Mid-term exam – March 20., 2026

No document is allowed. Unless indicated otherwise, answers must be carefully justified to receive full credit. The exercises are independent, but questions within the same exercise may depend on each other. You may use a result from a previous question by clearly stating it. You may answer in English or French. The duration is 1 hour 15 minutes.

Exercise 1 (4 points). *Short questions*

1. Define what a hash function and a compression function are, highlighting the differences between the two notions.
2. For each of the following statements, tell whether it is true or false *and justify*.
   - **i.** A collision-resistant hash function is also second preimage resistant.
   - **ii.** The one-time pad is IND-CPA secure.
   - **iii.** A *good* hash function has to be randomized.

Exercise 2 (10 points). *CFB mode of operation*

Let $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. The *cipher feedback* (CFB) mode of operation is defined as follows: The encryption of a message $m = m_1 \| \cdots \| m_t$ of length $t \times n$ is $c = c_0 \| \cdots \| c_t$ of length $(t+1) \times n$ where $c_0 = IV$ is an initialization vector and $c_i = m_i \oplus E_k(c_{i-1})$ for $i = 1, \ldots, t$.

1. Give the decryption algorithm. *A diagram may help!*
2. - **i.** To obtain a secure mode of operation, should the initialization vector be fixed or random? *Justify.*
   - **ii.** How can we encrypt a message whose length is not a multiple of n? Propose an explicit solution for the encryption and the decryption.
3. Let $m = m_1 \| \cdots \| m_t$ be a message and $c_0 \| \cdots \| c_t$ be a corresponding ciphertext. *We assume that E_k is a random permutation*.
   - **i.** Prove that if $c_i = c_j$ for some $i \neq j$, then $m_{i+1} \oplus m_{j+1} = c_{i+1} \oplus c_{j+1}$.
   - **ii.** Justify that the ciphertext blocks $c_0, \ldots, c_t$ are uniform in $\{0,1\}^n$.
   - **iii.** Give a value for t such that with probability $\geq \frac{1}{4}$, $c_i = c_j$ for some $i \neq j$.
4. In the IND-CPA game, the adversary queries pairs of equal-length mes-

sages $(m_{i,0}, m_{i,1})$. The challenger computes $c_i \leftarrow \mathsf{Enc}_k(m_{i,b})$ where b is either 0 or 1. From the c_i's, the adversary computes $\hat{b}$. Its advantage is $\left|\Pr\left[\hat{b}=1 \middle| b=1\right] - \Pr\left[\hat{b}=1 \middle| b=0\right]\right|$.
Describe an adversary for the IND-CPA game, when the encryption scheme is based on the CFB mode of operation, that has an advantage $\geq \frac{1}{4}$. *Be precise on the description of the pairs of messages* $(m_{i,0}, m_{i,1})$ *used in the attack: how many messages? of which length?*

Exercise 3 (6 points). *Multi-key security for MACs*

The *multi-key EUF-CMA security* is defined using the mk-EUF-CMA game below. The difference with the standard EUF-CMA game is that the adversary $\mathcal{A}_{\mathsf{mk}}$ plays against s challengers $\mathcal{C}_1, \ldots, \mathcal{C}_s$ instead of a single challenger:

1 Each challenger $\mathcal{C}_j$ samples a key $k_j \twoheadleftarrow \mathcal{K}$ (independently of the other ones);
2 For $1 \leq i \leq q$:
3 The adversary creates a query (m_i, ℓ_i), sent to the challenger $\mathcal{C}_{\ell_i}$;
4 The challenger $\mathcal{C}_{\ell_i}$ answers with a valid tag $t_i = \mathsf{Mac}_{k_{\ell_i}}(m_i)$;
5 The adversary outputs a pair (m, t) with $m \notin \{m_1, \ldots, m_q\}$.

The adversary is successful if there exists a key k_j such that $\mathsf{Vrfy}_{k_j}(m, t) = 1$.

The advantage $\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A}_{\mathsf{mk}})$ of an adversary $\mathcal{A}_{\mathsf{mk}}$ is its probability of success. The advantage function is

$$\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(q, s, t) = \max_{\mathcal{A}_{q,s,t}} \mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A})$$

where $\mathcal{A}_{q,s,t}$ is an adversary making q queries to s challengers with running time t.

1. Justify that $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Mac}}(q, t) = \mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(q, 1, t)$ for all q and t.

As a consequence, the mk-EUF-CMA security implies the standard EUF-CMA security. We shall now prove the converse: Both security are equivalent.

Assume we are given an adversary $\mathcal{A}_{\mathsf{mk}}$ that plays against challengers $\mathcal{C}_1$, $\ldots$, $\mathcal{C}_s$ in the mk-EUF-CMA game. Using $\mathcal{A}_{\mathsf{mk}}$, we build an adversary $\mathcal{A}$ playing against a challenger $\mathcal{C}$ in the EUF-CMA game: The adversary $\mathcal{A}$ simulates the mk-EUF-CMA game against $\mathcal{A}_{\mathsf{mk}}$. It must in particular answer each query of $\mathcal{A}_{\mathsf{mk}}$. To this end, $\mathcal{A}$ *guesses* $j \twoheadleftarrow \{1, \ldots, s\}$ and bets that $\mathcal{A}_{\mathsf{mk}}$ outputs a pair valid for the key k_j. It then plays the role of all the challengers but $\mathcal{C}_j$ and uses its own challenger $\mathcal{C}$ to play the role of $\mathcal{C}_j$. To play the role of a challenger $\mathcal{C}_\ell$, it samples a key k_ℓ and answers each query (m_i, ℓ) by computing $t_i = \mathsf{Mac}_{k_\ell}(m_i)$. At the end, $\mathcal{A}$ outputs the same pair (m, t) as $\mathcal{A}_{\mathsf{mk}}$.

2. **i.** How can $\mathcal{A}$ answer queries (m_i, j)? *Recall that $\mathcal{A}$ uses its own challenger $\mathcal{C}$ to play the role of $\mathcal{C}_j$.*

ii. Justify that whenever $\mathcal{A}_{\mathsf{mk}}$ output a valid pair for the key k_j, then $\mathcal{A}$ is successful.

iii. What is the probability that $\mathcal{A}$ correctly guessed j?

iv. Express $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A})$ in terms of $\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A}_{\mathsf{mk}})$ and s.

3. Deduce a bound on $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Mac}}(q,t)$ in terms of $\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(q,s,t)$ and s. *Carefully justify the bound.*