Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчёт**

**по лабораторной работе №6**

**Дисциплина: КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ**

**Тема: «Эллиптические кривые»**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ К. А. Корнилов

Направление подготовки 02.03.02 Фундаментальная информатика и

информационные технологии

Направленность (профиль) Математическое и программное обеспечение

компьютерных технологий

Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. А. Крамаренко

**Тема:** Эллиптические кривые.

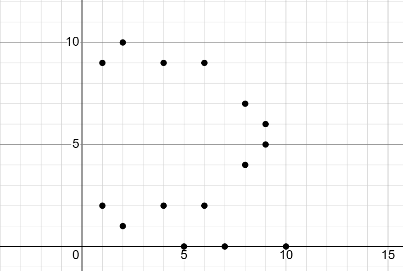
**Цель:** Изучение эллиптических кривых и их применения.

**Ход работы:**

1. В эллиптической кривой E(1,2) в поле GF(11):
2. Найти уравнение кривой:

Уравнение кривой: y^2 = x^3+x+2

1. Найти все точки на кривой и сделать рисунок:
2. 0 => y^2 = 2 mod 11 => 2^5 mod 11 = 32^2 mod 11 = -1 =>QNR
3. 1 => y^2 = 4 mod 11 => 4^5 mod 11 = 1 =>QR => y1 = 9 y2 = 2
4. 2 => y^2 = 1 mod 11 => 1^5 mod 11 = 1 =>QR => y1 = 1 y2 = 10
5. 3 => y^2 = 10 mod 11 => (-1)^5 mod 11 = -1 =>QNR
6. 4 => y^2 = 4 mod 11 => 4^5 mod 11 = 1 =>QR => y1 = 9 y2 = 2
7. 5 => y^2 = 0 mod 11 => y = 0
8. 6 => y^2 = 4 mod 11 => 4^5 mod 11 = 1 =>QR => y1 = 9 y2 = 2
9. 7 => y^2 = 0 mod 11 => y = 0
10. 8 => y^2 = 5 mod 11 => 5^5 mod 11 = 1 =>QR => y1 = 4 y2 = 7
11. 9 => y^2 = 3 mod 11 => ^5 mod 11 = 1 =>QR => y1 = 5 y2 = 6
12. 10 => y^2 =0 mod 11 => y = 0
13. График



1. Сгенерировать общедоступный и секретный ключ для Боба

Е1 = (2,1) d = 2 =>

L = (3\*4+1)/(2\*1) = 1 => xe2 = 1 – 2 – 2 = 1 + 9 + 9 = 19 = 8

Ye2 = -(1+1\*(8-2)) = 4

Открытый ключ: E11(1,2) = x^3+x+2 e1 = (2,1) e2 = (8,4)

Закрытый: d = 2

1. Выбрать точку на кривой как исходный текст Алисы: P = (1,2)
2. Создать зашифрованный текст, соответствующий исходному тексту Алисы в пункте d.

R = 1 => C1 = (2,1)

C2 = P +e2

L = (4-2)/(8-1) = 5 => xc2 = 25 – 1 -8 = 5 yc2 = -(2+5\*(5-1)) = -22 = 0

C1 = (2,1) C2 = (5,0)

1. Расшифровать зашифрованный текст для Боба, чтобы найти исходный текст, передаваемый Алисой.

P = C2 – (d\* C1) = (5,0) – 2 \* (2,1) = (5,0) – (8,4) = (5,0) + (8,-4)

L = -4/(8-5) = 6 => x = 36 -8 – 5 = 1 y = -(0+6\*(1-5)) = 2 => P=(1,2)

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

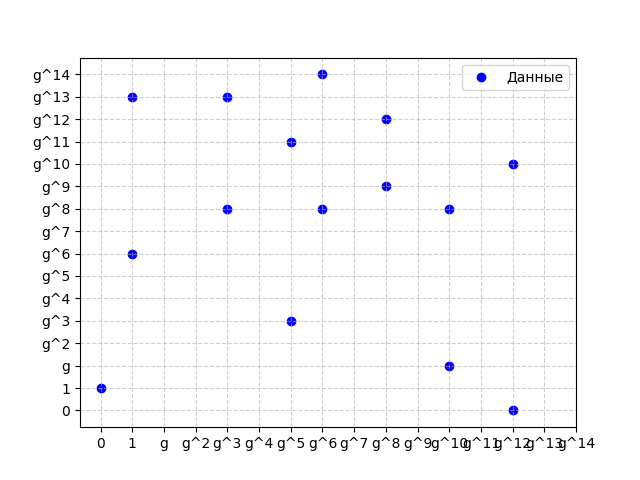
Пусть будет примитивный полином: x^4+x+1

Уравнение кривой: y^2 +xy = x^3+(g+1)x+1

1. Найти все точки на кривой и сделать рисунок:

Все элементы поля Галуа: 0, 1, g, g^2, g^3, g+1, g^2+g, g^3+g^2, g^3+g+1, g^2+1, g^3+g, g^2+g+1, g^3+g^2+g, g^3+g^2+g+1, g^3+g^2+1, g^3+1

1. 0 => y^2 = 1 => y = 1
2. 1 => y^2 +y = 1 + g + 1 + 1 => y^2+y+g+1 = 0 => y1 = g^3+g^2 y2 = g^3+g^2+1
3. g => y^2 +g \* y = g^3 + g^6 + 1 => y^2+g \* y+g^3 + g^2 + 1 = 0 => нет решения в данном поле
4. g^2 => y^2 +g^2 \* y = g^6 + g^8 + 1 => y^2+g^2 \* y+g^3 = 0 => нет решения в данном поле
5. g^3 => y^2 + g^3\*y + g^3 + g^2 = 0 => y1 = g^2+1 y2 = g^3+g^2+1
6. g+1 => y^2 +(g+1) \* y +1 = 0 => нет решения в данном поле
7. g^2+g => y^2 +(g^2+g) \* y +g^3 + 1 = 0 => y1 = g^3 y2 = g^3+g^2+g
8. g^3 + g^2 => y^2 +(g^3 + g^2) \* y + g^3 + g + 1 = 0 => y1 = g^2+1 y2 = g^3 + 1
9. g^3 + g + 1 => y^2 +(g^3 + g + 1) \* y + g^2 + 1 = 0 => нет решения в данном поле
10. g^2 + 1 => y^2 +(g^2+1) \* y + g^3 + g^2 = 0 => y1 = g^3+g y2 = g^3+g^2+g+1
11. g^3 + g => y^2 +(g^3+g)\*y + g^2 = 0 => нет решения в данном поле
12. g^2 + g + 1 => y^2 + (g^2+g+1) \* y +g^3 + g = 0 => y1 = g y2 = g^2+ 1
13. g^3+ g^2 + g => y^2 +(g^3 + g^2 + g) \* y + g^2 + g + 1 = 0 => нет решения в данном поле
14. g^3 + g^2 + g +1 => y^2 + (g^3 + g^2 +g + 1) \* y = 0 => y1 = 0 y2 = g^3 + g^2 + g + 1
15. g^3 + g^2 + 1 => y^2 + (g^3 + g^2 + 1) \* y +g^3 + g = 0 => нет решения в данном поле
16. g^3 + 1 => y^2 + (g^3 + 1) \* y + g^3 + g + 1 = 0 => нет решения в данном поле
17. График



1. Сгенерировать общедоступный и секретный ключ для Боба

Е1 = (g^3+g^2,g^2+1) d = 2 =>

L = g^3+g^2 + (g^2+1) \* (g^2+1) = g^3 + g^2 + g

X = L^2 + L + a = g^2 + g + 1

Y = L \* (x + x1) + y1 + x = g^2 + 1

Открытый ключ: y^2+xy = x^3 + (g+1) \* x^2 + 1 e1 = (g^3+g^2, g^2+1) e2 = (g^2 + g + 1, g^2 + 1)

Закрытый: d = 2

1. Выбрать точку на кривой как исходный текст Алисы: P = (g^2+g+1, g)
2. Создать зашифрованный текст, соответствующий исходному тексту Алисы в пункте d.

R = 1 => C1 = (g^3 + g^2, g^2 + 1)

C2 = P +r \* e2 = P +e2 = (g^2 + g, g^3 + 1)

C1 = (g^2 + 1, g^3 + g) C2 = (g^2 + g, g^3 + g^2 + 1)

1. Расшифровать зашифрованный текст для Боба, чтобы найти исходный текст, передаваемый Алисой.

2C1 = (g^2+g+1, g^2+1)

P = C2 – (2\* C1) = (g^2+1, g^3+g)