**Information Security Homework #2**

**Question I. DH key exchange**

**1. Simulate Diffie-Hellman algorithm to exchange keys**

***Answer***:Based on the Diffie-Hellman Key Exchange protocol, the process of key exchange between Alice and Bob is shown in Figure 1. Following this procedure, suppose Alice randomly generates private key and computes the public key:

Then, Alice sends **A** to Bob. Suppose Bob randomly generates a private key and computes the public key:

Then, Bod sends **B** to Alice. Based on this, Alice can calculate the shared key:

Similarly, Bob can calculate the shared key:

**So, the shared key between Alice and Bod is 5**.

**2. Simulate Diffie-Hellman Man-in-the-middle attack**

**(a). *Answer***: As shown in Figure 2. The Man-in-the-middle attack assumes an attacker is **blocking communication between Alice and Bob in the middle**. Attackers can disguise themselves as Bob or Alice 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 a Man-in-the-middle attack is that the attacker first generates a key **m** and sends 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). *Answer***: The overall calculation process is the **same** as in question 1.

* **a** and **c**: Alice generates private key and computes . Then, Alice sends **A** to Mallory. Because Mallory generates and computes . Then, Mallory sends **C** to Alice. Alice can calculate the shred key and Mallory can calculate the shared key . **So, the shared key between a and c is 5.**
* **b** and **c**: Bob generates private key and computes . Then, Bob sends **B** to Mallory. Because Mallory generates and computes . Then, Mallory sends **C** to Bob. Bob can calculate the shred key and Mallory can calculate the shared key . **So, the shared key between b and c is 8.**

**Question Ⅱ. RSA Encryption**

**1.Briefly describe RSA Asymmetric Encryption Process**

***Answer***:The RSA Asymmetric Encryption Process can be divided into the following steps.

* *Step 1.* Choose two huge primes and and compute
* *Step 2.* Define
* *Step 3.* Find a public key such that and mutually prime with . Calculate a modulo inverse element of the chosen private key as the public key, where . Then get the public key and private key **.**
* *Step 5.* Perform encryption and decryption, where is plaintext and is ciphertext:

**2. Calculation**

**(a). *Answer***: Because Bob chooses the secret key **d** as 19. Then, we can calculate the public key **e** for Bob as (Knowing that ) and 59 is mutually prime with 160. **So, the public key for Bob is (187, 59).**

**(b). *Answer***: Based on the encryption process, we can get the ciphertext

To verify that the result is correct, it can be verified by decryption. Based on the decryption function, the plaintext can be obtained:

The same as the original plaintext value, so the result is correct.

**Appendix Figures:**

**Figure 1.** The process of key exchange between Alice and Bob.



**Figure 2.** The process of Man-in-the-middle attack.

