Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

[Кафедра информационных](https://www.belstu.by/fakultety/fit/vm) систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №13**

по дисциплине Информационная безопасность

Тема: Исследование криптографических алгоритмов на основе эллиптических кривых

Исполнитель:

Студент 3 курса группы 6

Руководитель:

Ассистент Нистюк О. А.

Минск, 2024

**Лабораторная работа №13**

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

**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 криптонафии 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

# Теоретические сведения

Эллиптические кривые – математический объект, который может быть определен над любым полем.

Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением

у2 = х3 + aх + b,

при этом константы (а и b – вещественные числа) должны удовлетворять условию

4a3 + 27b2 ≠ 0.

Частью ЭК является бесконечно удаленная точка (также известная как идеальная точка), которую мы обозначим символом О.

Группа для ЭК есть непустое множество, элементы которого являются точками ЭК, обладающими следующими свойствами:

• единичный элемент – это бесконечно удаленная точка О;

• обратная величина точки R – это точка, симметричная относительно оси Х;

• сложение задается следующим правилом: сумма трех ненулевых точек P, Q и –R, лежащих на одной прямой, будет равна

P + Q + (–R) = О.

В соответствии с этим можем сформулировать законы сложения точек эллиптической кривой:

• прямая, проходящая через точки R и –R, является вертикальной прямой, которая не пересекает ЭК ни в какой третьей точке; если R = (х, –у), то R + (х, у) = О. Точка (х, у) является отрицательным значением точки R и обозначается –R. Таким образом, по определению R + (–R) = О;

• P + Q = R: пусть P и Q – две различные точки ЭК, и Р не равно Q; если проведем через P и Q прямую, то она пересечет ЭК еще только в одной точке, называемой –R; точка –R отображается относительно оси Х в точку R, равную сумме точек P и Q: P + Q = R.

Конечное поле – это множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю p, где p – простое число.

Поле обозначается как GF(p) или Fp. Здесь операции сложения и умножения работают как в модулярной арифметике.

Эллиптическая кривая над полем Fp задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю р (mod p):

у2 ≡ х3 + aх + b (mod p),

далее для упрощения используем знак простого неравенства:

4a3 + 27b2 ≠ 0 (mod p)

и т. д.

Если мы складываем два значения, кратных Р, то получаем значение, кратное Р (т. е. значения, кратные Р, замкнуты относительно операции сложения). Это означает, что множество кратных Р значений – это циклическая подгруппа группы, образованной эллиптической кривой.

Наименьшее значение числа q, для которого выполняется равенство qР = О, называется порядком точки Р.

Порядок группы точек эллиптической кривой равен числу различных точек ЭК, включая точку О.

Точка Р называется генератором или базовой точкой циклической подгруппы (такую точку во многих документах обозначают символом G).

# Ход работы

Было необходимо разработать приложение, выполняющее нахождение точек на эллиптической кривой. Параметры кривой: у2= х3 – х + 1 (mod 751): а = –1, b = 1, р = 751, т. е. Е751(–1, 1).

Функция getCurvePoints принимает на вход диапазон изменения координаты x. Код функции представлен на рисунке 2.1.

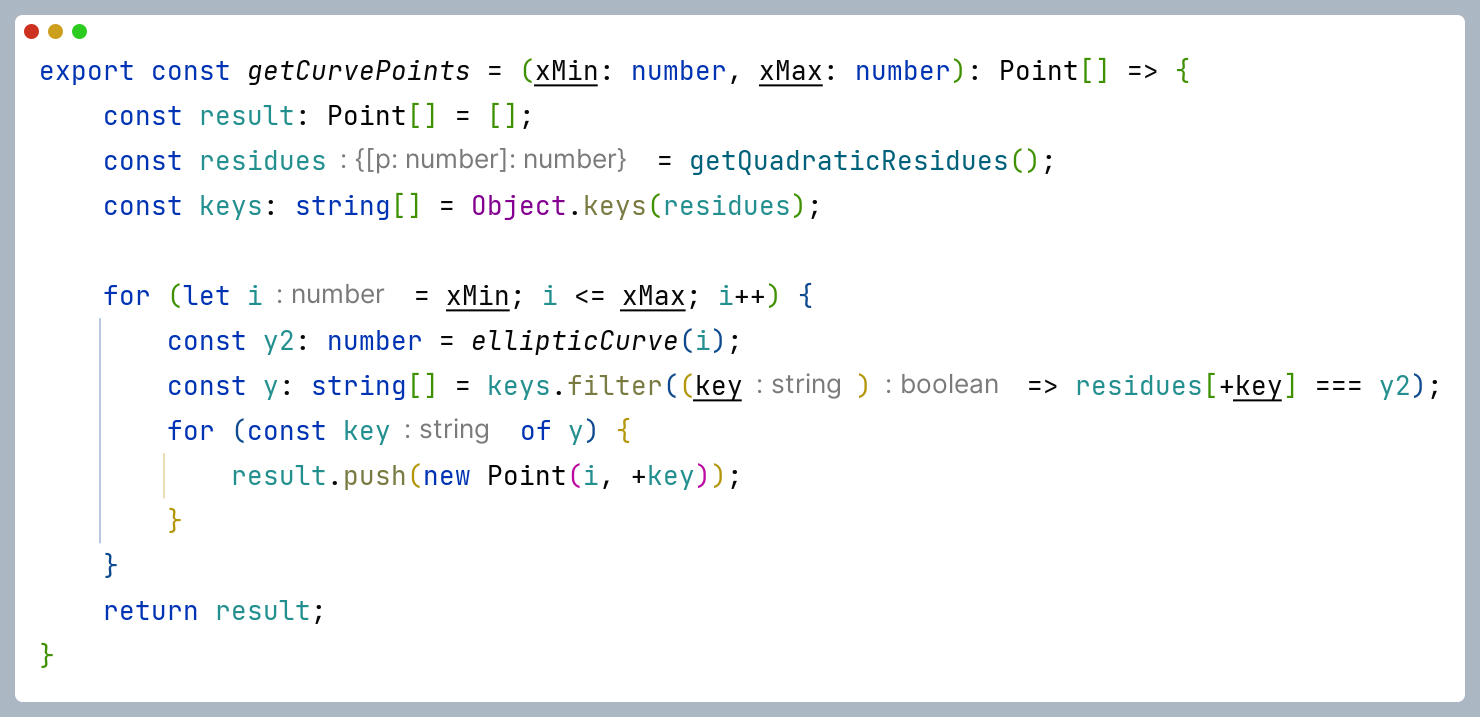


Рисунок 2.1 – Получение точек кривой в заданном диапазоне

Результат работы приложения для диапазона от 586 до 620 представлен на рисунке 2.2.

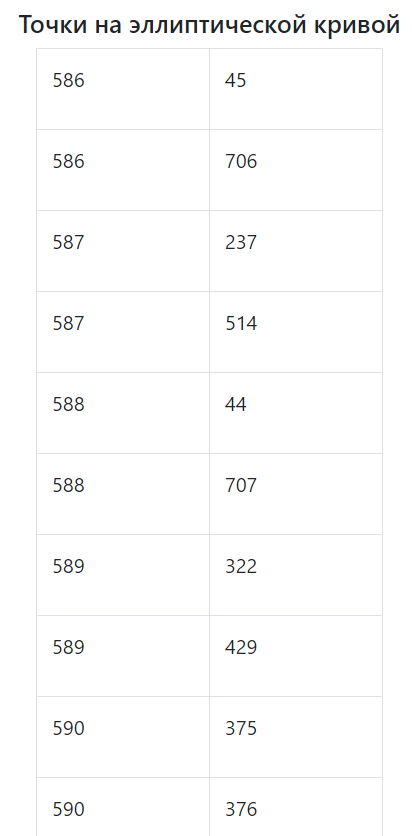


Рисунок 2.2 – Результат работы приложения

Далее было необходимо разработать приложение, выполняющее операции над точками кривой. Код функции сложения точек представлен на рисунке 2.3.

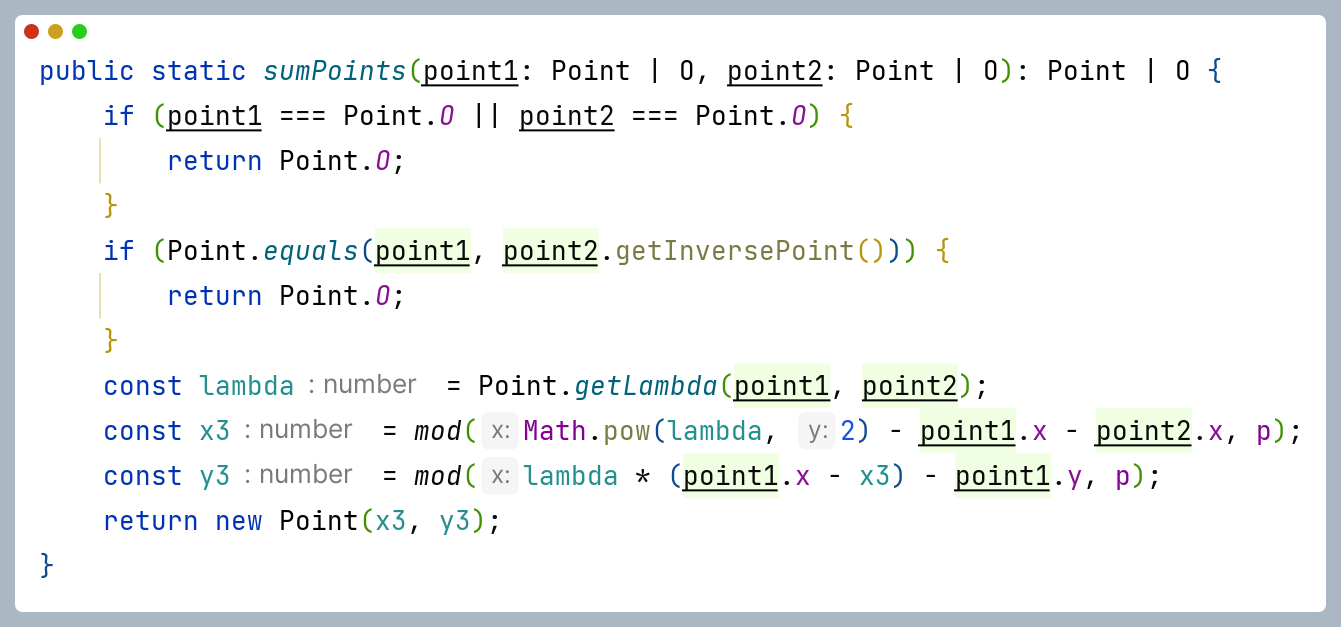


Рисунок 2.3 – Функция сложения двух точек ЭК

Код функции умножения точки на число представлен на рисунке 2.4.

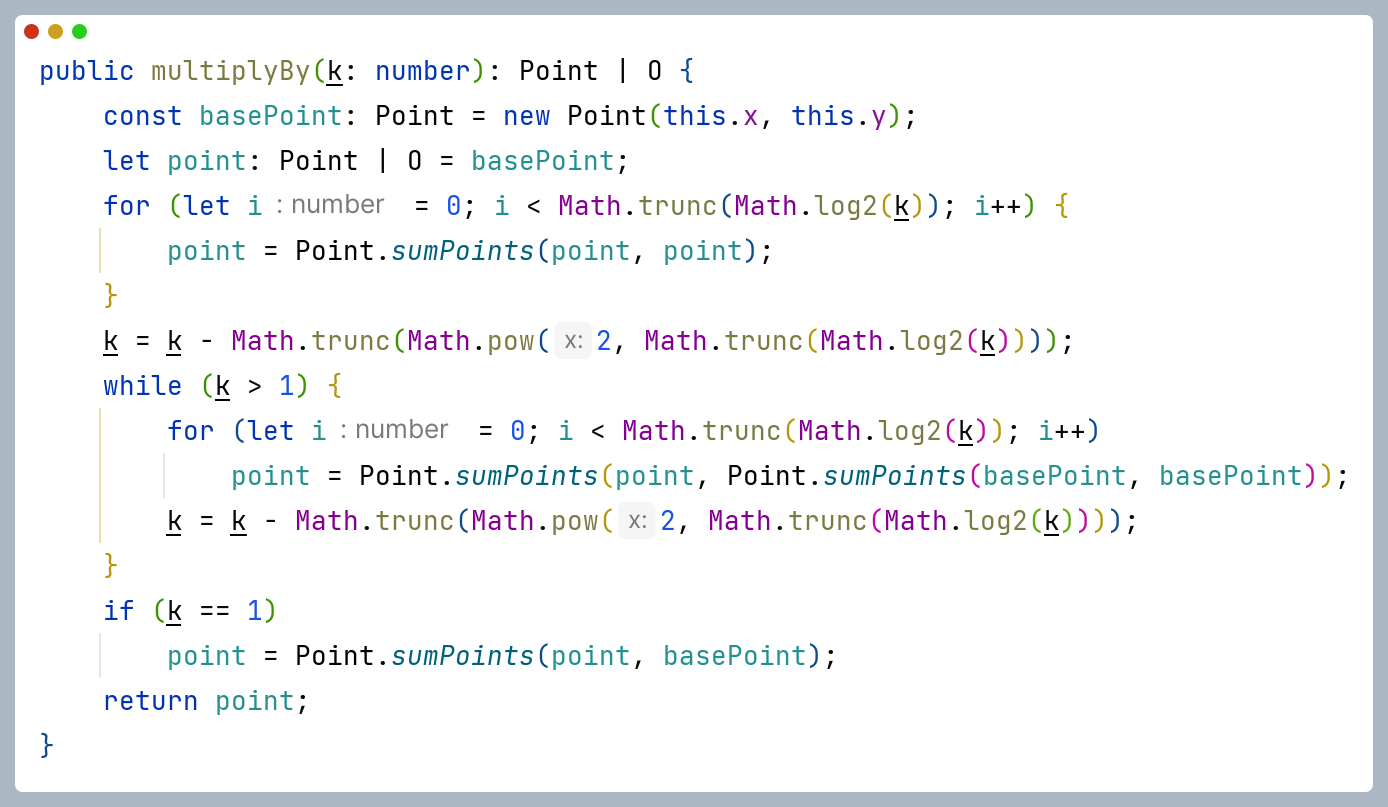


Рисунок 2.4 – Функция умножения точки на число

Результат работы приложения для P = (59, 365), Q = (59, 386), R = (105, 382), k = 7, l = 7 с представлен на рисунке 2.5.

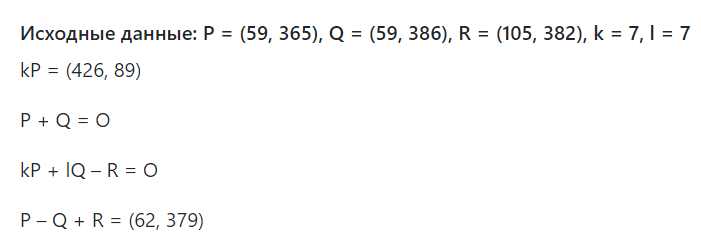


Рисунок 2.5 – Результат работы приложения

Можно заметить, что P = –Q, поэтому по правилу R + (–R) = О. Тоже самое касается сложения P и Q, множенных на одинаковые коэффициенты.

Далее было необходимо разработать приложение, выполняющее шифрование и дешифрование открытого текста.

Функция encryptText принимает на вход исходный текст, тайный ключ d (для вычисления открытого ключа) и базовую точку G. Код функции шифрования представлен на рисунке 2.6.



Рисунок 2.6 – Функция шифрования

Функция decryptText принимает на вход полученный от отправителя текст и тайный ключ. Код метода представлен на рисунке 2.7.

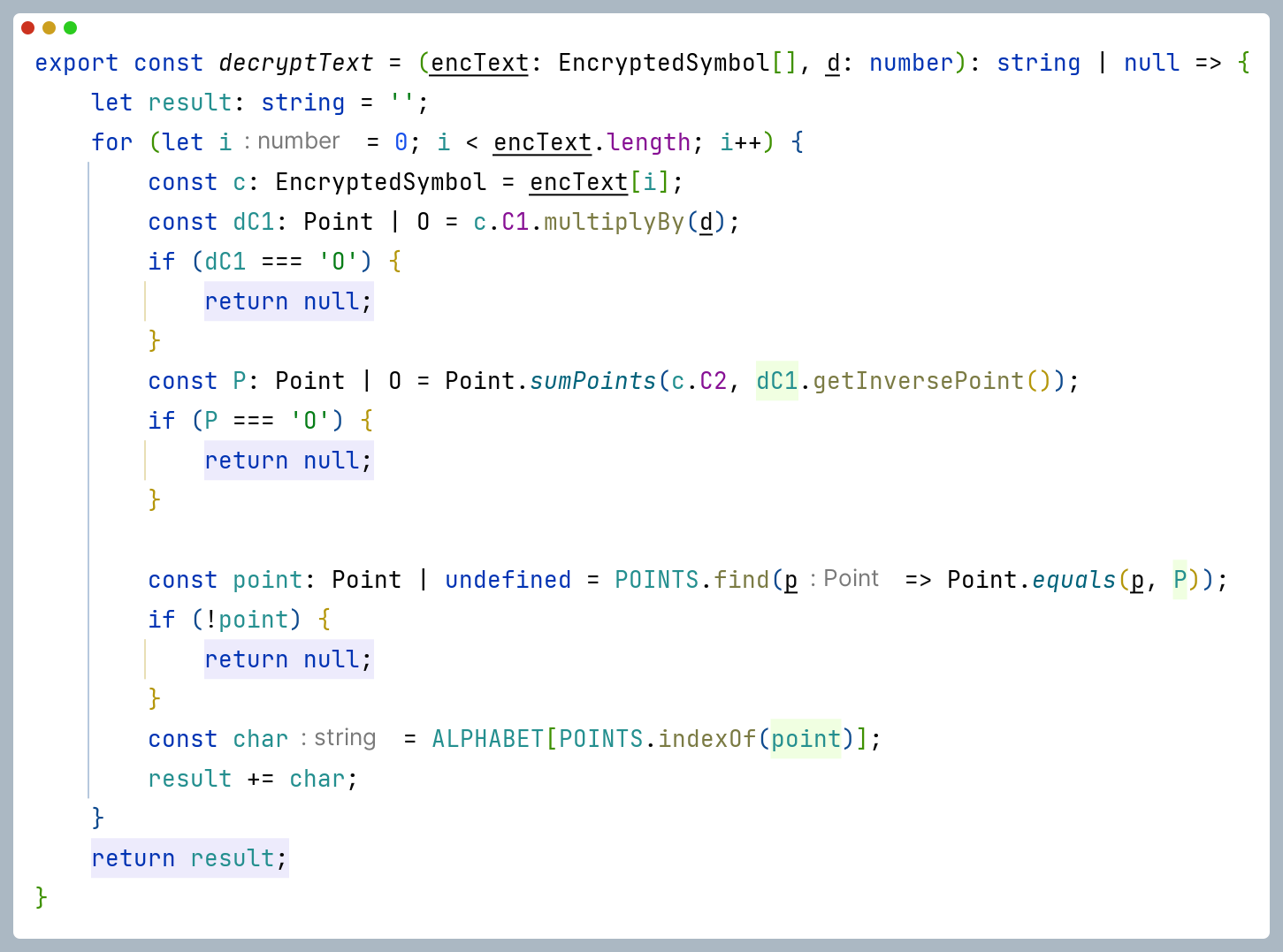


Рисунок 2.7 – Функция расшифрования

Результат работы приложения с исходным текстом «ивановиваниванович» представлен на рисунке 2.8.

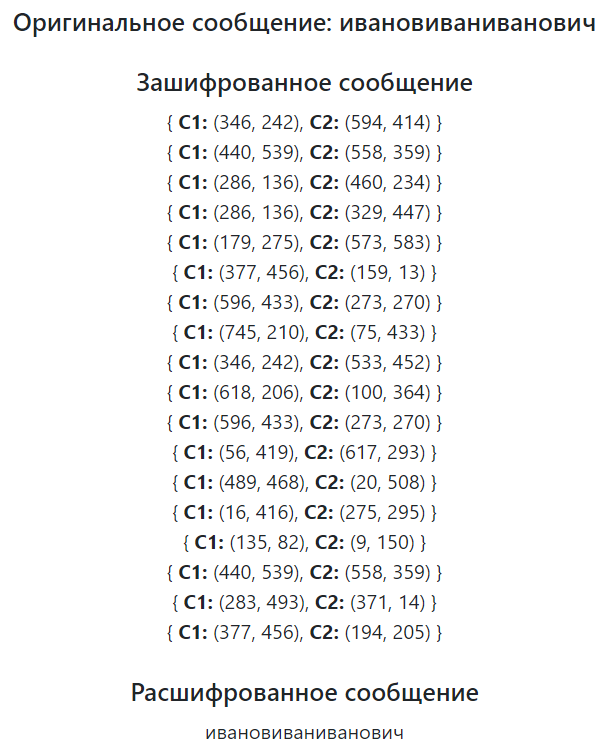


Рисунок 2.8 – Результат работы приложения

Последним заданием была разработка приложения, выполняющего генерацию и верификацию ЭЦП на основе ECDSA.

Функция generateDigitalSignature принимает на вход базовую точку G, порядок q, хеш сообщения h и тайный ключ d. Код функции представлен на рисунке 2.9.



Рисунок 2.9 – Функция генерации ЭЦП

Функция verifyDigitalSignature принимает на вход полученную ЭЦП, порядок, хеш сообщения, базовую точку G и тайный ключ (для вычисления открытого ключа). Код метода представлен на рисунке 2.10.

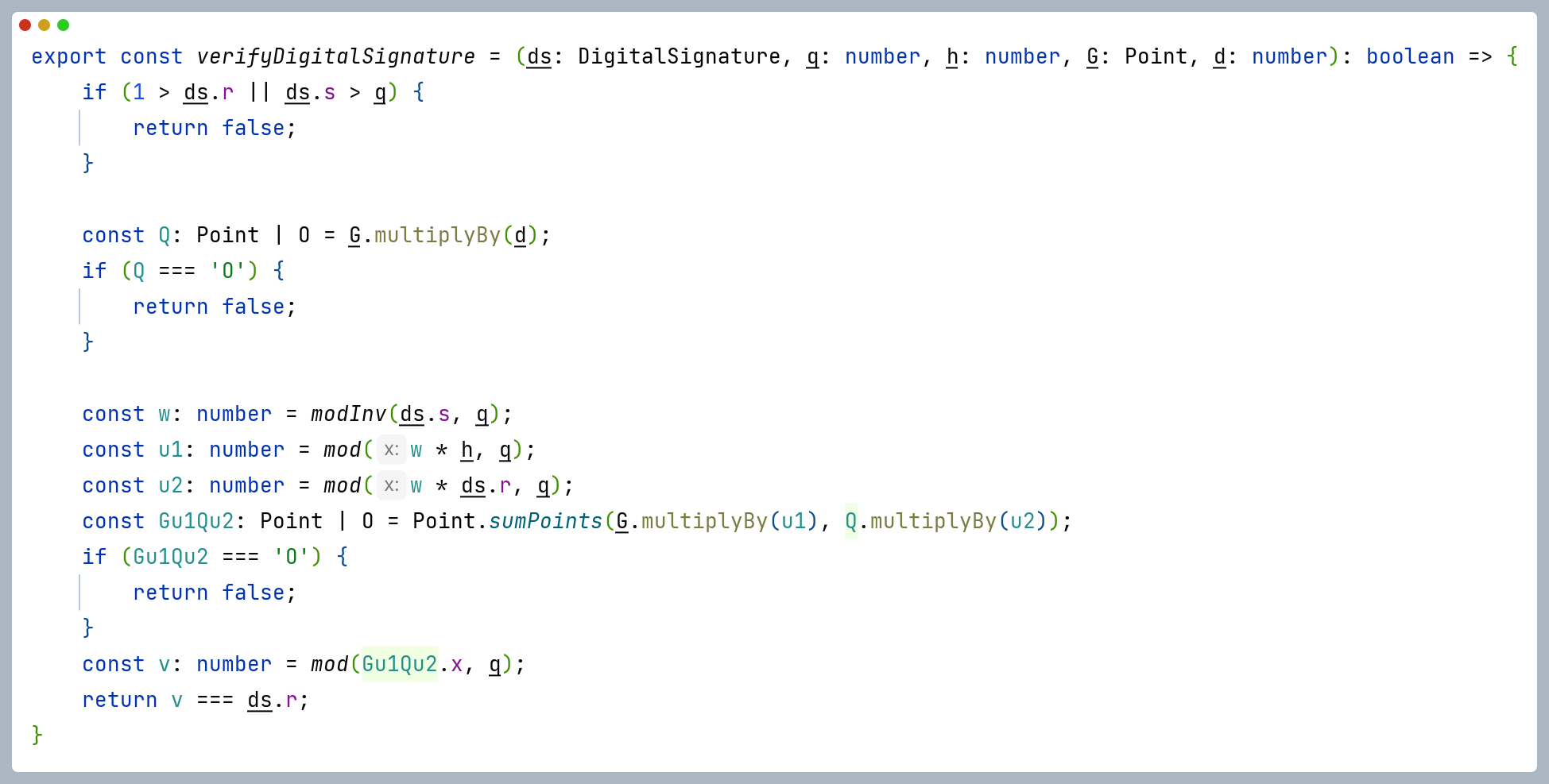


Рисунок 2.10 – Функция верификации ЭЦП

Результат работы приложения при G = (416, 55), q = 13, d = 12, H(M) = 3 представлен на рисунке 2.11.

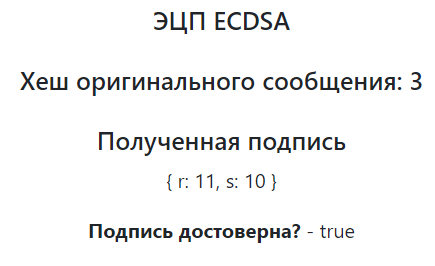


Рисунок 2.11 – Результат работы приложения

**Вывод:** в ходе выполнения лабораторной работы был изучены принципы реализации криптографических алгоритмов на основе эллиптических кривых. Было разработано приложение, выполняющее операции над точками ЭК, выполняющее шифрование и расшифрование открытого текста на основе ЭК, а также выполняющее генерацию ЭЦП на основе ECDSA.