TD2 - Sécurité inconditionnelle et sécurité calculatoire

Exercice 1. *Vernam et chiffrements multiples*

On s'intéresse au chiffrement de Vernam utilisé pour chiffrer plusieurs messages.

1. Supposons qu'on chiffre deux messages m_1 et m_2 avec une même clef k. Quelle information sur m_1 et m_2 peut-on calculer à partir de leurs chiffrés c_1 et c_2 ?

On cherche maintenant à mettre en œuvre cette technique en pratique. On suppose que les messages sont des caractères ASCII (sur 8 bits). De plus, on *sait* que les caractères chiffrés sont soit des lettres (non accentuées, majuscules ou minuscules) soit le caractère espace. *Le codage ASCII, vu comme un entier sur* 8 *bits, des lettres majuscules est compris entre* 65 *(*`A`*) et* 90 *(*`Z`*), celui des minuscules entre* 97 *(*`a`*) et* 122 *(*`z`*), et l'espace est* 32*.*

2. **i.** Par quel bit peut-on distinguer le caractère espace des lettres ?
   ii. On observe les chiffrés `1011 0111` et `1110 0111`. Que peut-on déduire sur les caractères qui ont été chiffrés ?
   iii. On observe les chiffrés `0110 0110`, `0011 0010` et `0010 0011`. Que peut-on déduire sur les caractères qui ont été chiffrés ?

Exercice 2. *Sécurité inconditionnelle*

Pour chacun des schémas de chiffrements suivants, décrire l'algorithme de déchiffrement Dec, et indiquer si le schéma est *inconditionnellement sûr*.

1. L'espace des messages est $\mathcal{M} = \{0,1,2,3,4\}$, Gen choisit uniformément une clef dans $\mathcal{K} = \{0,1,2,3,4,5\}$ et $\mathsf{Enc}_k(m) = m + k \bmod 5$.
2. L'espace des messages est $\mathcal{M} = \{m \in \{0,1\}^\ell : m_{[\ell-1]} = 0\}$, Gen choisit uniformément une clef dans $\{0,1\}^{\ell-1}$ et $\mathsf{Enc}_k(m) = m \oplus (k\|0)$.

Exercice 3. *Nécessité du chiffrement probabiliste*

On rappelle que l'*EAV-sécurité pour les chiffrements multiples* se base sur l'expérience suivante : l'attaquant produit deux listes de messages, le protocole chiffre l'une des deux listes choisie aléatoirement, et l'attaquant gagne s'il détermine correctement laquelle des deux listes a été chiffrée.
Soit $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ un schéma de chiffrement *déterministe*, c'est-à-dire dans lequel Enc est une fonction déterministe de la clef et du message à chiffrer.

✎ Montrer qu'un attaquant peut gagner avec probabilité 1, en produisant deux listes de longueur 2 bien choisies.

Exercice 4. *Générateurs pseudo-aléatoires*

1. Soit $G(s) = s\|s$ où $\|$ désigne la concaténation. Montrer que G n'est pas un générateur pseudo-aléatoire.
2. **i.** Soit G un générateur pseudo-aléatoire d'expansion $\ell(n)$, et $G^*(s) = G(s_{[0,\lfloor n/2 \rfloor[})$. Calculer le facteur d'expansion $\ell^*(n)$ de G^*, et montrer que c'est un générateur pseudo-aléatoire. *Indication. Montrer que pour tout algorithme* D*,* $\Pr_{s\in\{0,1\}^n}[D(G^*(s)) = 1] = \Pr_{s^*\in\{0,1\}^{\lfloor n/2 \rfloor}}[D(G(s^*)) = 1]$.
   ii. Montrer qu'il existe un générateur pseudo-aléatoire G tel que $G'(s) = G(0^{|s|}\|s)$ n'est pas pseudo-aléatoire. *Indication. Considérer un générateur pseudo-aléatoire* H*, le générateur* H^* *comme dans la question précédente, et* $H^*(0^{|s|}\|s)$.