**Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации**

**ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникации им. проф. М.А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Факультет: ИКСС

Отчет по лабораторной работе №1

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

Выполнил: Громов А.А.

Группа: ИКТЗ-83

Проверил: Яковлев В.А.

Санкт-Петербург

2021 г.

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

**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).

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

2. Выполнить вручную следующие вычисления:

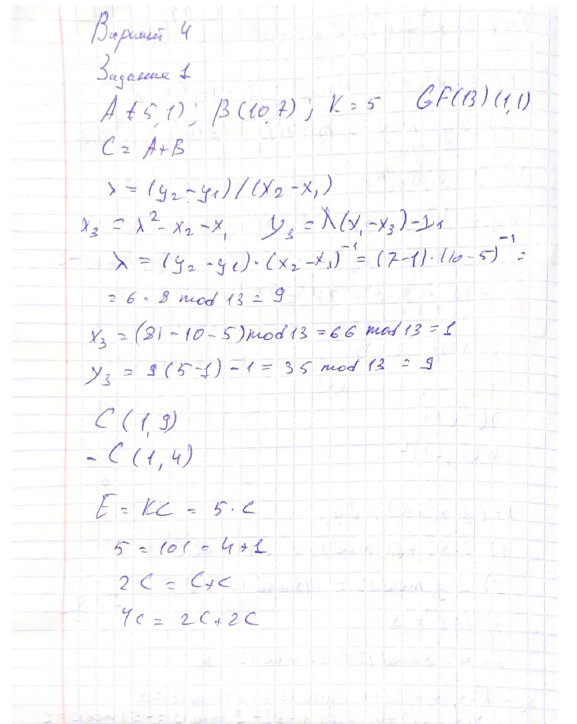
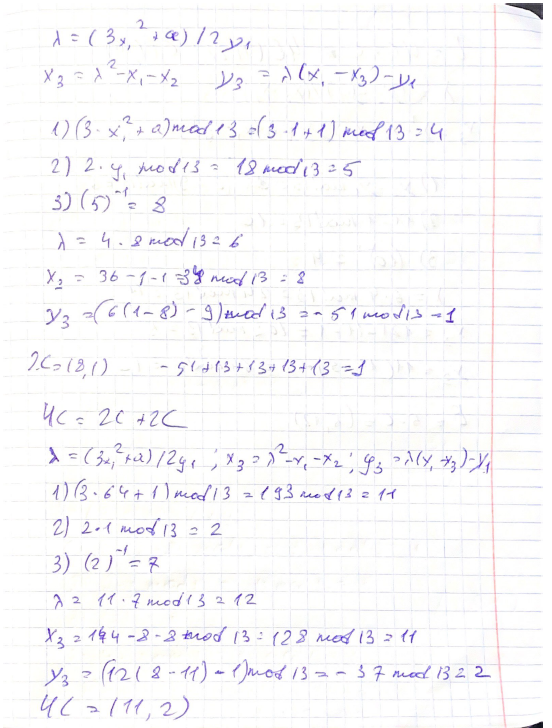
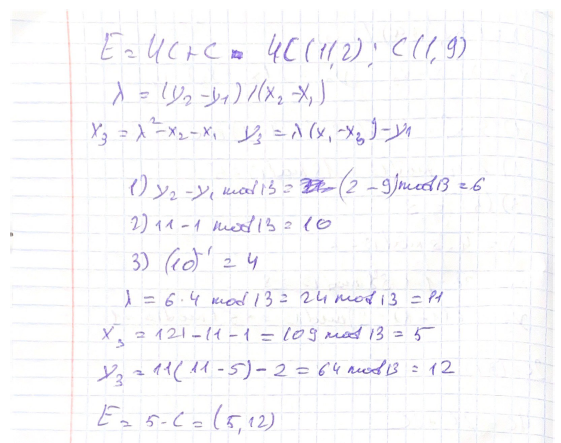
- найти точку С равную сумме двух точек , координаты точек и  соответствуют вашему варианту задания.

-найти противоположную точку .

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

Таблица 1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nвар | A | B | k | C | -C | kC |
| 4 | 5,1 | 10,7 | 5 | (1,9) | (1,4) | (5,12) |

**** **** 

**Задание2**.

1.Моделирование криптосистемы Эль-Гамаля на эллиптической кривой.

a = 2, b =4

- задана кривая Е67(2,4),ее уравнение:

y2 = x3 + 2x + 4

**Генерирование ключей** (корреспондент А):

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

E1 = (13,4)

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

y2 = x3 + 2x + 4

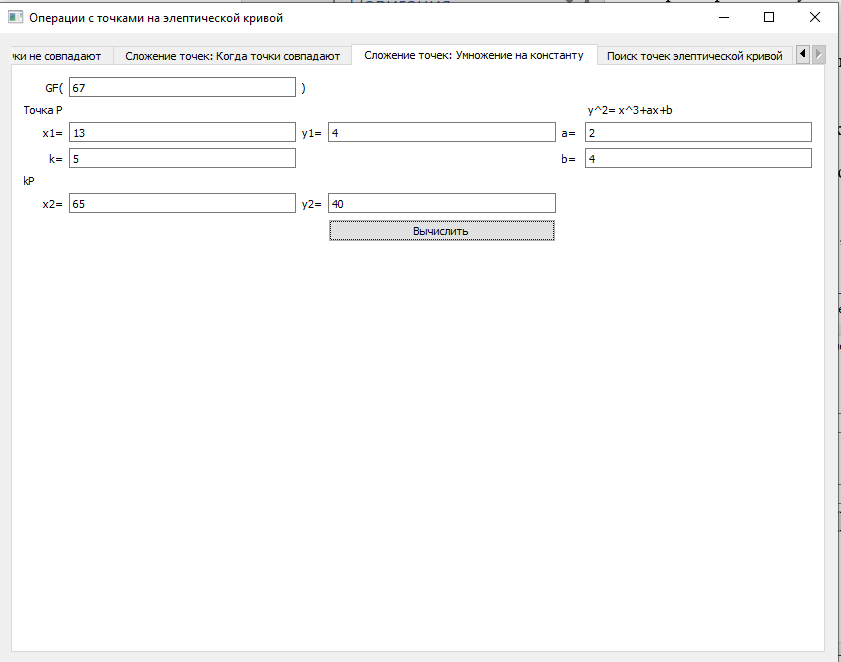
16 = 2197 + 26 + 4

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

d = 5

-вычислить точку, используя алгоритм быстрого вычисления.

E2 = d \* E1 = 5 \* E1(13,4)



E2 = (65,40)

- параметры: ЭК Е67(2,4), 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);

P (20,2)

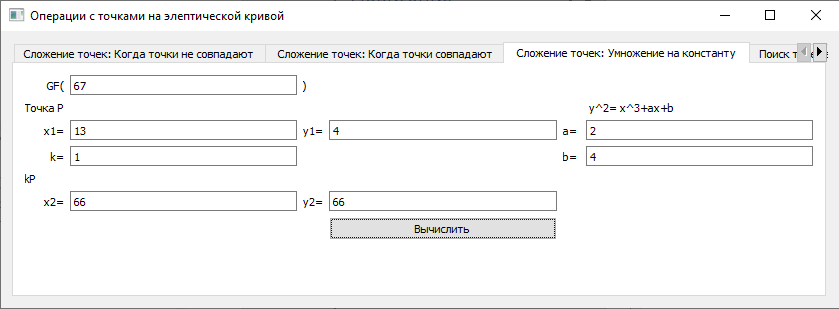
-выбрать случайное число r;

r = 1

-вычислить криптограмму в виде пары точек:

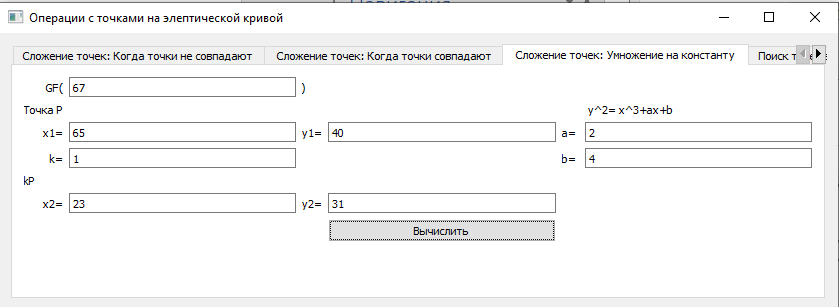


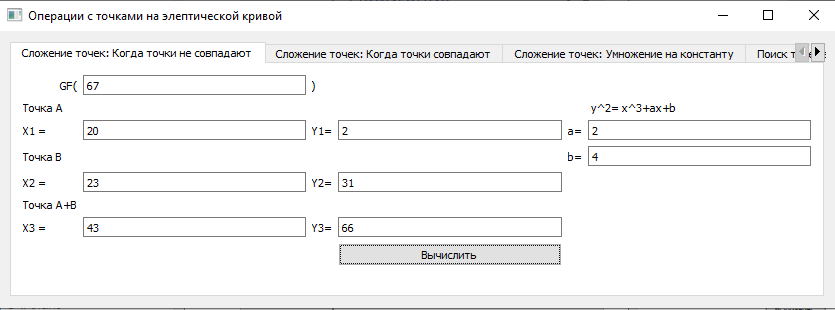
C1 = 1\*(13,4)



C1 (66,66)

C2 = P (20,2) + 1\*E2 (65,40)





C2 (43,66)

-передать С1 и С2 корреспонденту А.

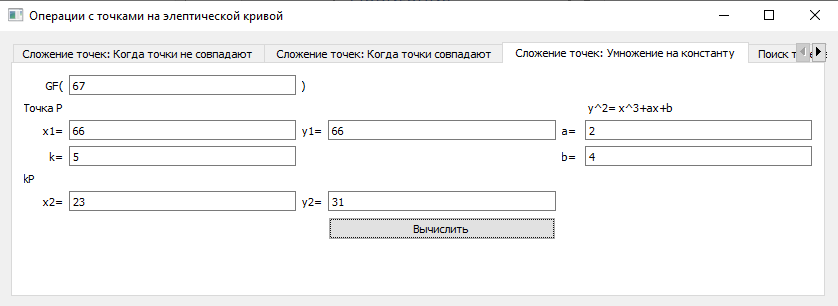
**Расшифрование криптограммы** (корреспондент А)

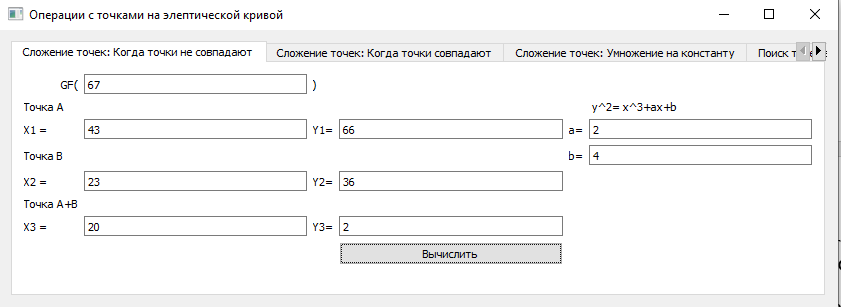
-получить криптограмму: С1 и С2

-найти переданное сообщение по формуле

,

P = C2 (43,66) – (5\*C1 (66,66))





P (20,2)

где знак минус означает сложение с противоположным элементом к точке .

Таблица 2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nвар | d | r | E1 | E2 | C1 | C2 |
| 4 | 5 | 1 | 13,4 | 65,40 | 66,66 | 43,66 |

**Вывод:**

В ходе лабораторной работы мы приобрели навыки анализа алгоритмов криптосистем с открытыми ключами на основе эллиптических кривых