Advanced Course on Computer Security, course exam

You can write your answers in Finnish, Swedish, English, German and French. In every case, write clearly using big enough letters. Write on every paper your name, the name of the course, date, your student or identification number and your signature. Enumerate the pages.

1. Explain the basic Diffie-Hellman key agreement and show the man-in-the-middle attack against it.

2. Show how an opponent can use the vulnerability of the following protocol in order to decrypt the messages. Each node N in the network has been assigned a unique secret key K_n. This key is used to secure communication between the node and a trusted server. That is, all the keys are stored also on the server. User A, wishing to send a secret message M to user B, initiates the following steps:

   Step1. A generates a random number R and sends to the server his name A, destination B, and $E(K_a, R)$.

   Step2. Server responds by sending $E(K_b, R)$ to A.

   Step3. A sends $E(R, M)$ together with $E(K_b, R)$ to B.

   Step4. 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.

3. Explain the concept of a key tree. Show how a member can be deleted from a key tree, what nodes then need new keys and what members have to calculate new keys in the leave operation.

4. Explain the concept of a hash chain. What is the motivation to use them in network protocols? Show the modifications to the HIP Base Exchange, if hash chains are used instead of signatures. Below is the standard Base Exchange.

   I1 $I \longrightarrow R$: HIT(i), HIT(r)

   R1 $R \longrightarrow I$: HIT(r), HIT(i), puzzle, $DH(r), K(r)$, sig

   I2 $I \longrightarrow R$: HIT(i), HIT(r), solution, $DH(i), K(i)$, sig

   R2 $R \longrightarrow I$: HIT(r), HIT(i), sig