Final: Part I

Note

This is a closed-book exam. Part I contains five problems, each accounting for 10 points.

Problems

1. Explain the following properties concerning the strength of a cryptographic hash function.
   (a) preimage resistant (one-way property)
   (b) collision resistant (strong collision resistant)
   (c) second preimage resistant (weak collision resistant)

2. A hash code can be used to provide message authentication in various ways. Let H be a hash function. Assume that A and B share a secret key K and a common secret value S. Below are three possible ways to achieve message authentication for message transmissions from A to B:

   (1) A $\rightarrow$ B: $E(K, [M \parallel H(M)])$
   (2) A $\rightarrow$ B: $M \parallel E(K, H(M))$
   (3) A $\rightarrow$ B: $M \parallel H(M \parallel S)$

   (a) In each case, what are the corresponding operations that should be performed by B?
   (b) How do the three schemes compare?

3. What is a hierarchical key control (for key distribution)? How does it operate? What are its advantages?

4. Below is a protocol for A and B to establish a session with a secure session key.

   (1) A $\rightarrow$ B: $ID_A \parallel N_a$
   (2) B $\rightarrow$ KDC: $ID_B \parallel N_b \parallel E(K_b, [ID_A \parallel N_a \parallel T_b])$
   (3) KDC $\rightarrow$ A: $E(K_a, [ID_B \parallel N_a \parallel K_s \parallel T_b]) \parallel E(K_b, [ID_A \parallel K_s \parallel T_b]) \parallel N_b$
   (4) A $\rightarrow$ B: $E(K_b, [ID_A \parallel K_s \parallel T_b]) \parallel E(K_s, N_b)$

Note that T_b is a time relative to B's clock.

(a) What is the purpose of T_b? What is the main advantage of having T_b relative to B's clock?

(b) How can A use $E(K_b, [ID_A \parallel K_s \parallel T_b])$ to establish another session with B without involving the KDC?

5. Below is a one-way authentication protocol based on asymmetric encryption.

(1) A $\rightarrow$ B: ID_A

(2) B $\rightarrow$ A: R_1

(3) A $\rightarrow$ B: $E(PR_a, R_1)$

(a) Explain the protocol.

(b) What type of attack is this protocol susceptible to? Please describe an attack scenario.