Answer for homework 2

Question 1:

1.

Suppose that Alice and Bob choose a=4 and b=7, and then Alice calculates $g^a \, mod \, p = 7^4 \, mod \, 13 = 9$, Bob calculates $g^b \, mod \, p = 7^7 \, mod \, 13 = 6$.

After that Alice and Bob exchange the number they calculated, which means Alice receives 6 and Bob receives 9.

And then Alice calculates $g^{ba} \, mod \, p = 6^4 \, mod \, 13 = 9$, Bob calculates $g^{ab} \, mod \, p = 9^7 \, mod \, 13 = 9$.

Then Alice and Bob share the key **9**.

2.

(a)

The Man-in-the-middle attack assumes that there is an attacker blocking communication between Alice and Bob in the middle. Attackers can disguise themselves as Alice and Bob and exchange keys with them, making Alice and Bob think they have exchanged keys, but in reality, they have exchanged keys with the middle attacker.

The process of Man-in-the-middle attack is that the attacker first selects an m and sends $g^m \, mod \, p$ to Alice and Bob respectively, and accepts the keys sent back by Alice and Bob. This way, the attacker establishes so-called symmetric keys with Alice and Bob respectively, and can decrypt their ciphertext.

(b)

a & c:

Alice sends $g^a \, mod \, p = 7^4 \, mod \, 13 = 9$ to Mallory, Mallory sends $g^m \, mod \, p = 7^5 \, mod \, 13 = 11$ to Alice.

Alice calculates $g^{am} \, mod \, p = 11^4 \, mod \, 13 = 3$, Mallory calculates $g^{ma} \, mod \, p = 9^5 \, mod \, 13 = 3$.

So Alice and Mallory shares key **3**.

b & c:

Bob sends $g^b \, mod \, p = 7^7 \, mod \, 13 = 6$ to Mallory, Mallory sends $g^m \, mod \, p = 7^5 \, mod \, 13 = 11$ to Bob.

Bob calculates $g^{bm} \, mod \, p = 11^7 \, mod \, 13 = 2$, Mallory calculates $g^{mb} \, mod \, p = 6^5 \, mod \, 13 = 2$.

So Bob and Mallory shares key **2**.

Question 2:

1.

First, find two very big prime number **p** and **q**, N=p*q;

Let z=(p-1)(q-1), find a number **e** that **e** is relatively prime to z and 2<e<z;

Calculate d = e^(-1) mod N;

Then we get public key (N, e) and private key (N, d).

To do the encryption, we calculate the C = M^e mod N(M means plaintext, C means Ciphertext).

If we want to do the decryption, calculate C^d mod N and we will get M.

2.

1)

e = d^(-1) mod (p-1)(q-1) = 19^(-1) mod 160 = 59

(Knowing that 19*59 mod 160 = 1)

2)

c = m^e mod N = 8^59 mod 187 = 172

to verify the result,

c^d mod N = 172^19 mod 187 = 8 = m