Assignment # 4

Due : 11/20/2023

1. *Elliptic Curve Cryptography*
   Elliptic Curve $E : y^2 \equiv x^3 + x + 7 \bmod 29$ is given.

   (a) Find any point α on the curve.

   (b) Compute the coordinates of the points $2\alpha, 3\alpha, 4\alpha$ and 5α on the given curve.

   (c) Find the coordinates of the points 8α by computing $3\alpha + 5\alpha$ and $4\alpha + 4\alpha$. Verify that you find the same point.

   (d) Find the number of points $\|E\|$ of the given curve.

2. *Elliptic Curve D-H Key Exchange*
   Alice and Bob want to share a key using D-H Key Exchange on Elliptic Curves. And, they choose the elliptic curve $E : y^2 = x^3 - x + 188 \bmod 751$ and a generator point $\alpha = (0, 376)$.
   Bob chooses $a_B = 5$ as the private key and Alice chooses $a_A = 3$.

   (a) Find the public keys for Alice and Bob.

   (b) Using D-H Key Exchange, find the common key generated by Alice and Bob.

3. Implement the square and multiply algorithm using a computer language of your choice (I recommend sage, python, java, or other math environments such as magma. The environment should have native BigInteger support, so do not use C/C++ etc.). The program should print all intermediate results. For sage and python, you can use the following template:

```
def my_pow(b,e,m):
    """ Computes b^e mod m using the square and multiply algorithm"""
x =pow(b,e,m) # remove this line  and place your code here instead
return x
```

   Compute the following exponentiation $a^b \bmod N$ using your program:

   (a) $a = 235973, b = 456872884723247, N = 583884$

   (b) $a = 984327455683, b = 1253489582, N = 994348472542$

   Print the output of your program (including the intermediate steps) and turn it in together with your source code.