МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №13**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ

АЛГОРИТМОВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ

КРИВЫХ

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](#_Toc136540851)

[Задание 1 4](#_Toc136540852)

[Задание 2 4](#_Toc136540853)

[Задание 3 5](#_Toc136540854)

[Выводы 6](#_Toc136540855)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми (ЭК):
  + по алгоритмам согласования ключевой информации на основе ЭК;
  + алгоритмам зашифрования/расшифрования информации на основе асимметричной криптографии и ЭК;
  + алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК;
  + оценке криптостойкости систем на основе ЭК.
* Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК;
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Практические задания**

## Задание 1

Найти точки ЭК для значений х, где *хмин* = 36, а *хмакс* = 70.

Для реализации данного задания можно с помощью цикла от 141 до 175 посчитать значения по формуле:

Результат работы алгоритма представлен на рисунке 1.

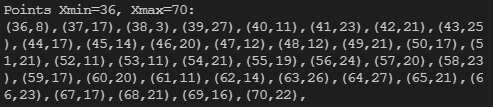


Рисунок 1 – Результат работы алгоритма

Разработать приложение для выполнения операций над точками кривой:

* *kР*;
* *Р* + *Q*;
* *kР* + *lQ* – *R*;
* *Р* – *Q* + *R*.

При этом примем *P* = (37; 17), *Q* = (40; 11), *R* = (64; 27), *k* = 6, *l* = 10.

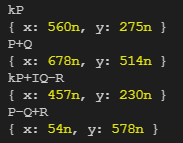


Рисунок 2 — Результат вычислений операций над точками эллиптической кривой

## Задание 2

Создать приложение для зашифрования/расшифрования собственного имени на основе ЭК.

В результате работы алгоритма получается набор точек, который в 2 раза больше, чем исходное сообщение. Вывод алгоритма представлен на рисунке 3.

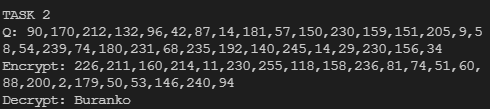


Рисунок 3 – Результат работы алгоритма

## Задание 3

Создать приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA.

В результате работы алгоритма на консоль выводится результат генерации ЭЦП и прошла ли верификация ЭЦП. Результат работы алгоритма продемонстрирован на рисунке 4.

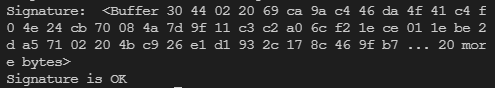


Рисунок 4 – Результат работы алгоритма верификации ЭЦП

Одним из основных параметров для пользователя является скорость шифрование и расшифрование документа. На рисунке 5 представлен график зависимости времени выполнения алгоритма от количества символов в сообщении.

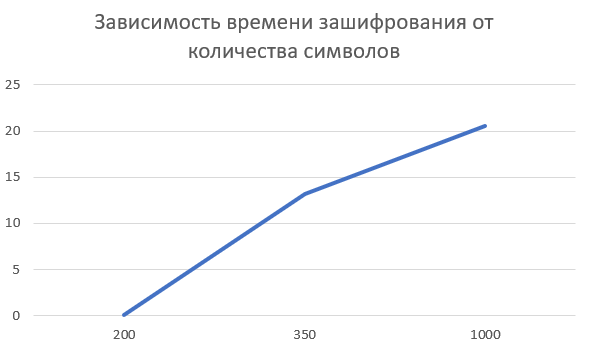


Рисунок 5 – Зависимость времени зашифрования от количества точек

# **Выводы**

В ходе выполнения данной лабораторной работы мы изучили и приобрели практические навыки реализации криптографических алгоритмов на основе эллиптических кривых.