Київський національний університет імені Тараса Шевченка

Факультет комп’ютерних наук та кібернетики

Кафедра інтелектуальних програмних систем

Математичні основи захисту інформації

Лабораторна робота №7

“Використання еліптичних кривих у криптографії. Пошук кількості точок на еліптичній кривій над скінченним полем”

Виконали студенти 3-го курсу

Групи ІПС-32

Роботу виконали:

Ольховатий Ігор

Ковальов Володимир

Тряско Софія

Цілинко Олександр

Бондар Юлія

Волик Артем

Київ 2023

Завдання:

Знайти кількість точок на еліптичній кривій:

$y^2 = x^3 + 2x + 6 (a = 2, b = 6)$ над Z_{11}

Розв'язання

Застосуємо наївний алгоритм.

Будемо додавати значення X від 0 до 10 і обчислювати при них значення У:

X=0	Y^2=6	У не існує
X=1	Y^2=1+2+6=9	Y=3;8
X=2	Y^2=8+4+6=7	У не існує
X=3	Y^2=9+6+6=6	У не існує
X=4	Y^2=1	Y=1;10
X=5	Y^2=9	У=3;8
X=6	Y^2=3	Y=5;6
X=7	Y^2=0	Y=0
X=8	Y^2=6	У не існує
X=9	Y^2=5	Y=4;7
X=10	Y^2=3	Y=5;6

Кількість знайдених розв'язків = 12. Додаємо нескінченно віддалену точку і отримаємо,що

$$|E_{11}(2, 6)| = 13$$

Література:

- Лекції з предмету "Математичні основи захисту інформації"
- https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D1%96%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D0%B0_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F
- https://ela.kpi.ua/bitstream/123456789/12387/1/06_p64.pdf