Advanced Course on Computer Security, separate exam, April 12, 2011

You can write your answers in Finnish, Swedish, English, German. 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 Diffie-Hellman key exchange. Show also the weakness of the basic scheme.
3. Consider the following protocol. In the protocol, A and B have a secret symmetric key with server S and they try to agree on a common secret session key with the help of the server.

   1. $A \longrightarrow S$: A, B
   2. $S \longrightarrow A$: $\{K_{AB}\}_{K_{AS}}$, $\{K_{AB}\}_{K_{BS}}$
   3. $A \longrightarrow B$: $\{K_{AB}\}_{K_{BS}}$, A

   Show the weakness of the protocol by constructing a man-in-the-middle attack, where A thinks he is communicating with B but in reality he is communicating with C.
4. Simulate the following version of the Burmester-Desmedt group key agreement protocol using 4 members (in the algorithm $b_0 = c_0 = 1$.):

Phase 1	$U_i \longrightarrow U_{i-1}, U_{i+1}$:	$t_i = g^{r_i}$
	Then U_i calculates	$X_i = (t_{i+1}/t_{i-1})^{r_i}$,
		$Z_{i-1,i} = t_{i-1}^{r_i}$
Phase 2	$U_i \longrightarrow U_{i+1}$:	b_i, c_i, where recursively
		$b_i = X_i b_{i-1}$, $c_i = b_{i-1} c_{i-1}$.
Phase 3	U_1 sets	$d_0 = c_m = X_1^{m-1} \cdot X_2^{m-2} \cdots X_{m-1}$
	$U_i \longrightarrow U_{i+1}$:	d_i, where recursively
		$d_i = d_{i-1}/X_i^m$
		and U_i calculates $K = d_{i-1} \cdot Z_{i-1,i}^m$

   Show the calculations done by every member. Especially, show how everybody calculates the common key step by step.