HAI709I - TD 2

Rocco Mora

15 Septembre, 2025

Exercice 1 :

Dire si les fonctions suivantes sont :

- bornées par un polynôme: $f_1(n) = n, f_2(n) = n^3 - 4n^2 + 2n + 9, f_3(n) = n\log_2(n), f_4(n) = 1.1^n, f_5(n) = 2^{0.5n}, f_6(n) = 2^{\sqrt{n}}, f_7(n) = n^{\log_2(n)}$.
- negligeables: $f_1(n) = \frac{1}{n^2+n+1}, f_2(n) = \frac{3}{\log_2(n)}, f_3(n) = 2^{-n}, f_4(n) = 2^{-0.5n}, f_5(n) = \frac{n^2+n+1}{e^n}, f_6(n) = 2^{-\sqrt{n}}, f_7(n) = n^{-\log_2(n)}$.

Exercice 2 :

Considérons un chiffrement de Vigenère Π où l'espace de messages est constitué de toutes les chaînes de 3 caractères et `Gen` fonctionne de la manière suivante : d'abord, une période t est tirée uniformément au hasard dans $\{2, 3\}$, puis une clé k est tirée uniformément au hasard dans $\{0, \ldots, 25\}^t$.

- Définissez un adversaire $\mathcal{A}$ tel que $\Pr(\texttt{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) > 1/2$.
- Définissez un adversaire $\mathcal{A}$ tel que $\Pr(\texttt{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) \geq 3/4$.

Exercice 3 :

Soit G un PRG avec un facteur d'expansion $\ell(n) > 2n$. Dans chacun des cas suivants, prouver que G' est *aussi* un PRG, si tel est le cas. Sinon, trouver un contre-exemple.

- Définissez $G'(s) \stackrel{\text{def}}{=} G(s_1, \ldots, s_{\lceil n/4 \rceil})$, où $s = s_1, \ldots, s_n$.
- Définissez $G'(s) \stackrel{\text{def}}{=} G(s_1, \ldots, s_{\lceil n/2 \rceil})$, où $s = s_1, \ldots, s_n$.
- Définissez $G'(s) \stackrel{\text{def}}{=} G(s||0^{|s|})$.

Exercice 4 :

Montrez que les fonctions à clé préservant la longueur suivantes ne sont PAS pseudo-aléatoires :

- $\mathcal{K} = \mathcal{M} = \{0,1\}^n$. $F_k(m) \stackrel{\text{def}}{=} k \oplus m$.
- Pour un paramètre de sécurité n, la clé k est donnée par une matrice A de dimension $n \times n$ et un vecteur colonne b, tous deux avec des coefficients dans $\{0,1\}$. Définissons $F_{A,b}(m) \stackrel{\text{def}}{=} Am + b$, où le message $m \in \{0,1\}^n$ est interprété comme un vecteur colonne et toutes les opérations sont effectuées modulo 2.

Exercice 5 :

Soit F une fonction pseudo-aléatoire et G un générateur pseudo-aléatoire avec $\ell(n) = n + 1$. Soit $k \in \{0,1\}^n$ une clé. Indiquez si les schémas de chiffrement suivants sont EAV-sûrs et/ou CPA-sûrs, en expliquant de manière informelle votre réponse :

- Étant donné le texte en clair $m \in \{0,1\}^n$, chiffrez-le sous la forme $(r, G(r) \oplus m)$ où r est choisi uniformément au hasard dans $\{0,1\}^{n-1}$.
- Étant donné le texte en clair $m \in \{0,1\}^n$, chiffrez-le sous la forme $m \oplus F_k(0^n)$.
- Étant donné le texte en clair $m \in \{0,1\}^{2n}$, décomposez $m = m_1||m_2$ avec $|m_1| = |m_2| = n$ et chiffrez-le sous la forme $(r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1))$, où r est choisi uniformément au hasard dans $\{0,1\}^n$.