Университет ИТМО

Факультет ПИиКТ

Информационная безопасность

Лабораторная работа №7

«Расчет точки 2P + 3Q – R на эллиптической кривой»

Вербовой Александр

Группа P3400

Вариант 4

**Цель работы**

Даны точки P, Q, R на эллиптической кривой E751 (−1,1). Найти точку 2P + 3Q – R

**Задание (вариант 4)**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ Варианта** | **Координаты точек** | | |
| **P** | **Q** | **R** |
| 4 | (56, 332) | (69,241) | (83,373) |

**Описание:**

Изображение выглядит как текст

Автоматически созданное описание

**Изображение выглядит как текст

Автоматически созданное описание**

**Изображение выглядит как текст

Автоматически созданное описание**

**Вывод**

В ходе лабораторной работы была найдена точка на эллиптической кривой 2P+3Q-R.