Лабораторна робота 5

Варіант 10

10. $A = 1$

$B = 03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AA$
$EAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3$

$m = 431$

$f(x) = x^{431} + x^5 + x^3 + x + 1$

Є основні класи Point та BinaryPolynomial

В BinaryPolynomial.cpp описані операції з поліномами, а також методи для отримання по рандомно згенерованій x точки координату y так, щоб точка (x,y) знаходилась на еліптичній кривій.

Point.h містить реалізацію довгої арифметики з використанням уже оверрайднутих операцій для BinaryPolynomial, адже координати цього типу. Також там міститься вже конвертнутий в бінарний вигляд B та A - коеффіцієнти кривої. Іще там же можна знайти метод для перевірки того, що точка на кривій.

Point.cpp містить лише генерацію точки та метод для виведення точки в консоль і результату перевірки, що точка знаходиться на еліптичній кривій.

diffie_hellman.cpp містить просто основний код для виклику усіх потрібних функцій алгоритму, з генерацією точки, її виведенням, отриманням точки Боба, отриманням точки Аліси, а потім шифруванням їх.

Отже спочатку ми маємо згенерувати точку. Для цього згенеруємо її координату x, я генерую рандомно по вісім бітів до 431, а потім вирішую квадратне рівняння для отримання розв’язку у функції get_square_solution(), повторюю поки рішення не буде нормальним, адже має бути додатним дискримінант - все це відбувається в generate_point(). Далі я використовую таку ж рандомну генерацію по 8 бітів для ключів Боба та Аліси. Помноживши кожну точку на свій ключ отримуємо точки кожного з них.

Множення реалізоване в функції mul() зі зменшенням степені поліному, при цьому перевіряється можливість того, що при домноженні на x в i-тій степені степінь остатку(всіх членів крім старшого) залишається меншою за 431. Операції над точками double_point() та add() в свою чергу використовують цю реалізацію множення поліномів, а вони вже використовуються для довгої арифметики над точками - додавання та множення.

Для мого варіанту отримав такі результати на випадково згенерених точках:

```
base =
x = 1100101011101000011010000100000100001111100001011110001001100101011010101001011010110110010011010000001001010100010
1110100110011010011101111110001000100011000111000000111001000101111110010011010111010100101000111001100000001100001010101011
1001110001010100100000011111010100101111101100010110111001001111011010101100101000101101011111010110011001001110110000001
1100000111111100000001011111101110000001111011001010100111100100011011010100
y = 10010011101100111010101111101100011011010010101010000100101111001001111111011000000000110100101111001010111110111011
1111110111001000100011001110110000000000010100011011010011101110001100100010101100001010010011010011011110100110000110000
0111111011011100101001001100100000010100100101110000100001110001010100001000010100100101011100101001100110101000011111011
1100111111011111100111001011100010010010110100001011111100011111101110001001
on curve = 1
```

```
Alice key = 1010011101001000010000011000001111111001010011101000110111010101111100101010100000001010001101100111
Alice point =
x = 0010010100110000000011000110101001001010101001111100100100100101101100110010110111101000010011001011110011000100011
01111100100000101001100011110110001111100110000010110000100111110011100000111100111100010001011000110100010101001010100
1111010010111100111011010011010011111010011100101000001101110001000000110110111100001010101110110000011001010000110100011
0011001000010110111110000111001100010100100111101110101000011111111011110110
y = 000011001000110100110010000110000000111010000000111101010101100001000010100011001011111000011110110010010001000101110
0001001000100010001100001110011010100100110001010010010011111111011101011111110100101011001000010110000000100011100000000
1111101101001010011101100010101101000111010111000000100000011010110100011001000010001100101110110101001011111111000111101
1110101000010010011011001011111000110111100110000110001010001011010110011001000
on curve = 1
  Bob key = 0010101000001101011100011001000000000001100100101011111011010111000100010100111101101001110100111100001011100
1010100011111111011001001011100111101101111011100110001001000101101000010001010101000000111
  Bob point =
x = 0111001011111000100010001110101001010011001101110011010101100100110011011000111010101001001010100000000100000000100001
0111001100000001010110100100101001010000000101010111111111000101010101100110111101000000010010000010100011101110001101011010
1110100100111000010111111110000000100011100110100011111011001011101100001100010111001011111111000101000000110111111010001010
000100100000011000100001111011111100000001111111010011110100010011101001111110
y = 101111000111000011100000000000110001000111010000000101111010011100010000110101101000111001011001100000000111010000100
1001100000010010011100000110111110101011101111000101000100000011000000000001100000001000010101111011011110010111111101111110111
0000101001011111100011000001101011001010010001010110001101010010101101100010010100111000111011111001010010000001001100010O
1111001010101011111100000110011111011011110110011100111111110011111101010101100
on curve = 1
  Bob's coded point =
x = 0111111000010010000100110101110101110001011110010100100111001000101101101110110101001100100011010101100100100111000000
0010000010010101100101000000000011101100011011100101110111111111000000101111111010011011110111010100101110101100100110101111
1101110010010100101010001001100011000101101001100001111111100101100100000101100000000110110110000000010110001101111010010
1111000111100010010011001111011101111111110000101011100110000000111010010100110
y = 0100011011001001010110001100010011110011110000000001101111111101010000000010110011101111111011000011011000111000101001O
0100000011001001011000110010111011100010000101101001000010011101101100000001011001100001111110101010101001010101110010110O
1000001011001000110000000100011100111011011001110111010000000101001101001011101010010101010101110111101101010010100000110001
0010010110011010011000101100101101110001101101110001111101000101110110011O
on curve = 1

Alice's coded point =
x = 0111111000010010000100110101110101110001011110010100100111001000101101101110110101001100100011010101100100100111000000
0010000010010101100101000000000011101100011011100101110111111111000000101111111010011011110111010100101110101100100110101111
1101110010010100101010001001100011000101101001100001111111100101100100000101100000000110110110000000010110001101111010010
1111000111100010010011001111011101111111110000101011100110000000111010010100110
y = 0100011011001001010110001100010011110011110000000001101111111101010000000010110011101111111011000011011000111000101001O
0100000011001001011000110010111011100010000101101001000010011101101100000001011001100001111110101010101001010101110010110O
1000001011001000110000000100011100111011011001110111010000000101001101001011101010010101010101110111101101010010100000110001
0010010110011010011000101100101101110001101101110001111101000101110110011O
on curve = 1
```

Перевірка on curve = 1 показує, що усі точки знаходяться на еліптичній кривій.