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 RSA and give a small example.
2. A is using the following protocol to send the message M to B. In the protocol, PU_b and PU_a are the public keys of B and A, respectively. The symbol $E(PU, M)$ means encryption of the message M with the public key PU.

   Step1. A sends B the following block: $(A, E(PU_b, M), B)$.

   Step2. B acknowledges receipt by sending to A the following block: $(B, E(PU_a, M), A)$.

   Show the vulnerability of the protocol by demonstrating an attack against it. Show also how the protocol can be improved so that the attack fails.
3. Explain the concept of the key tree. Show how a member can be joined to a key tree, what nodes need new keys and what members have to calculate new keys in the join operation.
4. Consider the HIP 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

   The Base Exchange protocol authenticates the communication partners to each other. Analyse, how sure I and R can be of their real partner, if basic DNS is used with or without certificates.