Research in Information Security (CSE540)

Mid Semester Examination (Monsoon 2025)

International Institute of Information Technology, Hyderabad

Time: 1 hour and 30 minutes Total Marks: 40

Instructions: Answer *ALL* questions. This is a closed book and notes examination.
Calculator is allowed. No query is allowed during the examination period.

1. **(a)** Consider the following hierarchical access control scheme. The proposed scheme consists of three main phases, namely the initialization phase, the key generation phase, and the key derivation phase. The the initialization phase and the key generation phase described below.

Initialization Phase: To complete the initialization phase, the trusted Central Authority (CA) executes the following steps:

(a) Builds the hierarchical structure according to the relationships among the security classes.

(b) Randomly selects a large prime number p.

(c) Selects an elliptic curve E defined over $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ and selects a base point $G \in E(\mathbf{Z}_p)$.

(d) Chooses its private key d_{CA} and computes the public parameter $Q_{CA} = d_{CA} \cdot G$.

(e) Publishes (p, q, G, Q_{CA}).

Key Generation Phase: For each security class SC_i, CA executes:

(a) Selects a secret parameter d_i and computes $Q_i = d_i \cdot G$. Both d_i and Q_i are secret.

(b) Computes $k_{SC_i} = (Q_i + Q_{CA} + d_{CA}Q_i)$.

(c) Computes the secret key $SK_{SC_i} = ([k_{SC_i}]_x \| [d_{CA}Q_i]_x)$, where $[P]_x$ and $[P]_y$ denote the x-coordinate and y-coordinate of the elliptic curve point P, respectively.

(d) For all security classes SC_j where $SC_i \leq SC_j$:

i. Randomly selects a secret $r_{j,i}$ and computes the point $d_i r_{j,i} G = (\alpha_{j,i}, \beta_{j,i})$.

ii. Encrypts the point $(SK_{SC_i}, r_{j,i})$:

$$\omega_{j,i} = (SK_{SC_i}, r_{j,i}) + C_{j,i}Q_j$$

where $C_{j,i}$ is a random positive integer.

iii. Computes

$$\gamma_{j,i} = C_{j,i}G$$

iv. Computes $\delta_{j,i} = \beta_{j,i}Q_i$.

v. Declares $\{\omega_{j,i}, \gamma_{j,i}, \delta_{j,i}\}$ as public parameters.

Design the key derivation phase for the above hierarchical access control scheme.

(b) Suppose two users A and B use the ECC key exchange technique with a common prime $q = 211$ and an elliptic curve $E_q(a, b)$, where $a = 0$ and $b = -4$. Let $G = (2, 2)$ a base point on $E_q(a, b)$.

(i) If user A has private key $n_A = 2$, what is the A's public key P_A?

(ii) If user B has private key $n_B = 3$, what is the B's public key P_B?

(iii) What is the secret shared key?

[5 + 5 = 10]

2. (a) Explain the Cipher Block Chaining Mode (CBC) of Data Encryption Standard (DES) with encryption and decryption processes.

   (b) Discuss the man-in-the-middle attack on the Diffie-Hellman key exchange protocol.

[5 + 5 = 10]

3. (a) Explain a generalized Discrete Logarithm Problem (DLP)-based proxy signature model.

   (b) Consider the following bilinear-pairing based proxy signature scheme. Table 1 lists the notations and their meanings.

Table 1: Notations and their meanings used in Q3(b).

Notation	Meaning
Alice	Original signer
Bob	Proxy signer
G_1	A cyclic additive group, whose order is prime q
G_2	A cyclic multiplicative group of the same order q
P	A generator of G_1
$\hat{e}$	A bilinear pairing map
$H(\cdot)$	Map-to-Point function
$h(\cdot)$	Collision-resistant one-way hash function
s	KGC's secret key
Pub_{KGC}	KGC's public key, $\text{Pub}_{KGC} = sP$
y_o, x_o	Alice's public and private key, $y_o = H(ID_o)$
y_p, x_p	Bob's public and private key, $y_p = H(ID_p)$

Assumption: CDHP is hard.

- Alice (original signer) computes her public key $y_o = H(ID_o)$, where ID_o is her identity. Then, Alice obtains her private key $x_o \leftarrow KG_{\text{cdhp}}(\text{params-cdhp}, y_o)$ from KGC.
- Bob (proxy signer) computes his public key $y_p = H(ID_p)$, where ID_p is his identity. Then, Bob obtains his private key $x_p \leftarrow KG_{\text{cdhp}}(\text{params-cdhp}, y_p)$ from KGC.
- **Delegation capability generation:** Alice picks $k_o \in \mathbb{Z}_q^*$, computes $r_o = k_o P$, $C_o = H_o(ID_o, \omega, r_o)$ and $\sigma_o = x_o + k_o C_o$, where

$$H_o : \{0,1\}^* \times \{0,1\}^* \times G_1 \rightarrow G_1.$$

- **Delegation capability verification:** Bob accepts σ_o iff

$$\hat{e}(\text{Pub}_{KGC}, y_o)\, \hat{e}(r_o, C_o) =? \tag{1}$$

- **Proxy key generation:** Bob computes proxy key

$$\rho_p = h_1(ID_o, ID_p, \omega, r_o)x_p + \sigma_o,$$

where $h_1 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G_1 \rightarrow \mathbf{Z}_q^*$.

- **Proxy signature generation:** To sign a message m, Bob does the following:

  (a) Picks $k_p \in \mathbf{Z}_{q-1}^*$, computes $r_p = k_p P$ and then sets

$$C_p = H_o(ID_p, m, r_p).$$

  (b) Computes

$$\sigma_p = \rho_p + k_p C_p.$$

The proxy signature of message m is the tuple

$$\big((r_o, r_p), \sigma_p, (\omega, m)\big).$$

- **Proxy signature verification:** The verifier accepts the proxy signature of message m if and only if

$$\hat{e}(\text{Pub}_{KGC}, y_p)^{h_1(ID_o, ID_p, \omega, r_o)} \cdot \hat{e}(\text{Pub}_{KGC}, y_o) \cdot \hat{e}(r_p, C_p) \cdot \hat{e}(r_o, C_o) =? \quad (2)$$

For the delegation capability verification and proxy signature verification phases, complete Eqs. (1) and (2), respectively.

[5 + 6 = 11]

4. **(a)** With respect to Triple DES with Two Keys (3DES with Two Keys), explain the encryption and decryption methods.

   (b) Discuss in brief the Digital Signature Algorithm (DSA) and its security concern.

[4 + 5 = 9]

********** **End of Question Paper** **********