Exercice 1 (Chiffrement parfait : une solution)

Q1- Exemple 1(système de Vernam) :
Ce système est parfait (vu en TD)

Exemple 2 (système de Vigenère) :
Comme le nombre de clés est strictement inférieur au nombre de messages, d'après le théorème de Shannon, ce système n'est pas parfait.
Exemple 3 (Permutation des positions, messages de longueur 15) :
$\#(\mathcal{K}) = 5! = 120$ et $\#(\mathcal{M}) = 2^{15}$. Comme $120 < 128 = 2^7 < 2^{15}$ d'après le théorème de Shannon, ce système n'est pas parfait.
Q2 , Q3, Q4- Soit k une clé. La condition (1) exprime que :

$$\mathsf{Dec}(k, *) \circ \mathsf{Enc}(k, *) = \mathrm{Id}_{\mathcal{M}}. \tag{1}$$

L'application $\mathsf{Enc}(k, *)$ est donc injective.
Comme les ensembles $\mathcal{M}$ et $\mathcal{C}$ sont finis et ont même cardinalité, toute injection de $\mathcal{M}$ dans $\mathcal{C}$ est une bijection. Donc $\mathsf{Enc}(k, *)$ est une bijection. En composant les deux membres de (1). à droite, par l'application $\mathsf{Enc}(k, *)^{-1}$ (la réciproque de $\mathsf{Enc}(k, *)$), on obtient :

$$\mathsf{Dec}(k, *) = \mathsf{Enc}(k, *)^{-1}. \tag{2}$$

autrement dit : les applications $\mathsf{Enc}(k, *), \mathsf{Dec}(k, *)$ sont réciproques l'une de l'autre. On a donc aussi :

$$\mathsf{Enc}(k, *) \circ \mathsf{Dec}(k, *) = \mathrm{Id}_{\mathcal{C}}.$$

c'est à dire que, pour tous $k \in \mathcal{K}, c \in \mathcal{C}$:

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

Q5- Supposons que Γ est parfait. Soient $m, m' \in \mathcal{M}, c \in \mathcal{C}$.
Par définition de la propriété d'*indiscernabilité parfaite* : (**??**) est vraie. Comme la loi de K est uniforme, cette égalité revient à

$$\#\{k \in \mathcal{K} \mid \mathsf{Enc}(k, m) = c\} = \#\{k \in \mathcal{K} \mid \mathsf{Enc}(k, m') = c\}$$

Par Q4, on sait que $\mathsf{Enc}(k, m) = c$ ssi $\mathsf{Dec}(k, c) = m$. L'égalité ci-dessus revient donc à

$$\#\{k \in \mathcal{K} \mid \mathsf{Dec}(k, c) = m\} = \#\{k \in \mathcal{K} \mid \mathsf{Dec}(k, c) = m'\}$$

c'est à dire que l'application $\mathsf{Dec}(*, c)$ est équilibrée.
Q6- Supposons que $\mathsf{Dec}(*, c)$ est équilibrée. Soient $m, m' \in \mathcal{M}, c \in \mathcal{C}$.
l'image réciproque de m et de m' par $\mathsf{Dec}(*, c)$ ont donc même cardinalité :

$$\#\{k \in \mathcal{K} \mid \mathsf{Dec}(k, c) = m\} = \#\{k \in \mathcal{K} \mid \mathsf{Dec}(k, c) = m'\}$$

et comme $\mathsf{Dec}(k,*), \mathsf{Enc}(k,*)$ sont réciproques l'une de l'autre, cela revient à

$$\#\{k \in \mathcal{K} \mid \mathsf{Enc}(k,m) = c\} = \#\{k \in \mathcal{K} \mid \mathsf{Enc}(k,m') = c\}$$

et comme la loi de K est uniforme, cela entraine que (**??**) est vraie.
Q7- Supposons que Γ est parfait. Fixons un élément $c \in \mathcal{C}$ quelconque. On a :

$$\#(\mathcal{K}) = \sum_{m \in \mathcal{M}} \#\{k \in \mathcal{K} \mid \mathsf{Dec}(k,c) = m\} \tag{3}$$

Par Q5, $\mathsf{Dec}(*,c)$ est équilibrée, donc il existe un entier $\alpha \in \mathbb{N}$ tel que

$$\forall m \in \mathcal{M}, \#\{k \in \mathcal{K} \mid \mathsf{Dec}(k,c) = m\} = \alpha. \tag{4}$$

L'égalité (3) s'écrit donc

$$\#(\mathcal{K}) = \#(\mathcal{M}) \cdot \alpha.$$

Donc $\#(\mathcal{M})$ divise $\#(\mathcal{K})$.
Q8- Dans ce cryptosystème : $\#(\mathcal{K}) = 5! = 120, \quad \#(\mathcal{M}) = 2^5 = 32$. Or 32 ne divise pas 120. Le cryptosystème ne vérifie pas la condition nécessaire de perfection prouvée en Q8, donc il n'est pas parfait.

Exercice 2 (double-DES : une solution)

Q1- Pour tout $k \in \mathbb{B}^n$, DES_k est une injection de $\mathcal{M}$ dans $\mathcal{C}$. Comme $\mathcal{M}$ et $\mathcal{C}$ sont finis et de même cardinal, DES_k est une bijection de $\mathcal{M}$ dans $\mathcal{C}$.
Q2- On choisit $\mathsf{Dec}(k_1,k_2,c) := \mathsf{DES}_{k_1}^{-1} \circ \mathsf{DES}_{k_2}^{-1}$.

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

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

Q3- On suppose que :

$$y_i = \mathsf{Enc}(k_1,k_2,x_i),$$

donc

$$y_i = \mathsf{DES}_{k_2}(\mathsf{DES}_{k_1}(x_i)),$$

donc

$$\mathsf{DES}_{k_2}^{-1}(y_i) = \mathsf{DES}_{k_1}(x_i).$$

On fait deux hypothèses :
(H1) $\forall A \subseteq \mathrm{Im}(\varphi), \Pr(\varphi^{-1}(A)) = \Pr_{\mathcal{S}}(A)$
(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.
Q4- Définissons les parties $S_i \subseteq \mathcal{S}_{\mathbb{B}^\ell} \times \mathcal{S}_{\mathbb{B}^\ell}$ par

$$S_i := \{(\varphi_1,\varphi_2) \in \mathcal{S}_{\mathbb{B}^\ell} \times \mathcal{S}_{\mathbb{B}^\ell} \mid \varphi_1(x_i) = \varphi_2^{-1}(y_i)\}.$$

Évaluons le cardinal de chaque S_i.

$$\#S_i = \sum_{v \in \mathbb{B}^\ell} \#\{\varphi_1 \in \mathcal{S}_{\mathbb{B}^\ell} \mid \varphi_1(x_i) = v\} \cdot \#\{\varphi_2 \in \mathcal{S}_{\mathbb{B}^\ell} \mid \varphi_2^{-1}(y_i) = v\}.$$

Le nombre de permutations de $[1, m]$ qui envoient un entier x sur un entier v est égal au nombre de bijections de $[1, m] \setminus \{x\}$ dans $[1, m] \setminus \{v\}$, c'est à dire $(m-1)!$.
Comme $\mathbb{B}^\ell$ est en bijection avec $[1, 2^\ell]$, en appliquant le dénombrement précédent on obtient que :

$$\#\{\varphi_1 \in \mathcal{S}_{\mathbb{B}^\ell} \mid \varphi_1(x_i) = v\} = (2^\ell - 1)!$$

$$\#\{\varphi_2 \in \mathcal{S}_{\mathbb{B}^\ell} \mid \varphi_2^{-1}(y_i) = v\} = \#\{\varphi_2 \in \mathcal{S}_{\mathbb{B}^\ell} \mid \varphi_2(v) = y_i\} = (2^\ell - 1)!.$$

On conclut que

$$\begin{aligned} \#S_i &= \sum_{v \in \mathbb{B}^\ell} (2^\ell - 1)! \cdot (2^\ell - 1)! \\ &= 2^\ell \cdot ((2^\ell - 1)!)^2. \end{aligned}$$

Comme $\Pr_{\mathcal{S}}$ est la mesure de probabilité uniforme,

$$\begin{aligned} \Pr_{\mathcal{S}}(S_i) &= \frac{\#S_i}{\#\mathcal{S}_{\mathbb{B}^\ell} \times \#\mathcal{S}_{\mathbb{B}^\ell}} \\ &= \frac{2^\ell \cdot ((2^\ell - 1)!)^2}{((2^\ell)!)^2} \\ &= \frac{1}{2^\ell} \end{aligned}$$

Comme $EG_i = \{\omega \in \Omega \mid (K_1(\omega), K_2(\omega)) \in \varphi^{-1}(S_i))$ l'hypothèse (H1) permet de conclure que

$$\Pr(EG_i) = \frac{1}{2^\ell}.$$

Q5- Par l'hypothèse (H2) $\Pr(\bigcap_{i=1}^a EG_i) = \prod_{i=1}^a \Pr(EG_i)$, donc $\Pr(\bigcap_{i=1}^a EG_i) = \prod_{i=1}^a \frac{1}{2^\ell} = \frac{1}{2^{a\ell}}$.
Q6- Une reformulation de Q5 est que

$$\Pr(\{\omega \in \Omega \mid \forall i \in [1, a], \mathsf{DES}_{K_1(\omega)}(x_i) = \mathsf{DES}^{-1}_{K_2(\omega)}(y_i)\}) = \frac{1}{2^{a\ell}}.$$

Comme la loi de (K_1, K_2) est uniforme, on en déduit que

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

comme $\#(\mathcal{K} \times \mathcal{K}) = 2^{2n}$ on obtient :

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

En fait, les hypothèses (H1,H2) ne peuvent être rigoureusement vraies, c'est pourquoi nous concluons que

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

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. $\mathsf{DES}_k^{-1}(y_i)$).
Q7- Complétons ces deux calculs.
On stocke dans `L2cle` les couples (clé, liste de clés) : $[k, [...k'...]]$, tels que $\mathsf{DES}_k(x_i) = \mathsf{DES}_{k'}^{-1}(y_i)$. La boucle 1 traite l'indice $i = 1$. La boucle 2 selectionne dans la liste des k' associés à k, ceux qui sont compatibles avec l'indice $i \geq 2$ courant :
- la boucle 3 enumère les k
- la boucle 4 enumère les k'

```
L2cle=[]
#loop 1
for k in B^n:
    lkp=[]
    v= DES(k,x1)
    #recherche dichotomique de v dans la liste L'_1
    forall kp such that DES^{-1}(kp,y_i)==v:
        lkp+=[kp]
    L2cle += [k,lkp]
#loop 2
for i in range(2,a+1):
    NL2cle=[]
    #loop 3
    for l2cle in L2cle:
        k = l2cle[0]
        lkp=l2cle[1]
        #loop4
        for kp in lkp:
            nl2cle=[]
            if DES( kp,DES(k,x_i))==y_i:
            nl2cle+=[kp]
        NL2cle+=[[k,nl2cle]]
    L2cle=NL2cle
 return L2cle
```

Q8- Évaluons la complexité en temps :
I1, I2 : $O(n2^n)$.
Chaque liste est calculée en temps $O(2^n)$ puis triée en temps $O(n2^n)$.
Boucle 1 : $O(2^n \cdot n)$.
Il y a 2^n valeurs de k et, pour chacune, la recherche dichotomique prend un temps $O(n)$: en effet la longueur de la liste L'_1 est 2^n et l'hypothèse d'équilibre de $\mathsf{DES}(*, m)$ entraine que l'ensemble des k' tels que $\mathsf{DES}(k', DES(k, x_i)) = y_i$ est de cardinal proche de $2^\ell/2^n < 1$ c'est à dire, souvent vide, et de petite taille losqu'il n'est pas vide.

Boucle 4 : O(1).
D'après l'hypothèse d'équilibre de $\mathsf{DES}(*, m)$.
Boucle 3 : $O(2^n)$.
La longueur de `L2cle` est 2^n.
Boucle 2 : $O(\frac{n \cdot 2^n}{\ell})$.
Elle exécute $(a-1)$ fois la boucle 3 et $a = 2n/\ell$.
Temps de l'algorithme :$O(n2^n \frac{n \cdot 2^n}{\ell} + 2^n) = O(n2^n)$.
Somme des temps de I1, I2, Boucle 1 et Boucle 2.
Espace de l'algorithme : $O(\frac{n \cdot 2^n}{\ell})$.
On stocke 2a listes de longueur 2^n.
Q9- Le protocole double DES utilise les paramètres $n = 56, \ell = 64$. Nous avons exhibé une attaque de complexité en temps $O(n2^n)$ c'est à dire $O(56 \cdot 2^{56})$. Cette complexité est seulement 50 fois celle d'une attaque force-brute du simple DES. Le double DES n'est donc pas beaucoup plus sûr que le simple DES (sauf s'il existe une attaque plus subtile du simple DES que par essai exhaustif de toutes les clés). Il exige seulement d'intercepter 2 couples (message en clair, message crypté).