БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №11**

**«Исследование криптографических алгоритмов**

**на основе эллиптических кривых**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

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

**Ход работы**

**Задание 1.** Найти точки ЭК для значений х, указанных в таблице, разработать приложение для операций над точками кривой.

**Вариант 3**

Выполнение задания 1 представлено на рисунке 1.

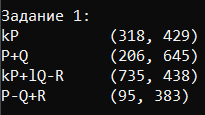


Рисунок 1 – Вывод задания 1

**Задание 2.** Создать приложение для зашифрования/расшифрования фамилии на основе ЭК задания 1, вычислить значение ключа.

Выполнение задания 2 представлено на рисунке 2.

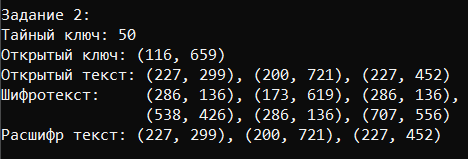


Рисунок 2 – Вывод задания 2

**Задание 3.** Создать приложение для генерации/верификации ЭЦП на основе алгоритма ECDSA, вычислить значение открытого ключа.

Выполнение задания 3 представлено на рисунке 3.

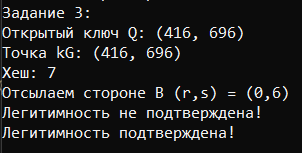


Рисунок 3 – Вывод задания 3

**Вывод:** в ходе лабораторной работы были закреплены 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. Также было разработано приложение для реализации методов криптопреобразования на основе ЭК.