Public Key Encryption II

IMPORTANT NOTES: Study lecture materials at least 1 hour and prepare Question 1-3 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. Briefly explain Diffie-Hellman key exchange.

2. Alice and Bob are the employees of S&M investment funds. Alice needs to send a 1GB (GigaByte) file to Bob over a public network. By the instruction of the company's CIO all employees have taken a course in using modern cryptographic tools including symmetric and asymmetric encryption algorithms. Alice and Bob each have generated a pair of public and private keys and exchanged their public keys.

   What are Alice's options to **efficiently** send the file to Bob when it contains confidential information? Discuss the potential security threats for each of the options.

3. Perform encryption and decryption using RSA algorithm where: $n = p \times q$; $C = M^e \bmod n$; $P = C^d \bmod n$; $e \times d \bmod \phi(n) = 1$; plaintext M and Ciphertext C; e and d are public and private key. for p=3; q=11; e = 7; M = 5.

4. Users A and B use the Diffie-Hellman key exchange technique with a common prime p=11, primitive root g= 2.

   (a) a = 6 (A's private key), what is A = $g^a \bmod p$ (A's public key)?

   (b) If B = $g^b \bmod p$ (B's public key) = 3, what is the shared secret session key?

   (c) What is b, B's private key?

5. (Security Analysis) Given the RSA public key (N, e) and ciphertext c, why is it hard for an attacker to compute the message m?

6. (Security Analysis) In the lectures, we discussed the insecurity of basic Diffie-Hellman key exchange to the Man-in-the-Middle (MITM) attack, where an attacker replaces the public keys A, B of Alice and Bob with its own M. Discuss how this weakness can be fixed, and why it will prevent the MITM attack.

7. (Security Analysis) Consider the El-Gamal public-key cipher described in the lectures.

   (a) Can an MITM attack apply? Explain your reasons.

   (b) Given the El-Gamal public keys A, B and ciphertext c are known, discuss why it is hard for an attacker to compute the message m.