1. Consider the finite field $GF(2^8)$ which is defined with the help of the irreducible polynomial $X^8 + X^4 + X^3 + X + 1$. Calculate the product $(x^5 + x^3 + x + 1) \cdot (x^6 + x^4 + x^3 + x^2)$.

2. Explain the Anderson’s and Needham’s robust principles for public key protocols.

3. Consider the following key transport protocol using public key cryptography:
   
   1. $A \rightarrow B$: $A, K_A$
   2. $B \rightarrow A$: $E_A(K_{AB})$
   3. $A \rightarrow B$: $\{N_A\}_{K_{AB}}$
   4. $B \rightarrow A$: $\{B, K_B, Cert(B), Sig_B(N_A)\}_{K_{AB}}$

   In the first message, $A$ sends his identity and his public key. $B$ then returns a symmetric key, generated by him and encrypted with $A$’s public key. In the third message, $A$ sends a nonce encrypted with the new session key. Finally, $B$ acknowledges by sending his identity, public key, certificate and signature. All is encrypted with the new session key.

   There is an attack against this protocol. The adversary, $C$, is a legitimate user known to $B$. Further, $C$ is able to set up simultaneous sessions with both $A$ and $B$. In the attack, $C$ is able to convince $A$ that $C$ is $B$. The attack starts as follows:
   
   1. $A \rightarrow C_B$: $A, K_A$
   2. $C_B \rightarrow A$: $E_A(K_{AB})$
   3. $A \rightarrow C_B$: $\{N_A\}_{K_{AB}}$
   4'. $C \rightarrow B$: $C, K_C$

   How does it continue? How is it possible, by modifying the protocol, to avoid the attack?

4. 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. Draw a diagram to clarify your explanations.