритма RSA, используя ключи, размерностью 256 бит.

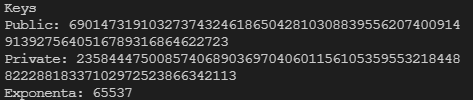


Рисунок 1 — Сгенерируемые ключи для зашифрования/расшифрования сообщения при помощи алгоритма RSA



Рисунок 2 — Результаты выполнения функций зашифрования/расшифрования алгоритмом RSA

Задание 2:

Приложение так же должно реализовывать алгоритм RC4, используя ключ «76, 111, 85, 54, 211» и выполнять оценку скорости выполнения операций.

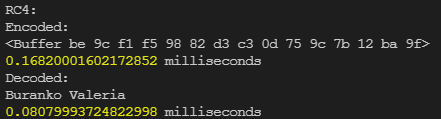


Рисунок 3 — Результаты выполнения операций зашифрования/расшифрования при помощи алгоритма RC4 и скорости выполнения операций

# **Выводы**

В ходе выполнения данной лабораторной работы мы изучили и приобрели практические навыки разработки и использования приложений для реализации потоковых шифров. Мы ознакомились с различными видами потоковых шифров, а также с особенностями их реализации в коде.