МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №9**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ АССИМЕТРИЧНЫХ 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 5](#_Toc136180296)

[Выводы 6](#_Toc136180297)

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

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости ассиметричных шифров;
* Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для ассиметричного зашифрования/расшифрования;
* Выполнить анализ криптостойкости ассиметричных 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:

Приложение должно реализовывать следующие операции:

* генерация сверхвозрастающей последовательности (тайного ключа); старший член последовательности – 100-битное число; в простейшем случае принимается *z* = 6 (для кодировки Base64) и *z* = 8 (для кодировки ASCII);
* вычисление нормальной последовательности (открытого ключа);
* зашифрование сообщения, состоящего из собственных фамилии, имени и отчества;
* расшифрование сообщения;
* оценка времени выполнения операций зашифрования и расшифрования.

Для начала нужно сгенерировать тайный и открытый ключ.

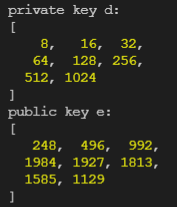


Рисунок 1 — Тайный и открытый ключи

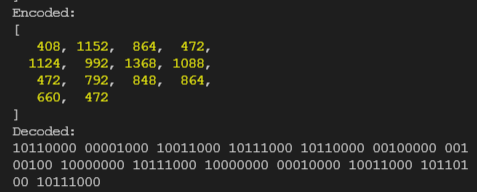


Рисунок 2 — Пример работы алгоритма на основе сообщения «BurankoValeria»

Задание 2:

Проанализировать время выполнения операций зашифрования/расшифрования при увеличении числа членов ключевой последовательности; при использовании разных таблиц кодировки.

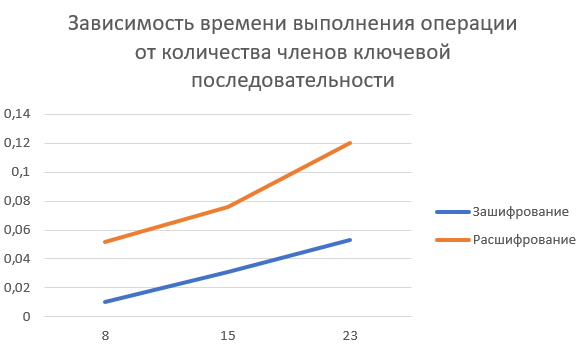


Рисунок 3 — График зависимости времени выполнения операция зашифрования/расшифрования от количества членов ключевой последовательности

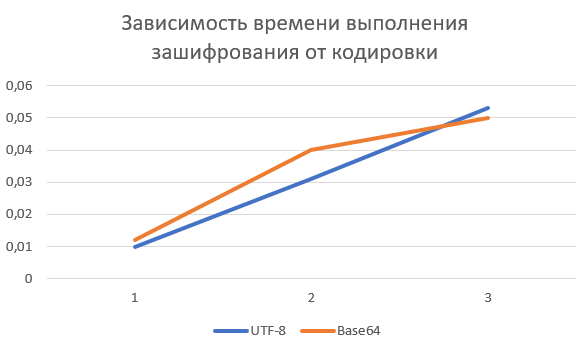


Рисунок 4 — График зависимости времени выполнения операции зашифрования от кодировки

# **Выводы**

В ходе выполнения данной лабораторной работы мы изучили и приобрели практические навыки разработки и использования приложений для реализации ассиметричных шифров. При увеличении числа членов ключевой последовательности увеличивается и время выполнения операций зашифрования/расшифрования. При использовании кодировок UTF-8 и Base64 время выполнения операция отличается незначительно.