Examen partiel – 14 mars 2025

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 (sur 6 pts). *Questions courtes*

1. Quelles sont les deux constructions décrites dans le cours pour construire une fonction de hachage ? *Donner le nom de chaque construction et définir l'objet sur lequel elle est basée. Il ne vous est pas demandé d'expliquer le fonctionnement de la construction.*
2. L'AES est-il un chiffre par blocs ou un système de chiffrement symétrique ?
3. Décrivez la syntaxe d'un MAC et son rôle.
4. Une attaque contre un schéma de chiffrement qui a un avantage p et un temps d'exécution t pose-t-elle un problème en pratique pour les valeurs suivantes de p et t : $p = \frac{1}{2}$ et $t = 2^{128}$; $p = (\frac{1}{2})^{120}$ et $t = 2^{32}$; $p = \frac{1}{2}$ et $t = 2^{32}$?

Exercice 2 (sur 6 pts). *Modes opératoires*

Soit $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ un chiffre par blocs. Nous considérons deux modes opératoires. *Il est fortement recommandé de dessiner les modes opératoires pour répondre aux questions.*

Soit $m = m_1 \| \cdots \| m_\ell$ où $m_1, \ldots, m_\ell \in \{0,1\}^n$, et $c_0 \twoheadleftarrow \{0,1\}^n$ est un IV aléatoire.

1. Soit $\mathsf{Enc}_k^1(m) = c_0 \| c_1 \| \cdots \| c_\ell$ où $c_i = E_k(m_i) \oplus c_{i-1}$ pour $1 \leq i \leq \ell$.
   - **i.** Écrire l'algorithme de déchiffrement $\mathsf{Dec}_k^1(c)$.
   - **ii.** Montrer que ce mode ne permet pas d'obtenir une sécurité IND-CPA, quelle que soit la qualité de E. *Indice. Montrez qu'un adversaire peut vérifier, étant donné le chiffrement de $m = m_1 \| m_2$, si $m_1 = m_2$, et en faire un avantage dans le jeu IND-CPA.*
2. Soit $\mathsf{Enc}_k^2(m) = c_0 \| \cdots \| c_\ell$ où pour $1 \leq i \leq \ell$, $c_i = r_i \oplus m_i$ avec $r_i = E_k(r_{i-1})$ et $r_0 = c_0$.
   - **i.** Écrire l'algorithme de déchiffrement $\mathsf{Dec}_k^2(c)$.

   On remplace E_k par une fonction aléatoire $f : \{0,1\}^n \to \{0,1\}^n$.
   - **ii.** Justifier, intuitivement, qu'un adversaire ne peut obtenir aucune information sur le message d'entrée m à partir du seul chiffré c.

Exercice 3 (sur 10 pts). *Réseaux de Feistel*

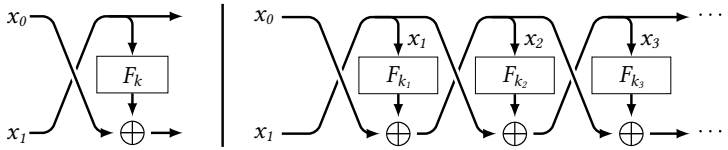

FIGURE 1 – Un tour de Feistel (à gauche) et un réseau de Feistel (à droite) [1]

Un *tour de Feistel* transforme une fonction $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ en un chiffre par blocs $E : \{0,1\}^\kappa \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ de la manière suivante : $E_k(x_0\|x_1) = x_1\|(F_k(x_1) \oplus x_0)$, où $x_0, x_1 \in \{0,1\}^n$, $\|$ désigne la concaténation et $\oplus$ le XOR bit-à-bit.

1. **i.** Montrer que E est un chiffre par blocs, c'est-à-dire que E_k est une permutation pour chaque k. *Indice. Décrire le calcul de* $E_k^{-1}(\cdot)$.

ii. Montrer que E n'est *pas* un chiffre par blocs sûr : un adversaire peut distinguer E_k d'une permutation aléatoire en faisant une seule requête, avec une très bonne probabilité.

Un *réseau de Feistel* à r tours transforme $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ en un chiffre par blocs $E : \{0,1\}^{r\kappa} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ de la manière suivante : soit $k = k_1\|\cdots\|k_r$ la clé de $r\kappa$ bits, $x_0\|x_1$ le message de $2n$ bits, et $x_{\ell+1} = F_{k_\ell}(x_\ell) \oplus x_{\ell-1}$ pour $1 \le \ell \le r$; alors $E_{k_1\|\cdots\|k_r}(x_0\|x_1) = x_r\|x_{r+1}$.
On montre qu'un réseau de Feistel à 3 tours possède une sécurité PRF. **On suppose que chaque F_{k_i} est remplacée par une fonction $f_\ell : \{0,1\}^n \to \{0,1\}^n$ tirée uniformément parmi les fonctions de $\{0,1\}^n$ dans lui-même. Les probabilités dépendent de ces choix aléatoires.**
Soit $\mathcal{A}$ un adversaire qui effectue q requêtes $m^1, \ldots, m^q$ où $m^i = x_0^i\|x_1^i$ pour $1 \le i \le q$, et soit $x_{\ell+1}^i = f_\ell(x_\ell^i) \oplus x_{\ell-1}^i$ pour $\ell = 1$ à 3. On suppose que les requêtes sont distinctes deux-à-deux.

2. **i.** Justifier que les x_2^i sont distincts deux-à-deux, les x_3^i sont indépendants et uniformes. *Indice. Le masque jetable (one-time pad).*

ii. Soit $1 \le i < j \le q$. Montrer que $\Pr\left[x_2^i = x_2^j\right] \le 1/2^n$. *Indice. Considérer deux cas distincts* $x_1^i = x_1^j$ *et* $x_1^i \ne x_1^j$.

iii. En déduire que $\Pr\left[\exists i \ne j, x_2^i = x_2^j\right] \le q(q-1)/2^{n+1}$.

On admet de même que $\Pr\left[\exists i \ne j, x_3^i = x_3^j\right] \le q(q-1)/2^{n+1}$, et que si les x_3^i sont distincts deux-à-deux, les x_4^i sont indépendants et uniformes.

3. Conclure que l'adversaire ne peut pas distinguer $E_{k_1\|k_2\|k_3}$ d'une fonction aléatoire avec probabilité supérieure à $q(q-1)/2^n$.

1. Source : M. Rosulek, *The Joy of Cryptography*, https://joyofcryptography.com.