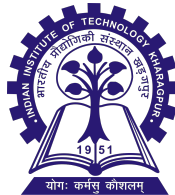


Tutorial on RSA and Diffie Hellmann

Cryptography and Network Security

October 25, 2022



Question 1

Alice has decided to use RSA for encryption and has generated two large primes p and q and computed $N = pq$. She has also chosen encryption key $e_A = 3$ and computed her private d_A . When her friend Bob hears about this, he also wants to use RSA. Alice assists him by choosing for him $e_B = 5$ and computing d_B , using the same N . Alice gives Bob his keys (N, e_B) and d_B . The next day their common friend Charlie sends message m encrypted to both Alice and Bob, using their respective encryption keys. However, the adversary Deborah eavesdrops and gets hold of the two ciphertexts c_A and c_B . Deborah also notices that Alice and Bob use the same N . Show how she can recover m . You may assume that $\gcd(m, N) = 1$.

Question 2

A web-based auction site uses textbook RSA encryption to maintain the secrecy of bids. The site has public RSA key (N, e) . For the sake of this problem we make the completely unrealistic assumption that a bid is sent in a message containing only a single integer, representing the bid value. Now, Alice has just made a bid and the adversary Mallory has eavesdropped and heard the ciphertext c . Mallory's main aim is to prevent Alice's bid from winning. Of course, he cannot recover Alice's bid, but makes the guess that her bid is an integer which is a multiple of 10. Show that, if Mallory's guess is right, he can himself make a bid which is 10% higher than Alice's.

Question 3

A DH-based key exchange protocol for wireless mobile networks was proposed by Jon: The system has a common prime modulus p and a generator g . Each party i has a long-term private key $x_i \in \mathbb{Z}_{p-1}$ and a public key $X_i = g^{x_i} \pmod{p}$. To establish a session key between a mobile subscriber M and a base station B , the following protocol is executed (with all arithmetic in \mathbb{Z}_p): (1) $B \rightarrow M : g^{x_B + N_B}$; (2) $M \rightarrow B : N_M + x_M$ where N_B and N_M are one-time random nonces (once used random numbers). B calculates the session key as $K_{MB} = (g^{x_M + N_M} X_M^{-1})^{N_B}$ and M calculates it as $K_{MB} = (g^{x_B + N_B} X_B^{-1})^{N_M}$. Then they complete the authentication with a challenge-response using this K_{MB} .

- (a) Show that the Jon's protocol is correct in the sense that B and M calculate the same K_{MB} value.
- (b) Show that an attacker who has compromised a session key from a previous run, for which (s)he has recorded the messages, can impersonate B . [Hint: Let the attacker replay B 's message from the previous session.]

Question 4

Design a protocol that allows three parties P_1 , P_2 and P_3 to exchange a single symmetric key K , minimizing the number of exchanged messages. To do this, extend the Diffie-Hellman key exchange discussed in the lecture to three parties. The following conditions have to be fulfilled:

- (a) Given the CDH-assumption, only the parties P_1 , P_2 and P_3 can know the key K .
- (b) A hash $H(K)$ has to be exchanged to verify the exchanged key K between all parties.
- (c) Use as few messages as possible.

You can give your solution as a sequence of messages sent from P_i to P_j , e.g., $P_i \xrightarrow{m} P_j$