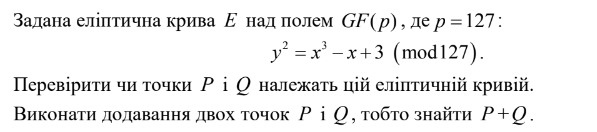
**Студент – Дворський Віталій**

**Варіант – 3**

**Завдання 1**

****

****

****

Для початку перевіримо, чи точки P i Q належать еліптичній кривій.

1. Для точки P = (56, 7):

72 = 563 – 56 + 3 (mod 127).

49 = 175593 – 56 + 3 (mod 127)

49 = 175540 (mod 127)

Умова виконується. Отже, точка P належить еліптичній криві.

1. Для точки Q = (62, 12)

122 = 623 – 62 + 3 (mod 127)

144 = 238328 – 62 + 3 (mod 127)

144 = 238269 (mod 127)

Умова виконується. Отже, точка Q належить еліптичній криві.

Тепер знайдемо суму точок P і Q. Для цього використаємо алгоритм подвійного і потрійного зведення точок на еліптичній кривій. Враховуючи, що P і Q належить кривій можна використати алгоритм додавання точок для знаходження суми P + Q.

Нехай P = (xP, yP) і Q = (xQ, yQ). Тоді P + Q = R = (xR, yR),

де

xR = s2 – xP – xQ (mod 127)

yR = s (xP – xR) – yP (mod 127)

Для знаходження s використовуємо наступний алгоритм.

1. Якщо P ≠ Q: s = ((yQ – yP) / (xQ = xP)) (mod 127)
2. Якщо P = Q: s = (3\*x2 \* p – 1 / 2 \* y \* p) (mod 127)

Додавання точок:

Λ = (12 – 7) / (62 – 56) = 5/6 = 5 \* 6-1 = 5 \* 12 = 105 (127)

Для P ≠ Q  
xR = 1052 – 56 – 62 = 95 (mod 127)

yR = 105 \* (56 – 95) – 7 = 65 (mod 127)

Таким чином, P + Q = (95, 65)

Отже, точки P і Q належать еліптичній криві, і результат додавання також є точкою на цій криві.

**Завдання 2**



Щоб зашифрувати повідомлення методом Ель-Гамаля на кривій, потрібно обрати велике просте число P та генератор G (базову точку) на еліптичній криві E. Також потрібно обрати закритий ключ dA та обчислити відкритий ключ

QA = dA \* G.

1. C1 = k \* G
2. C2 = P + k \* QA

Для розшифрування використовуємо закритий ключ dA:

1. Обчислимо –dA \* C1 (де –dA – обернене за модулем dA) для отримання точки –dA \* C1 = -dA \* k \* G = -dA \* k \* G
2. Обчислимо P + (-dA \* k \* G), щоб отримати оригінальне повідомлення P

Реалізацію можна побачити у файлі main.py!!!