

Homework 3 due on March 20, 2007

Problems from the textbook:

- 5.3
- 5.6
- 5.12
- 5.19

Problem 1.

One way to protect Diffie-Hellman against the Man-in-the-Middle attack is to encrypt the Diffie-Hellman value with the other side's public key. Why is this the case, given that an attacker can encrypt whatever it wants with the other side's public key?

Problem 2

Each node N of a network is been assigned a unique secret key K_n . This key is used to secure communications between the node and a trusted server. That is, all the keys are stored on a server. User A , wishing to send a secret message M to user B , initiates the following protocol:

1. A generates a random number R and sends to the server his name A , destination B , and $E_{K_a}[R]$
2. Server responds by sending $E_{K_b}[R]$ to A
3. A sends $E_R[M]$ together with $E_{K_b}[R]$ to B .
4. B knows K_b , thus decrypts $E_{K_b}[R]$ to get R and will subsequently use R to decrypt $E_R[M]$ to get M .

Analyze this protocol. Is it safe?

Problem 3

Devise a protocol based on a pre-shared secret key that hides identities and gives PFS for identity hiding. Make two variants, one in which an active attacker can learn only the initiator's identity, and one in which an active attacker can learn only the target's identity.

