Advanced Course on Computer Security, separate exam, February 4, 2011

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. Construct the multiplication table of the finite field $GF(2^3)$.
2. Explain the design principles for cryptographic protocols.
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 $I \longrightarrow R$: $\mathrm{HIT}(i),\ \ \mathrm{HIT}(r)$
   R1 $R \longrightarrow I$: $\mathrm{HIT}(r),\ \ \mathrm{HIT}(i), \mathrm{puzzle}, DH(r), K(r), \mathrm{sig}$
   I2 $I \longrightarrow R$: $\mathrm{HIT}(i),\ \ \mathrm{HIT}(r), \mathrm{solution}, DH(i), K(i), \mathrm{sig}$
   R2 $R \longrightarrow I$: $\mathrm{HIT}(r), \mathrm{HIT}(i), \mathrm{sig}$

   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 and certificates are in use or not in use. What kind of checks is it necessary or possible to make, if certicates are used?