Name: ________________ **Matr. number:** ____________

Midterm Exam Introduction to Cryptography VU (Total: 30 points) 3 December 2025

1) (+1/-1 point per correct/incorrect answer... minimum 0, maximum 10 points)

Are the following statements true (T) or false (F)? Check the corresponding box.

☐ T ☐ F a) In an encryption scheme, key generation is a randomized algorithm, but encryption and decryption must be deterministic to ensure ciphertexts can be uniquely decrypted.

☐ T ☐ F b) Unlike monoalphabetic substitution ciphers (such as the Caesar cipher), polyalphabetic substitution ciphers (such as the Vigenère cipher) are immune to frequency analysis.

☐ T ☐ F c) Every perfectly secret encryption scheme is perfectly indistinguishable, and vice versa.

☐ T ☐ F d) According to Shannon's theorem, an encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ is perfectly secret if for every $m \in \mathcal{M}, c \in \mathcal{C}$, there is a unique key $k \in \mathcal{K}$ such that $\text{Enc}_k(m) = c$.

☐ T ☐ F e) Even if any of the round functions in a Feistel network are not invertible, the Feistel network as a whole is still invertible.

☐ T ☐ F f) A meet-in-the-middle attack allows an attacker to break a double-key cipher $E'_{(k,k')} := E_{k'} \circ E_k$ with approximately square root of the time complexity of a brute-force attack on E'.

☐ T ☐ F g) The AES block cipher is a substitution-permutation network.

☐ T ☐ F h) If $f(n)$ is a negligible function, then $n^{|f(n)|}$ is negligible.

☐ T ☐ F i) The block-cipher modes of operation ECB, CBC, and CTR are all EAV-secure (i.e., computationally indistinguishable in the presence of an eavesdropper).

☐ T ☐ F j) CTR mode is secure even with non-random IVs, as long as a different IV is used whenever calling the encryption algorithm Enc.

2) (5 points) Security definition:

Fill in the gaps. A private-key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is CCA-secure, i.e., *secure against chosen-ciphertext attacks*, if for every p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\epsilon(\cdot)$ such that $\Pr[\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}(n) = 1] \leq$ _____, where the experiment $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}(n)$ is defined as follows:

1. A key $k \leftarrow \text{Gen}(1^n)$ is generated.
2. $\mathcal{A}$ is given 1^n and access to _________________.
3. $\mathcal{A}$ outputs a pair of messages m_0, m_1 ___________.
4. A bit $b \leftarrow \{0,1\}$ is sampled and the challenge ciphertext $c^* := \text{Enc}_k(m_b)$ is given to $\mathcal{A}$.
5. $\mathcal{A}$ continues to have the same access as in step 2, but ______________________.
6. $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$. The output of the experiment is 1 if and only if _____.

3) (2+4 points) Private-key encryption:

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator (PRG). Also, for any binary string x, let $p(x) \in \{0,1\}$ denote its parity, i.e., whether the number of 1's in x is even (0) or odd (1). Consider the following encryption scheme Π for messages of length n:

- $\mathrm{Gen}(1^n)$: Return $k \leftarrow \{0,1\}^n$.
- $\mathrm{Enc}_k(m)$: Compute $k_0 \| k_1 := G(k)$ with $k_i \in \{0,1\}^n$. Let $r := k_{p(m)}$ and return $c := m \oplus r \oplus (p(r) \| 0^{n-1})$.
- $\mathrm{Dec}_k(c)$: Compute $k_0 \| k_1 := G(k)$. Let $s := k_{p(c)}$ and return $m := c \oplus s \oplus (p(s) \| 0^{n-1})$.

a) Show that Π is a correct encryption scheme. Hint: What is the parity of $r \oplus (p(r) \| 0^{n-1})$?

b) Show that Π is not EAV-secure. Make sure to specify the initial values of all variables you use!

4) (6 points) Message authentication codes (MACs):

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function (PRF). Prove, by giving a reduction, that the following MAC Π for messages of length n is secure (i.e., existentially unforgeable under adaptive chosen-message attacks).

$$\mathrm{Gen}(1^n)\text{: Return } k \leftarrow \{0,1\}^n. \quad \mathrm{Mac}_k(m) := F_k(m) \oplus m. \quad \mathrm{Vrfy}_k(m,t) := \mathrm{Mac}_k(m) \stackrel{?}{=} t.$$

5) (3 points) Authenticated encryption:

Let $(\mathrm{Gen}_E, \mathrm{Enc}, \mathrm{Dec})$ be a CPA-secure encryption scheme, and $(\mathrm{Gen}_M, \mathrm{Mac}, \mathrm{Vrfy})$ be a secure (deterministic, canonical) MAC. Use them to construct a secure authenticated encryption scheme by specifying all 3 algorithms.

Solutions

Are the following statements true (T) or false (F)? Check the corresponding box.

☐ T ☑ F a) In an encryption scheme, key generation is a randomized algorithm, but encryption and decryption must be deterministic to ensure ciphertexts can be uniquely decrypted.

☐ T ☑ F b) Unlike monoalphabetic substitution ciphers (such as the Caesar cipher), polyalphabetic substitution ciphers (such as the Vigenère cipher) are immune to frequency analysis.

☑ T ☐ F c) Every perfectly secret encryption scheme is perfectly indistinguishable, and vice versa.

☐ T ☑ F d) According to Shannon's theorem, an encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ is perfectly secret if for every $m \in \mathcal{M}, c \in \mathcal{C}$, there is a unique key $k \in \mathcal{K}$ such that $\text{Enc}_k(m) = c$.

☑ T ☐ F e) Even if any of the round functions in a Feistel network are not invertible, the Feistel network as a whole is still invertible.

☑ T ☐ F f) A meet-in-the-middle attack allows an attacker to break a double-key cipher $E'_{(k,k')} := E_{k'} \circ E_k$ with approximately square root of the time complexity of a brute-force attack on E'.

☑ T ☐ F g) The AES block cipher is a substitution-permutation network.

☐ T ☑ F h) If $f(n)$ is a negligible function, then $n^{|f(n)|}$ is negligible.

☐ T ☑ F i) The block-cipher modes of operation ECB, CBC, and CTR are all EAV-secure (i.e., computationally indistinguishable in the presence of an eavesdropper).

☐ T ☑ F j) CTR mode is secure even with non-random IVs, as long as a different IV is used whenever calling the encryption algorithm Enc.