МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КУБГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчет**

**по практическому заданию №6**

**по курсу**

**«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**

Работу выполнила

Студентка 49 группы

Шестак В. А.

Преподаватель:

Крамаренко А. А.

Краснодар 2025

**Цель работы:** Изучение эллиптических кривых.

**Теория:**

1. Уравнение эллиптической кривой

**Теория:** Эллиптическая кривая над конечным полем GF(p) обычно задается уравнением вида: y^2=x^3+ax+b где a и b — константы из поля GF(p), а 4a^3+27b^2≠0 для обеспечения гладкости кривой.

1. Нахождение точек на кривой

**Теория:** Чтобы найти точки на эллиптической кривой, необходимо подставить все возможные значения x из поля GF(p) в уравнение кривой и вычислить соответствующие значения y, проверив, является ли y2 квадратом в поле GF(p).

1. Генерация ключей

**Теория:** Для генерации ключей в криптографии на основе эллиптических кривых используется следующий процесс:

* **Секретный ключ:** Выбирается случайное целое число d в диапазоне от 1 до n−1, где n — порядок генерирующей точки G.
* **Открытый ключ:** Вычисляется как Q=dG, где G — базовая точка на кривой.

1. Шифрование и расшифрование

**Теория:** Шифрование и расшифрование в криптографии на основе эллиптических кривых, например, в протоколе Эль-Гамаля, включает в себя следующие шаги:

* **Шифрование:** Алиса выбирает точку P на кривой как исходный текст и случайное число k. Затем она вычисляет зашифрованный текст как пару точек (kG, P+kQ), где Q - открытый ключ Боба.
* **Расшифрование:** Боб использует свой секретный ключ d для расшифрования, вычисляя P =(kQ+d(kG))−kG, что упрощается до P.

**Ход работы:**

1. ﻿﻿﻿﻿В эллиптической кривой Е (1, 2) в поле GF (11):

а. Найдите уравнение кривой.

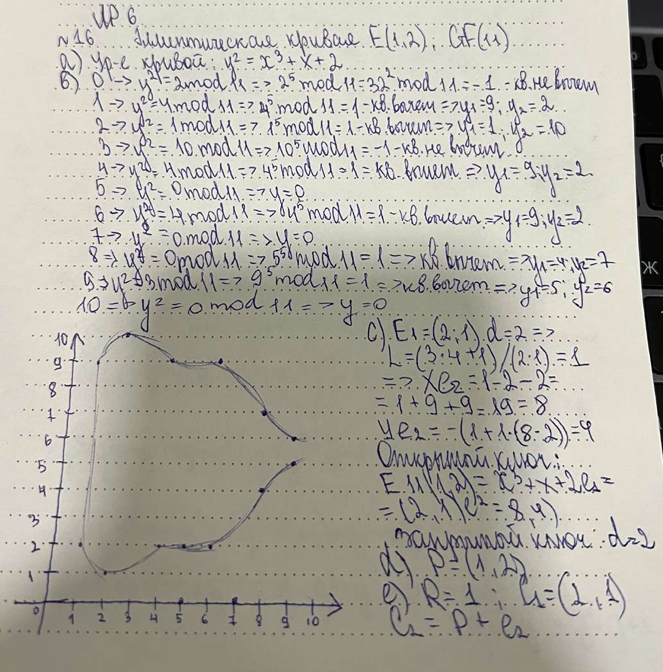
б. Найдите все точки на кривой и сделайте рисунок, такой же, как рис. 10.14.

в. Сгенерируйте общедоступный и секретный ключи для Боба.

г. Выберите точку на кривой как исходный текст Алисы.

д. Создайте зашифрованный текст, соответствующий исходному тексту Алисы в пункте d.

е. Расшифруйте зашифрованный текст для Боба, чтобы найти исходный текст, передаваемый Алисой.



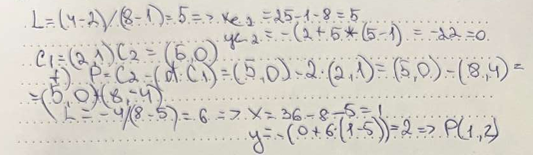
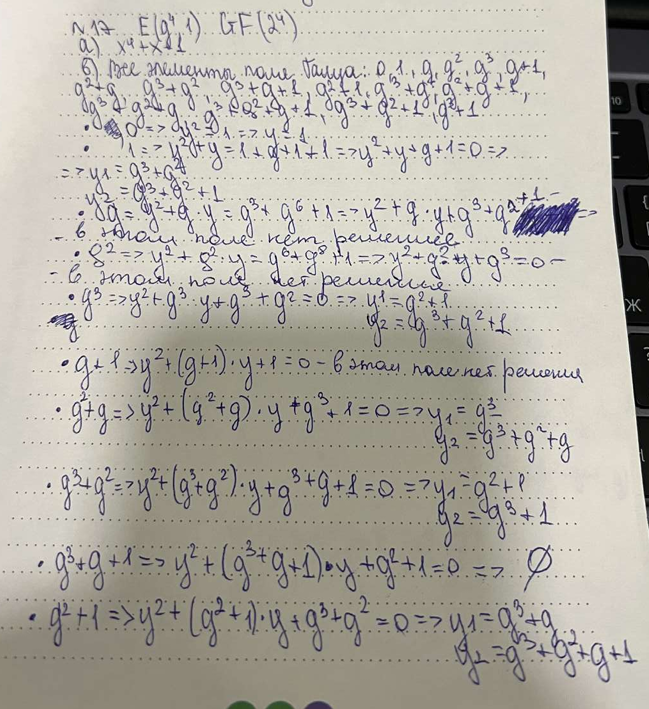


Рисунок 1 – Решение задания 16

1. В эллиптической кривой E (g^4, 1) в поле GF(2^4):

а. Найдите уравнение кривой.

б. Найдите все точки на кривой и сделайте рисунок, такой же, как рис. 10.14.

в. Сгенерируйте общедоступный и секретный ключи для Боба.

г. Выберите точку на кривой как исходный текст Алисы.

д. Создайте зашифрованный текст, соответствующий исходному тексту Алисы в пункте г. е. Расшифруйте зашифрованный текст для Боба, чтобы найти исходный текст, передаемый Алисе.

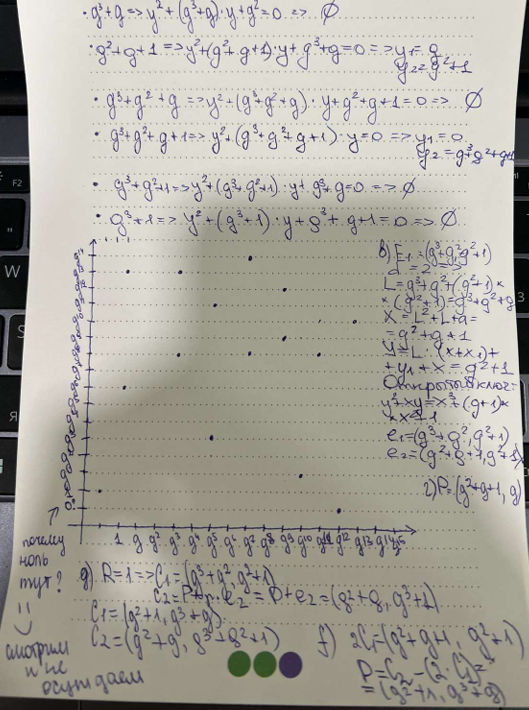


Рисунок 2 – Решение задания 17