Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Защита информации и надёжность информационных систем**

**Лабораторная работа №13**

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Студент: Вайсера Р.Л.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова

Минск 2023

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых (содержит 3 самостоятельных задания, каждое из которых рассчитано на 2 часа аудиторных занятий).

**Задачи**:

1. 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.

2. Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.

3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Практическое задание**

В ходе лабораторной работы было разработано приложение, которое находит точку на эллиптической кривой в заданной диапазоне и считает их количество, выполняет математические действия над точками эллиптического поля, проводит зашифрования сообщения с помощью эллиптических кривых и генерирует ЭЦП на основе ECDSA.

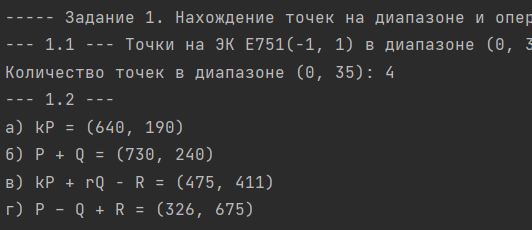
В первом задании надо было найти точки на ЭК в диапазоне (201, 235), а также провести разные математический операции над точками ЭК. Консольный вывод первого задания представлен на рисунке 1.

Рис. 1 – консольный вывод первого задания

В качестве точки *P* была взята точка (58, 139), *Q* – (67, 677) и R – (82, 481).

Во втором задании нужно было зашифровать и расшифровать сообщение с помощью эллиптических кривых. Консольный вывод второго задания представлен на рисунке 2.

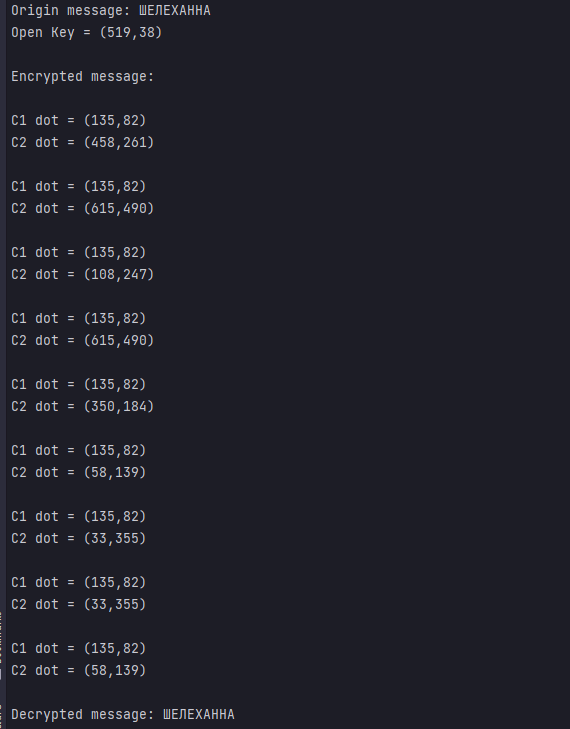


Рис. 2 – консольный вывод задания 2

В третьем задании надо было сгенерировать ЭЦП на основе ECDSA. Консольный вывод третьего задания представлен на рисунке 3.

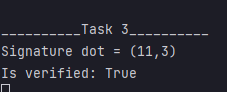


Рис. 3 – консольный вывод задания 3

Шифрация:

*С*1 = *kG*, *С*2 = *P* + *kQ*.

Получатель для расшифрования сообщения вычисляет:

*P* = *С*2 – *d*×*C*1.

Для генерации ЭЦП надо выполнить следующий алгоритм:

1. Выбрать число *k* (1 < *k* < *q*), *q* – порядок точки *G*, *d* – закрытый ключ.

2. Вычислить точку *k*×*G* = (*х*, *у*), вычислить *r* ≡ *x* mod *q*; при *r* = 0 изменить k и повторить шаг 2.

3. Вычислить *t* ≡ *k*–1 mod *q* (например, на основе расширенного алгоритма Евклида).

4. Вычислить *s* = (*t* × (H(*M*) + *d*×*r*)) mod *q*; при *s* = 0 изменить *k* и повторить алгоритм.

Отправляется М и ЭЦП(*r*, *s*).

Для верификации используется следующий алгоритм:

1. Проверить выполнение условия: 1 < *r*, *s* < *q*; если условие не выполняется, то легитимность подписи не подтверждается, в противном случае – выполняются дальнейшие шаги.

2. Вычисляются Н(*М*) и *w* ≡ *s*–1 mod *q*.

3. Вычисляются *u*1 ≡ *w* × Н(*М*) (mod *q*), u2 ≡ *w*×*r* (mod *q*).

4. Вычисляются *G*×*u*1 + *Q*×*u*2 = (*x'*, *y'*), *v* ≡ *x'* mod *q*.

5. Сравниваются *v* и *r*; если равенство выполняется, подтверждается легитимность подписи и целостность полученного сообщения.

*Q* = *d*×*G*

**Вывод**: в ходе лабораторной работы были изучены методы для работы с эллиптическими кривыми, а также была написана программа, соответствующая цели лабораторной работы.