Information Security Homework #2

I. DH key exchange

1. Simulate Diffie-Hellman algorithm to exchange keys

Alice and Bob share primes $p = 13$ and generators $g = 7$. Requirements: Choose the secrete random numbers a and b for Alice and Bob respectively (note: a, b $\in$ [1,p-1]), and then show how Alice and Bob generate the shared key.

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

(a) Briefly describe the principle and process of Man-in-the-middle attack.

(b) Assume that the private random number of Mallory $c = 5$, and find the shared key between a and c, *b* and c (a and b are taken from the first question).

II. RSA Encryption

1. Briefly describe RSA Asymmetric Encryption Process

2. Calculation

Given prime numbers $p = 11, q = 17,$ assume Bob chooses the secret key d as 19.

1) Calculate the public key e for Bob;
2) Suppose Alice wants to send the plaintext $m = 8$ to Bob, calculate the ciphertext c and verify its decryption results.

To speed up the calculation, exponentiation by squaring algorithm can be used.

➢ Submission method

- Please name the PDF file "2024.M2.InformationSecurity_hw2_yourname" then email it to both TA and Teacher before 11:59 pm on December 26th. Email title has the same name as the PDF file.
- Please refer to the file “Homework template.docx” for the homework format.