Exercice 1 (Chiffrement parfait)

Soit $\Gamma = \langle \mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C} \rangle$ un cryptosystème. On rappelle que :

— $\mathcal{K}$ est l'ensemble des clés (il est fini)
— $\mathcal{M}$ est l'ensemble des messages en clair (il est fini)
— $\mathcal{C}$ est l'ensemble des cryptogrammes ; il a le même nombre d'éléments que $\mathcal{M}$
— Enc est une application de $\mathcal{K} \times \mathcal{M}$ dans $\mathcal{C}$.
— Dec est une application de $\mathcal{K} \times \mathcal{C}$ dans $\mathcal{M}$.

On se donne un espace probabilisé $\langle \Omega, \mathcal{P}(\Omega), \Pr \rangle$ et deux variables aléatoires indépendantes :

$$K : \Omega \to \mathcal{K}, \quad M : \Omega \to \mathcal{M}.$$

La loi de K est uniforme i.e.

$$\forall E \subseteq \mathcal{K}, \quad \Pr(\{\omega \in \Omega \mid K(\omega) \in E\}) = \frac{\#(E)}{\#(\mathcal{K})}.$$

On suppose que, pour tous $k \in \mathcal{K}, m \in \mathcal{M}$:

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m. \tag{1}$$

On rappelle que Γ a la propriété d'*indiscernabilité parfaite*[1] ssi pour tous $m, m' \in \mathcal{M}, c \in \mathcal{C}$,

$$\Pr(\mathsf{Enc}(K(\omega), m) = c) = \Pr(\mathsf{Enc}(K(\omega), m') = c) \tag{2}$$

Exemple 1(système de Vernam) :

$$\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^5, \quad \mathsf{Enc}(k, m) = k \oplus m, \quad \mathsf{Dec}(k, m) = k \oplus m$$

où l'opération $\oplus$ est le ou exclusif sur chaque composante : si $k = k[0]k[1]\dots k[4]$ et $m = m[0]m[1]\dots m[4]$ alors

$$k \oplus m := (k[0] \oplus m[0]) \cdot (k[1] \oplus m[1]) \cdots (k[4] \oplus m[4])$$

Exemple 2 (système de Vigenère) :

$$\mathcal{K} = \{0,1\}^5, \mathcal{M} = \mathcal{C} = \{0,1\}^{10}, \quad \mathsf{Enc}(k, m) = (k \cdot k) \oplus m, \quad \mathsf{Dec}(k, m) = (k \cdot k) \oplus m$$

Exemple 3 (Permutation des positions, messages de longueur 15) :

$$\mathcal{K} = \mathcal{S}_5, \mathcal{M} = \mathcal{C} = \{0,1\}^{15}$$

Chaque élément de $\mathcal{S}_5$ est une permutation des entiers de $[0,4]$ donnée par la suite de ses images. Par exemple $\sigma = (3,0,4,1,2)$ dénote la permutation $(0 \mapsto 3, 1 \mapsto 0, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 2)$. Chaque message m peut être décomposé en 3 messages de longueur 5 :

$$m = f_0 \cdot f_1 \cdot f_2$$

1. ce que nous désignerons par "parfait" dans la suite

On pose alors

$$\mathsf{Enc}(\sigma, m) := (f_0 \circ \sigma) \cdot (f_1 \circ \sigma) \cdot (f_2 \circ \sigma).$$

Par exemple,

$$\mathsf{Enc}(((3,0,4,1,2), 110101100000111) = 11010 \cdot 01010 \cdot 10101$$

1- Pour chacun des exemples ci-dessus, déterminer si le cryptosystème est parfait.

Étant donnée une application à deux arguments

$$f : A \times B \to C$$

nous noterons pour tous $a \in A, b \in B$, $\quad f(*, b) : A \to C$ et $\quad f(a, *) : B \to C$ les applications partielles :

$$f(*, b) : x \mapsto f(x, b), \quad f(a, *) : x \mapsto f(a, x).$$

2- Montrer que l'égalité (1) entraine que, pour toute clé $k \in \mathcal{K}$, l'application $\mathsf{Enc}(k, *)$ est injective.
3- En déduire que, pour toute clé $k \in \mathcal{K}$, l'application $\mathsf{Enc}(k, *)$ est une bijection de $\mathcal{M}$ dans $\mathcal{C}$.
4- Montrer que, pour tout cryptosystème vérifiant les hypothèses de l'énoncé (i.e. jusqu'à l'équation (1) comprise), et tous $k \in \mathcal{K}, c \in \mathcal{C}$:

$$\mathsf{Enc}(k, \mathsf{Dec}(k, c)) = c.$$

Aide : On pourra montrer que les deux applications $\mathsf{Enc}(k, *)$ et $\mathsf{Dec}(k, *)$ sont réciproques l'une de l'autre.
Une application $f : A \to B$ est dite *équilibrée* ssi

$$\forall b, b' \in B, \#(f^{-1}(b)) = \#(f^{-1}(b')). \tag{3}$$

5- Montrer que, si Γ est parfait, alors pour tout $c \in \mathcal{C}$, $\mathsf{Dec}(*, c)$ est équilibrée.
6- Montrer que, si pour tout $c \in \mathcal{C}$, $\mathsf{Dec}(*, c)$ est équilibrée, alors Γ est parfait.
7- Montrer que, si Γ est parfait, alors $\#(\mathcal{M})$ divise $\#(\mathcal{K})$.
Exemple 4 : (Permutation des positions, messages de longueur 5) :

$$\mathcal{K} = \mathcal{S}_5, \mathcal{M} = \mathcal{C} = \{0,1\}^5, \quad \mathsf{Enc}(\sigma, m) := m \circ \sigma.$$

8- Le cryptosystème de l'exemple 4 est-il parfait ?

Exercice 2 (double-DES)

Il a été suggéré d'augmenter la sécurité du DES en appliquant deux fois la fonction de chiffrement du DES avec deux clés différentes. On note n la taille des clés, ℓ la taille des messages, et $\mathsf{DES}_k : \mathbb{B}^\ell \to \mathbb{B}^\ell$ la fonction de chiffrement par bloc du DES avec la clé k (ici $\mathbb{B} := \{0,1\}$).
Le cryptosystème est donc de la forme :

$$\Gamma = \langle \mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C} \rangle$$

où

$$\mathcal{K} = \mathbb{B}^n \times \mathbb{B}^n, \mathcal{M} = \mathbb{B}^\ell, \mathcal{C} = \mathbb{B}^\ell, \mathsf{Enc}(k_1, k_2, m) = \mathsf{DES}_{k_2}(\mathsf{DES}_{k_1}(m)).$$

1- Vérifier que, pour tout $k \in \mathbb{B}^n$, DES_k est une bijection de $\mathcal{M}$ dans $\mathcal{C}$.
2- Exprimer $\mathsf{Dec}(k_1, k_2, c)$ en fonction de $\mathsf{DES}_{k_1}, \mathsf{DES}_{k_2}$ de facon que Γ soit bien un cryptosystème.

Un attaquant intercepte des couples clairs/textes chiffrés $\{(x_1, y_1), \ldots, (x_a, y_a)\}$ obtenus avec la même clé (k_1, k_2), c'est-à-dire que

$$\forall i \in [1, a],\ y_i = \mathsf{Enc}(k_1, k_2, x_i).$$

On cherche à déterminer la clé à partir de ces données.
3- Montrer que $\forall i \in [1, a], DES_{k_1}(x_i) = DES_{k_2}^{-1}(y_i)$.
On modélise les clés par deux variables aléatoires $K_1, K_2 : \Omega \to \mathbb{B}^n$ indépendantes et de loi uniforme i.e. pour tout $E \subseteq \mathcal{K}$

$$\Pr(\{\omega \in \Omega \mid (K_1(\omega), K_2(\omega)) \in E\}) = \frac{\#(E)}{\#(\mathcal{K})}.$$

On note aussi $\Pr_{\mathcal{S}}$ la loi de probabilité uniforme sur $\mathcal{S}_{\mathbb{B}^\ell} \times \mathcal{S}_{\mathbb{B}^\ell}$.
On note $\varphi : \mathbb{B}^n \times \mathbb{B}^n \to \mathcal{S}_{\mathbb{B}^\ell} \times \mathcal{S}_{\mathbb{B}^\ell}$ l'application définie par : $\varphi(k_1, k_2) = (\mathsf{DES}_{k_1}, \mathsf{DES}_{k_2})$.
On fait deux hypothèses :
(H1) $\forall A \subseteq \mathcal{S}_{\mathbb{B}^\ell} \times \mathcal{S}_{\mathbb{B}^\ell}, \Pr(\{\omega \in \Omega \mid (K_1(\omega), K_2(\omega)) \in \varphi^{-1}(A)) = \Pr_{\mathcal{S}}(A)$
(H2) Les événements $EG_i := \{\omega \in \Omega \mid \mathsf{DES}_{K_1(\omega)}(x_i) = \mathsf{DES}_{K_2(\omega)}^{-1}(y_i)\}$ sont indépendants dans leur ensemble.
4- Evaluer $\Pr(EG_i)$.
5- Evaluer $\Pr(\bigcap_{i=1}^a EG_i)$.
6- En déduire que

$$\#\{(k_1, k_2) \in \mathcal{K} \times \mathcal{K} \mid \forall i \in [1, a], \mathsf{DES}_{k_1}(x_i) = \mathsf{DES}_{k_2}^{-1}(y_i)\} \sim 2^{2n - a\ell}.$$

On suppose maintenant que $a \geq \frac{2n}{\ell}$.
I1 : On calcule les $2a$ listes

$$L_i = (k, \mathsf{DES}_k(x_i))_{k \in \mathbb{B}^n}, L'_i = (k, \mathsf{DES}_k^{-1}(y_i))_{k \in \mathbb{B}^n}.$$

I2 : On les trie suivant leur seconde composante $\mathsf{DES}_k(x_i)$ (resp. $\mathsf{DES}_k^{-1}(y_i)$).
7- Compléter ces deux calculs en un algorithme qui calcule la liste des clés (k_1, k_2) telles que

$$\forall i \in [1, a], \mathsf{DES}_{k_1}(x_i) = \mathsf{DES}_{k_2}^{-1}(y_i).$$

8- Évaluez la complexité en temps et en espace de votre attaque (on supposera que, pour tout x, la fonction $k \mapsto \mathsf{DES}_k(x)$ est équilibrée, au sens de l'exercice 1, definition (3)).
9- Le protocole double DES utilise les paramètres $n = 56, \ell = 64$. Que peut-on dire sur la sécurité de double DES ?