Théorème de Shannon

Le but de cet exercice est de prouver le résultat suivant de Shannon.

Theorem 1. *Soit* $\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}$ *un chiffrement symétrique tel que* $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$*. Le schéma est parfaitement sûr si et seulement si :*

1. *Toute clé* $k \in \mathcal{K}$ *est choisie avec probabilité* $1/|\mathcal{K}|$ *par* KeyGen
2. *Pour tout* $m \in \mathcal{M}$ *et tout* $c \in \mathcal{C}$*, il existe une unique clé* $k \in \mathcal{K}$ *telle que* $\mathsf{Enc}(m, k) = c$*.*

D'abord, nous justifions que l'hypothèse faite sur les espaces est raisonnable.

Question 1. *On rappelle la définition de la sécurité parfaite : pour toute variable aléatoire* M*,* m *et* c *:*

$$\Pr[M = m | \mathsf{Enc}(\mathsf{KeyGen}, M) = c] = \Pr[M = m] \ .$$

Montrer que si le chiffrement est correct, on a $|\mathcal{C}| \geq |\mathcal{M}|$ *; et que si le chiffrement est parfaitement sûr, on a* $|\mathcal{K}| \geq |\mathcal{C}|$*.*

On va utiliser la définition suivante de la sécurité parfaite :

> Un chiffrement symétrique est parfaitement sûr si, pour tous $m_1, m_2, c \in \mathcal{M} \times \mathcal{M} \times \mathcal{C}$:
>
> $$\Pr_{k \leftarrow \mathsf{KeyGen}}[\mathsf{Enc}(k, m_1) = c] = \Pr_{k \leftarrow \mathsf{KeyGen}}[\mathsf{Enc}(k, m_2) = c] \ . \tag{1}$$

Question 2. *Montrer l'équivalence avec l'autre définition.*

Question 3. *Montrer que les conditions 1. et 2. sont suffisantes pour la sécurité parfaite.*

Question 4. *Montrer le sens inverse de la preuve.*

Distance Statistique

On rappelle que la distance statistique entre deux variables aléatoires discrètes sur un espace dénombrable A est définie par :

$$\Delta(X, Y) = \frac{1}{2} \sum_{a \in A} |\Pr[X = a] - \Pr[Y = a]| \ .$$

Question 5. *Soit* X *et* Y *deux variables aléatoires discrètes sur un ensemble dénombrable* A*, et soit* Z *une troisième variable sur un ensemble* B *(possiblement différent). Montrer que si* Z *est indépendante de* X *et* Y*, alors* $\Delta((X, Z), (Y, Z)) = \Delta(X, Y)$*.*

Question 6. *Soit* $(X_1, \ldots, X_k)$ *et* $(Y_1, \ldots, Y_k)$ *deux listes de variables aléatoires totalement indépendantes. Montrer que :*

$$\Delta((X_i)_i, (Y_i)_i) \leq \sum_{i=1}^{k} \Delta(X_i, Y_i) \ . \tag{2}$$

Question 7. *Soit* X *et* Y *deux variables aléatoires à valeurs dans un ensemble* A*. Montrer que pour toute fonction (potentiellement randomisée)* f *de domaine* A*,* $\Delta(f(X), f(Y)) \leq \Delta(X, Y)$*.*

Question 8. *En déduire que l'avantage de tout adversaire* $\mathcal{A}$ *pour distinguer entre* X *et* Y en une requête *est inférieur à* $\Delta(X, Y)$*.*

Question 9. *Montrer que si* $\Delta(X, Y) = \mathrm{negl}(n)$*, les distributions* X *et* Y *sont calculatoirement indistinguables.*

Chiffrement de Vigenère

Le chiffrement de Vigenère sur un alphabet fini strictement ordonné Σ est une version relaxée et généralisée du OTP, où la clé peut être plus petite que les messages considérés, et on utilise l'addition modulaire au lieu du XOR (qui est l'addition modulo 2). Pour chiffrer / déchiffrer, on répète la clé ($abc \to abcabcabc\ldots$) pour obtenir une clé aussi longue que le message / chiffré, et on ajoute (modulairement) la clé au message / chiffré, caractère par caractère.

Question 10. *Définir formellement le schéma.*

Nous considérons le jeu de sécurité suivant sur un schéma de chiffrement Π avec un adversaire $\mathcal{A}$, noté G^{EAV}.

1. $\mathcal{A}$ choisit deux messages m_0, m_1 de $\mathcal{P}$
2. La clé k est générée par KeyGen, un bit $b \hookleftarrow U(0,1)$ est choisi
3. $c = \mathsf{Enc}(m_b, k)$ est donné à $\mathcal{A}$
4. $\mathcal{A}$ renvoie un bit b'

La sortie du jeu, notée $G^{EAV}(\mathcal{A}, n)$ est $\top$ si $b = b'$ et $\bot$ sinon. On peut donc remarquer que $G^{EAV}(\mathcal{A}, n)$ est une variable aléatoire à valeurs dans $\{\top, \bot\}$.

Formellement :

Definition 1 (Sécurité EAV)**.** Un schéma de chiffrement symétrique est EAV (*secure against eavesdropping*) si pour tout adversaire PPT $\mathcal{A}$ son avantage $\mathrm{Adv}^{EAV}(\mathcal{A}) = |\Pr\left[G^{EAV}(\mathcal{A}, n) \leftarrow \top\right] - 1/2|$ est négligeable en n. Le jeu de sécurité est donné par :

1. $(m_0, m_1) \in \mathcal{M}^2 \leftarrow \mathcal{A}(1^n)$
2. $k \leftarrow \mathsf{KeyGen}(1^n)$, $b \hookleftarrow U(0,1)$
3. $b' \leftarrow \mathcal{A}(\mathsf{Enc}(k, m_b))$
4. Si $b = b'$ alors $\top$ sinon $\bot$

Dans la suite, le chiffrement de Vigenère est noté Π, et l'alphabet latin Σ.

Question 11. *Montrer qu'un adversaire $\mathcal{A}$ participant au jeu EAV peut retrouver la clé k.*

Question 12. *Montrer que le chiffrement de Vigenère n'est pas EAV-sûr.*