Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов  
на основе эллиптических кривых

**Задание III**

Студент: Яскович М.Э.

ФИТ 3 курс 6 группа

Преподаватель: Сазанова Д.В.

Минск 2023

## 1. Описание приложения

Приложение написано на языке программирования Java и реализиует следующие операции:

* генерация ЭЦП на основе алгоритма ECDSA;
* верификация ЭЦП на основе алгоритма ECDSA.

## 2. Методика выполнения поставленных задач

Примем следующие значения: ЭК Е751(–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13. Тайный ключ d = 50.

Вычислим самостоятельно открытый ключ Q по формуле: Q = dG (mod 751).

Хешем подписываемого сообщения, (Н(М)), является модуль по основанию 13 координаты х точки ЭК, соответствующей первому символу собственной фамилии. Т.е., для фамилии «ЧИСТЯКОВА» хэшу сообщения будет соответствовать абсцисса по модулю 13 точки «Ч» (215, 504): x = 215, тогда 215 mod 13 = 7.

## 2.1. Генерация ЭЦП

1. Выбрать число k (1 < k < q), q – порядок точки G.

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

3. Вычислить t = k -1mod q (например, на основе расширенного алгоритма Евклида).

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

Стороне В отсылаются сообщение М и ЭЦП (числа r и s).

Программная реализация алгоритма генерации ЭЦП представлена на рисунке 2.1.

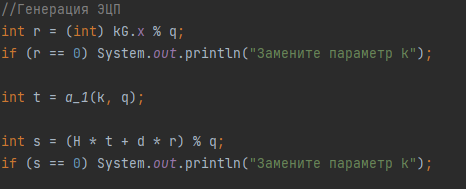


Рис 2.1 – Генерация ЭЦП

## 2.2. Верификация ЭЦП

Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над М и полученной ЭЦП (обозначения чисел оставим без изменений).

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 u1 = w Н(М) (mod q), u2 = wr (mod q).

4. Вычисляются Gu1 + Qu2 = (x', y'), v = x' mod q.

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

Программная реализация верификации ЭЦП представлена на рисунке 2.2.

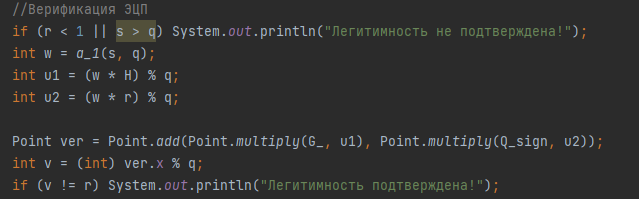


Рис. 2.2 – Верификация ЭЦП

Результат генерации и верификации ЭЦП представлен на рисунке 2.3.

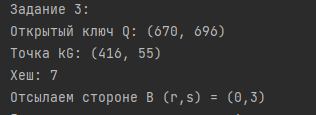


Рис. 2.3 – Результат генерации/верификации ЭЦП

Как видно из рисунка, легитимность подписи и целостность полученного сообщения подтверждены.

## Вывод

В ходе лабораторной работы было разработано приложения для реализации алгоритмов генерации и верификации ЭЦП на основе асимметричной криптографии и ЭК, оценена криптостойкость систем на основе ЭК.