Examen partiel – 20 mars 2026

Aucun document n'est autorisé. Sauf indication contraire, les réponses doivent être soigneusement justifiées pour obtenir tous les points. Les exercices sont indépendants, mais pas toutes les questions. Vous pouvez admettre un résultat d'une question précédente en l'indiquant clairement. Vous pouvez répondre en anglais ou en français. La durée est de 1 heure 15 minutes.

Exercice 1 (4 points). *Questions courtes*

1. Définir ce que sont une fonction de hachage et une fonction de compression, en mettant en évidence les différences entre ces deux notions.
2. Pour chacune des affirmations suivantes, dire si elle est vraie ou fausse *et justifier*.
   - **i.** Une fonction de hachage résistante aux collisions est également résistante à la seconde préimage.
   - **ii.** Le masque jetable (*one-time pad*) est IND-CPA sécurisé.
   - **iii.** Une *bonne* fonction de hachage doit être randomisée.

Exercice 2 (10 points). *Mode opératoire CFB*

Soit $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ un chiffrement par bloc. Le mode opératoire *cipher feedback* (CFB) est défini comme suit : le chiffrement d'un message $m = m_1 \| \cdots \| m_t$ de longueur $t \times n$ est $c = c_0 \| \cdots \| c_t$ de longueur $(t+1) \times n$ où $c_0 = IV$ est un vecteur d'initialisation et $c_i = m_i \oplus E_k(c_{i-1})$ pour $i = 1$ à t.

1. Donner l'algorithme de déchiffrement. *Un schéma peut aider !*
2. - **i.** Pour obtenir mode opératoire sécurisé, le vecteur d'initialisation doit-il être fixé ou aléatoire ? *Justifier.*
   - **ii.** Comment peut-on chiffrer un message dont la longueur n'est pas un multiple de n ? Proposer une solution explicite pour le chiffrement et le déchiffrement.
3. Soit $m = m_1 \| \cdots \| m_t$ un message et $c_0 \| \cdots \| c_t$ un chiffré correspondant. *On suppose que E_k soit une permutation aléatoire.*
   - **i.** Montrer que si $c_i = c_j$ pour certains $i \neq j$, alors $m_{i+1} \oplus m_{j+1} = c_{i+1} \oplus c_{j+1}$.
   - **ii.** Justifier que les blocs du chiffré $c_0, \ldots, c_t$ sont uniformes dans $\{0,1\}^n$.
   - **iii.** Donner une valeur de t telle que, avec probabilité $\geq \frac{1}{4}$, $c_i = c_j$ pour certains $i \neq j$.
4. Dans le jeu IND-CPA, l'adversaire envoie des paires de messages de même longueur $(m_{i,0}, m_{i,1})$. Le challenger calcule $c_i \leftarrow \mathsf{Enc}_k(m_{i,b})$ où b est soit 0 soit 1. À partir des c_i, l'adversaire calcule $\hat{b}$. Son avantage est $\left|\Pr\left[\hat{b} = 1 \middle| b = 1\right] - \Pr\left[\hat{b} = 1 \middle| b = 0\right]\right|$.
   Décrire un adversaire pour le jeu IND-CPA, lorsque le schéma de chiffrement

est basé sur le mode CFB, qui possède un avantage $\geq \frac{1}{4}$. *Soyez précis dans la description des paires de messages $(m_{i,0}, m_{i,1})$ utilisées dans l'attaque : combien de messages ? de quelle longueur ?*

Exercice 3 (6 points). *Sécurité multi-clé pour les MAC*

La *sécurité EUF-CMA multi-clé* est définie à l'aide du jeu mk-EUF-CMA ci-dessous. La différence avec le jeu standard EUF-CMA est que l'adversaire $\mathcal{A}_{\mathsf{mk}}$ joue contre s challengers $\mathcal{C}_1, \ldots, \mathcal{C}_s$ au lieu d'un seul :

1 Chaque challenger $\mathcal{C}_j$ tire une clé $k_j \twoheadleftarrow \mathcal{K}$ (indépendamment des autres) ;
2 Pour $1 \leq i \leq q$:
3 L'adversaire crée une requête (m_i, ℓ_i), envoyée au challenger $\mathcal{C}_{\ell_i}$;
4 Le challenger $\mathcal{C}_{\ell_i}$ répond avec un tag valide $t_i = \mathsf{Mac}_{k_{\ell_i}}(m_i)$;
5 L'adversaire produit une paire (m, t) avec $m \notin \{m_1, \ldots, m_q\}$.

L'adversaire gagne s'il existe une clé k_j telle que $\mathsf{Vrfy}_{k_j}(m, t) = 1$. L'avantage $\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A}_{\mathsf{mk}})$ d'un adversaire $\mathcal{A}_{\mathsf{mk}}$ est sa probabilité de succès. La fonction d'avantage est

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

où $\mathcal{A}_{q,s,t}$ est un adversaire effectuant q requêtes à s challengers en temps t.

1. Justifier que $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Mac}}(q, t) = \mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(q, 1, t)$ pour tout q et t.

En conséquence, la sécurité mk-EUF-CMA implique la sécurité standard EUF-CMA. Nous allons maintenant montrer la réciproque : les deux sécurités sont équivalentes.

Supposons que l'on dispose d'un adversaire $\mathcal{A}_{\mathsf{mk}}$ qui joue contre des challengers $\mathcal{C}_1, \ldots, \mathcal{C}_s$ dans le jeu mk-EUF-CMA. En utilisant $\mathcal{A}_{\mathsf{mk}}$, nous construisons un adversaire $\mathcal{A}$ jouant contre un challenger $\mathcal{C}$ dans le jeu EUF-CMA : l'adversaire $\mathcal{A}$ simule le jeu mk-EUF-CMA pour $\mathcal{A}_{\mathsf{mk}}$. Il doit en particulier répondre à chacune des requêtes de $\mathcal{A}_{\mathsf{mk}}$. Pour cela, $\mathcal{A}$ *devine* $j \twoheadleftarrow \{1, \ldots, s\}$ et parie que $\mathcal{A}_{\mathsf{mk}}$ renverra une paire valide pour la clé k_j. Il joue alors le rôle de tous les challengers sauf $\mathcal{C}_j$ et utilise son propre challenger $\mathcal{C}$ pour jouer le rôle de $\mathcal{C}_j$. Pour jouer le rôle d'un challenger $\mathcal{C}_\ell$, il tire une clé k_ℓ et répond à chaque requête (m_i, ℓ) en calculant $t_i = \mathsf{Mac}_{k_\ell}(m_i)$. À la fin, $\mathcal{A}$ produit la même paire (m, t) que $\mathcal{A}_{\mathsf{mk}}$.

2. **i.** Comment $\mathcal{A}$ peut-il répondre aux requêtes (m_i, j) ? *Rappel : $\mathcal{A}$ utilise son propre challenger $\mathcal{C}$ pour jouer le rôle de $\mathcal{C}_j$.*
ii. Justifier que si $\mathcal{A}_{\mathsf{mk}}$ produit une paire valide pour la clé k_j, alors $\mathcal{A}$ gagne.
iii. Quelle est la probabilité que $\mathcal{A}$ ait correctement deviné j ?
iv. Exprimer $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A})$ en fonction de $\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(\mathcal{A}_{\mathsf{mk}})$ et de s.

3. En déduire une borne sur l'avantage $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Mac}}(q, t)$ en fonction de $\mathsf{Adv}^{\mathsf{mk\text{-}EUF\text{-}CMA}}_{\mathsf{Mac}}(q, s, t)$ et de s. *Justifier soigneusement la borne.*