**Практическое занятие**

**Исследование криптосистем с открытым ключом на основе эллиптических кривых**

**Цель работы:** Приобретение навыков анализа алгоритмов криптосистем с открытыми ключами на основе эллиптических кривых.

Для закрепления знаний, полученных на лекции выполнить задание 1 и задание 2.

**Теоретические сведения**

*Сложение точек ЭК*

Пусть *P= (x1,y1) и Q=(x2,y2*),  две точки ЭК, тогда точка *R(x3,y3)=P+Q* может быть найдена как



Если , то точка R(x3,y3) может быть найдена, как



Если , то точка R(x3,y3)= 0 (точка в бесконечности).

Все вычисления следует проводить по *modp.*

*Умножение на константу.*

Для умножения точки на константу*kP* необходимо точку сложить саму с собой *k* раз. Для сложения может быть использован быстрый алгоритм, аналогичный быстрому возведению числа в степень.

Для этого необходимо:

- записать число k в двоичном виде;

- найти последовательность точек: P, 2P,4P, 8P…..

- из этой последовательности выбрать и сложить те точки, которым соответствуют единицы в двоичном представлении числа k.

Можно также использовать способ повторного удвоения. Например, чтобы найти 171Р представим 171 как 1+2\*85=1+2(1+2\*2\*21)=1+2(1+2\*2(1+2\*2(1+2\*2))).

Тогда 171Р=Р+2(Р+2\*2(Р+2\*2(Р+2\*2Р)))

То есть для вычисления нужно сделать 7 удвоенийР и 4 сложения с Р.

**Задание 1.**

Задана эллиптическая кривая Е13(1,1) в поле GF(13) по уравнению .

Точки Е13(1,1) (без нулевой точки) представлены на рис.1.

Рис1. Точки и граф эллиптической кривой

1. Проанализировать расположение точек на графе, проверить, что указанные точки действительно принадлежат, заданной кривой (2-3 точки).

Найтив взаимнообратные точки. Обратите внимание на то, что некоторые точки (x,y) не лежат на кривой.

2. Выполнить вручную следующие вычисления:

- найти точку С равную сумме двух точек , координаты точек и  соответствуют вашему варианту задания.

-найти противоположную точку .

-вычислить точку , где *k* число согласно варианту задания.

Таблица 1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| Nвар | A | B | k | C | -C | kC |  |
| 1 | 0,1 | 5,12 | 4 |  |  |  |  |
| 2 | 1,4 | 7,0 | 5 |  |  |  |  |
| 3 | 4,2 | 8,12 | 4 |  |  |  |  |
| 4 | 5,1 | 10,7 | 5 | (1,9) |  |  |  |
| 5 | 7,0 | 11,11 | 4 |  |  |  |  |
| 6 | 8,1 | 0,12 | 5 |  |  |  |  |
| 7 | 10.6 | 1,9 | 4 |  |  |  |  |
| 8 | 11,2 | 4,11 | 5 |  |  |  |  |
| 9 | 5,12 | 1,4 | 4 |  |  |  |  |
| 10 | 7,0 | 4,2 | 5 |  |  |  |  |
| 11 | 8,12 | 5,1 | 4 |  |  |  |  |
| 12 | 10,7 | 7,0 | 5 |  |  |  |  |
| 13 | 11,11 | 8,1 | 4 |  |  |  |  |
| 14 | 0,12 | 10.6 | 5 |  |  |  |  |
| 15 | 1,9 | 11,2 | 4 |  |  |  |  |
| 16 | 4,11 | 5,12 | 5 |  |  |  |  |
| 17 | 0,12 | 5,1 | 4 |  |  |  |  |
| 18 | 1,9 | 7,0 | 5 |  |  |  |  |
| 19 | 4,11 | 8,1 | 4 |  |  |  |  |
| 20 | 1,4 | 10.6 | 5 |  |  |  |  |
| 21 | 4,2 | 11,2 | 4 |  |  |  |  |
| 22 | 5,1 | 5,12 | 5 |  |  |  |  |
| 23 | 7,0 | 7,0 | 4 |  |  |  |  |
| 24 | 8,1 | 8,12 | 5 |  |  |  |  |
| 25 | 10.6 | 10,7 | 4 |  |  |  |  |
| 26 | 11,2 | 11,11 | 5 |  |  |  |  |
| 27 | 5,12 | 0,12 | 4 |  |  |  |  |
| 28 | 10.6 | 1,9 | 5 |  |  |  |  |
| 29 | 11,2 | 4,11 | 4 |  |  |  |  |
| 30 | 5,12 | 0,12 | 5 |  |  |  |  |

**Задание2**.

1.Моделирование криптосистемы Эль-Гамаля на эллиптической кривой.

-задана кривая Е67(2,N),*),* где параметр N соответствует номеру варианта. Записать ее уравнение.

**Генерирование ключей** (корреспондент А):

-выбрать произвольную точку  с координатами *(x,y*).

Проверить принадлежит ли точка кривой (проверку записать в отчет).

- выбрать целое число *d*, согласно варианту задания.

-вычислить точку, используя алгоритм быстрого вычисления.

- параметры: ЭК Е67(2,N), и точек , передать корреспонденту В, в качестве открытого ключа, параметр d-закрытый ключ (не передается).

**Шифрование сообщения** (корреспондент В):

-выбрать сообщение в виде произвольной точки ЭК P(x,y);

-выбрать случайное число r;

-вычислить криптограмму в виде пары точек:



-передать С1 и С2 корреспонденту А.

**Расшифрование криптограммы** (корреспондент А)

-получить криптограмму: С1 и С2

-найти переданное сообщение по формуле

,

где знак минус означает сложение с противоположным элементом к точке .

Заполнить строку таблицы 2, своего варианта+ открытое сообщение..

Таблица 2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nвар | d | r | E1 | E2 | C1 | C2 |
| 1 | 2 | 5 |  |  |  |  |
| 2 | 3 | 4 |  |  |  |  |
| 3 | 4 | 3 |  |  |  |  |
| 4 | 5 | 1 |  |  |  |  |
| 5 | 4 | r |  |  |  |  |
| 6 | 2 | 5 |  |  |  |  |
| 7 | 3 | 4 |  |  |  |  |
| 8 | 4 | 3 |  |  |  |  |
| 9 | 5 | 1 |  |  |  |  |
| 10 | 2 | 5 |  |  |  |  |
| 11 | 3 | 4 |  |  |  |  |
| 12 | 4 | 3 |  |  |  |  |
| 13 | 5 | 1 |  |  |  |  |
| 14 | 3 | 7 |  |  |  |  |
| 15 | 2 | 5 |  |  |  |  |
| 16 | 2 | 5 |  |  |  |  |
| 17 | 3 | 4 |  |  |  |  |
| 18 | 4 | 3 |  |  |  |  |
| 19 | 5 | 1 |  |  |  |  |
| 20 | d | 7 |  |  |  |  |
| 21 | 2 | 5 |  |  |  |  |
| 22 | 3 | 4 |  |  |  |  |
| 23 | 4 | 3 |  |  |  |  |
| 24 | 5 | 1 |  |  |  |  |
| 25 | 2 | 5 |  |  |  |  |
| 26 | 3 | 4 |  |  |  |  |
| 27 | 4 | 3 |  |  |  |  |
| 28 | 5 | 1 |  |  |  |  |
| 29 | 3 | 4 |  |  |  |  |
| 30 | 2 | 5 |  |  |  |  |

При выполнении задания 2 использовать программу в папке «Вычисление точек ЭК»

Отчет по работе должен включать расчеты по всем пунктам задания.