МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №10**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ АССИМЕТРИЧНЫХ ШИФРОВ RSA И ЭЛЬ-ГАМАЛЯ

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 8](#_Toc136180297)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации ассиметричных шифров RSA и Эль-Гамаля.

**Задачи:**

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

Составить табличную форму форму зависимости времени вычисления параметра *у*, функционально заданного выражением вида:

Вывод в консоль представлен на рисунке 1.



Рисунок 1 — Вывод в консоль зависимости вычисления параметра y

Задание 2:

Приложение должно реализовывать следующие операции:

* + - зашифрование и расшифрование текстовых документов на основе алгоритмов RSA и Эль-Гамаля;
* определение времени выполнения операций.

Исходный текст для зашифрования – собственные фамилия, имя, отчество.

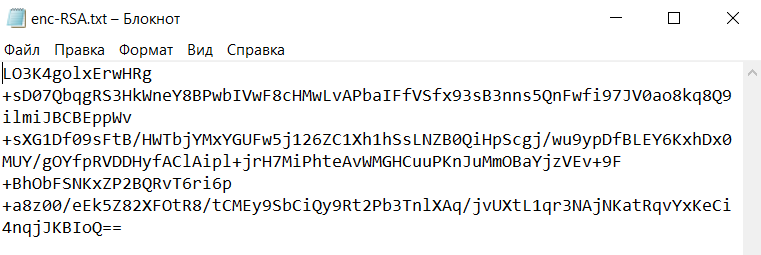


Рисунок 2 — Зашифрованное сообщение алгоритмом RSA

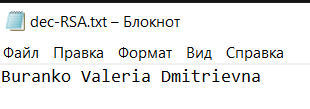


Рисунок 3 — Расшифрованное сообщение алгоритмом RSA

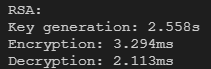


Рисунок 4 — Время выполнения операций алгоритма RSA

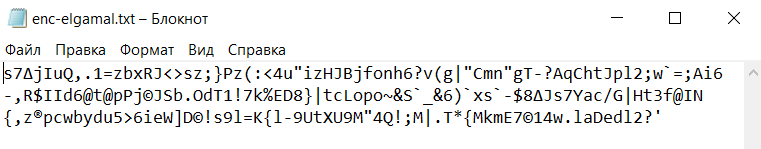


Рисунок 5 — Зашифрованное сообщение алгоритмом Эль-Гамаля

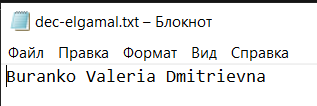


Рисунок 6 — Зашифрованное сообщение алгоритмом Эль-Гамаля

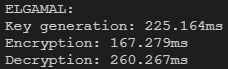


Рисунок 7 — Время выполнения операций алгоритма Эль-Гамаля

Чтобы оценить скорость работы и изменение объема криптотекстов, построим графики. На рисунке 8 представлен график зависимости выполнения алгоритмов от количества символов в сообщении.

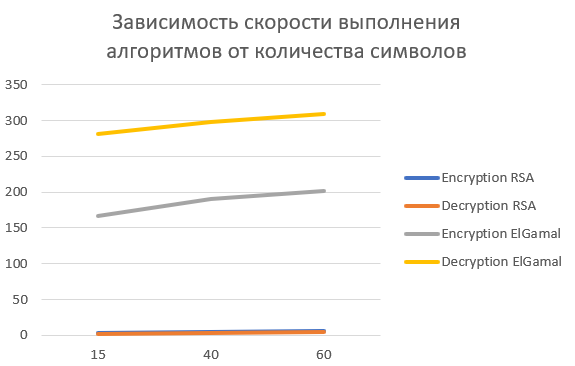


Рисунок 8 — График зависимости скорости выполнения алгоритма, от кол-ва символов в сообщении

На рисунке 9 представлена зависимость количества символов от выбранного алгоритма шифрования.

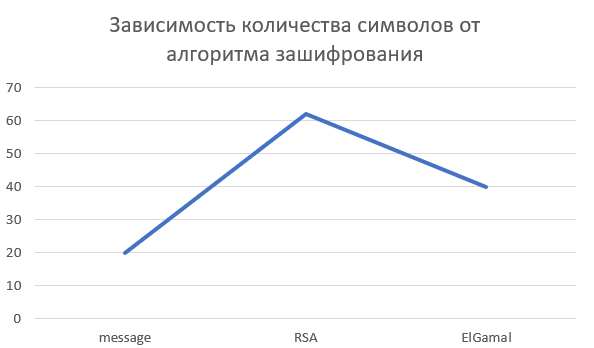


Рисунок 9 – Зависимость количества символов от алгоритма шифрования

Можно заметить, что больше всего места занимает шифротекст в RSA, Эль-Гамаля увеличивает количество в 2 раза, поскольку число представляет собой пару чисел.

# **Выводы**

В ходе выполнения данной лабораторной работы мы изучили и приобрели практические навыки разработки и использования приложений для реализации ассиметричных шифров RSA и Эль-Гамаля.