Vikash Deo
Lab 4: (Cryptography)
My N number -> 15708475

1. **RSA**

Using the prime numbers p=13 q=3
My N number -> 15708475

Plaintext Message (m) = 75 mod 38 = 37

Now, the plaintext message which we have to encrypt is **m = 37**.

Value of **n = pq = 13 x 3 = 39.**
Value of **Φ = (p-1) (q-1) = 12 x 2 = 24**.

Let, value of **e be 5** which is less than n = 39 and has no common factors with **Φ.**

So, (n, e) which is (39, 5) is the public key.

Now, choosing d such that **ed mod Φ = 1;**

Using brute force, we can see the (multiples of **Φ, 24**)+1 should be divisible by **5 (e)**.
(Multiples of **Φ, 24**)+1 = 25; 49; 73; 97; 121; 145

ed = 5 x 29 = 145 and 145 mod 24 = 1.

Here, I assumed the value of **d to be 29**. (I didn't use 25 because both d, e would have same vale, 5, which would make my public and private key same).

So, (n, d) which is (39,29) my private key.

Encrypting the message m = 37:

$$\mathbf{C = m^e \bmod n = 37^5 \bmod 39 = 69343597 \bmod 39}$$
$$\mathbf{C = 7}$$

Decrypting message received, c=7, to get original message:

$$m = c^d \bmod n = 7^{29} \bmod 39 = 37 \text{ (using WolframAlpha)}$$

So, decrypted message $\mathbf{m = c^d \bmod n = 7^{29} \bmod 39 = 37}$ which is the original message.

2. Diffie – Hellman

Last two digit of my NYU ID is 75. So, secrets chosen by Alice and Bob will be17 and 15, respectively.

Alice's secret integer: **a= 17**
Bob's secret integer**: b=15**.

Now, let value of **n, which should be prime is 13** and value for base **g to be 5** which is less than n. These numbers are shared between Alice and bob.

Therefore, a =17, b = 15, n=13 and g = 5.

Now Alice will calculate value of A which is given by:

$$\mathbf{A = g^{a} \bmod n = 5^{17} \bmod 13 = 5}$$

Hence, the value of **A is 5.**
Alice will share values of A, g and n with Bob.

At Bob, he will have his own secret value of b, which is 15. Now he will calculate value B as follows:

$$\mathbf{B = g^{b} \bmod n = 5^{15} \bmod 13 = 8}$$

This value of B computed will be shared back with Alice.

Now Alice has values, g, n, A, B shared ones and a as secret one

Now, Alice will calculate Key K as $\mathbf{K = B^{a} \bmod n = 8^{17} \bmod 13 = 8}$

Also, Bob will calculate Key K as $\mathbf{K = A^{b} \bmod n = 5^{15} \bmod 13 = 8}$

Here we can see that Alice and Bob both have same KEY **K = 8,** but still have their secret values 'a=17' and 'b=15' with them.