CSC427 Encryption Tutorial

1. Explain how Diffie-Hellman Key Exchange works in your own words.

2. We have provided you with the starter code (**ecc.py**) for *Elliptic Curve Cryptography (ECC).* More specifically, it is an example of multiplication of EC points. You don't need to implement anything. Simply run the code and describe what pattern did you notice.

3. For the last column, calculate what ciphertext should it be.
   Do it in the format similar to what is given in the slides and the final result should be similar to ***00000000000000000000000000001011100***

p	7	7	7	7
plaintext	1	1	0	0
q	13	2526	2022	26
ciphertext	92			

Note: *N = 2, Q = 32*

4. We have provided you with the starter code (rsa.py) for *Rivest-Shamir-Adleman (RSA)*. Follow the instructions in the file and paste the encrypted message here.