

Feuille d'exercices n° 1

Cryptographie classique et rappels divers

Exercice 1 (chiffrement double : l'attaque *meet-in-the-middle*). On cherche à améliorer un système de chiffrement $(f_k)_{k \in \mathcal{K}}$ dont les clés trop courtes n'interdisent pas la recherche exhaustive, en chiffrant deux fois de suite :

$$M \mapsto C = f_{K_2}(f_{K_1}(M))$$

On double donc la longueur de la clé secrète. On considère l'attaque à clair connu suivante. Oscar connaît M et $C = f_{K_2}(f_{K_1}(M))$ et cherche K_1 et K_2 . Il crée deux listes

$$\mathcal{L}_M = (f_K(M))_{K \in \mathcal{K}} \quad \mathcal{L}_C = (f_K^{-1}(C))_{K \in \mathcal{K}}.$$

1. En quoi la découverte d'un élément commun à ces deux listes permet-elle de trouver le couple (K_1, K_2) cherché ?
2. Vérifier que le nombre de comparaisons nécessaires pour trouver un élément commun aux deux listes est de l'ordre de

$$\#\mathcal{K} \log \#\mathcal{K}.$$

(Penser à ranger les listes par ordre alphabétique).

3. Conclure.

Exercice 2 (secret parfait). On considère un système de cryptographie à clé secrète, à espace de messages clairs \mathcal{M} , espaces de messages chiffrés \mathcal{C} , et espace de clés \mathcal{K} . On attribue à chaque message $M \in \mathcal{M}$ une probabilité d'émission $p_M > 0$ et à chaque clé K une probabilité d'utilisation $q_K > 0$.

1. Exprimer la probabilité de réception r_C d'un message chiffré C .

On suppose que chaque message chiffré a une probabilité > 0 d'être obtenu. On dit que le système est à secret parfait si, pour tout message chiffré $C \in \mathcal{C}$, la distribution de probabilité des messages $M \in \mathcal{M}$ conditionnellement à la réception de C est identique à la distribution d'origine $\{p_M, M \in \mathcal{M}\}$.

2. Montrer que, dans tout système cryptographique, on a $\#\mathcal{M} \leq \#\mathcal{C}$. Montrer que si le système cryptographique est à secret parfait, alors $\#\mathcal{C} \leq \#\mathcal{K}$. Vérifier que la propriété de secret parfait ne dépend pas de la distribution $\{p_M, M \in \mathcal{M}\}$.
3. Expliquer sur ces exemples en quoi la non perfection du secret permet l'attaque par analyse des fréquences :
 - (a) $K = \pi$ est une permutation des lettres de l'alphabet, et $C = \pi(M)$ est obtenu en appliquant la permutation π à chaque lettre qui compose le message M .
 - (b) *Le filtre de Vigenère.* K est une suite de k lettres. Elles sont inscrites répétitivement sous le message M , dont tous les espace ont été retirés, puis on calcule C en additionnant les deux lignes, lettre à lettre.
4. *Le système de Vernam, ou chiffrement à clé jetable.* Si M est un message de n bits, $M \in \{0, 1\}^n$, une clef K est un autre élément de $\{0, 1\}^n$. Le message chiffré C est obtenu comme la somme lettre à lettre $C = M + K \pmod 2$.
 - (a) Montrer que le chiffrement de Vernam a la propriété suivante : pour tout message chiffré $C \in \mathcal{C}$ et pour tout message clair $M \in \mathcal{M}$, il existe une clé K qui encode M en C .
 - (b) Montrer que si les clés sont choisies suivant une distribution uniforme, le chiffrement de Vernam est à secret parfait au sens précédent.

Exercice 3 (partage de secret : schéma à seuil). On décrit une méthode pour partager un secret entre n personnes, pour que le secret puisse être reconstitué par k quelconques d'entre elles, mais inaccessible à $k - 1$ d'entre elles.

1. Montrer qu'il existe n nombres premiers m_1, m_2, \dots, m_n tels que

$$(a) \ m_1 < m_2 < \dots < m_n, \quad (b) \ m_1 \dots m_k > m_n \dots m_{n-k+2}.$$

On pourra choisir les m_i dans un intervalle de la forme

$$]x^{\frac{k^2-1}{k^2}}, x]$$

où x est un nombre suffisamment grand pour que l'intervalle contienne n nombre premiers. On utilisera un théorème de répartition des nombres premiers pour obtenir l'existence d'un tel x .

On définit $M = m_1 \dots m_k$ et $N = m_n \dots m_{n-k+2}$, et on code le secret par un nombre s tel que $N \leq s \leq M$. On distribue à chaque personne P_i le nombre I_i tel que

$$0 \leq I_i \leq m_i - 1 \quad \text{et} \quad I_i \equiv s \pmod{m_i}.$$

2. Vérifier que la donnée de k des I_i permet de reconstituer s (appliquer le théorème chinois et le fait que $s \leq M$).
3. Montrer que la connaissance de $k - 1$ des I_i détermine s modulo un nombre inférieur à N , ce qui laisse au moins $\frac{M-N}{N}$ valeurs possibles pour s .

Exercice 4 (complexité de l'algorithme d'Euclide). On rappelle que l'algorithme d'Euclide peut être présenté par la fonction $\text{euclide}(\cdot, \cdot)$ définie ainsi :

$$\text{euclide}(a, b) = \begin{cases} a, & \text{si } b = 0, \\ \text{euclide}(b, r), & \text{si } b \neq 0, \text{ et où } a = bq + r \text{ avec } 0 \leq r < b. \end{cases}$$

On appelle *nombre d'étapes* dans l'exécution de l'algorithme le nombre d'appels *récurifs* de la fonction $\text{euclide}(\cdot, \cdot)$. Par exemple, $\text{euclide}(a, 0)$ s'effectue en 0 étape.

On définit la suite de Fibanocci $(F_n)_{n \geq 0}$ par la relation de récurrence suivante :

$$F_0 = 0, \quad F_1 = 1, \quad \forall n \geq 0, \quad F_{n+2} = F_n + F_{n+1}.$$

1. Montrer par récurrence sur $k \geq 0$: si a et b sont deux entiers positifs avec $a > 0$ et $a \geq b$ et si $\text{euclide}(a, b)$ s'effectue en k étapes, alors $a \geq F_{k+1}$ et $b \geq F_k$.
2. En déduire que pour tout entier $k \geq 1$ et pour tous entiers $a, b \geq 0$ avec $a \geq b$, si $b < F_k$ alors $\text{euclide}(a, b)$ s'effectue en au plus k étapes.
3. Montrer par récurrence sur $k \geq 0$ que $\text{euclide}(F_{k+1}, F_k)$ s'effectue en exactement k étapes.
4. Montrer que le nombre d'étapes pour effectuer $\text{euclide}(a, b)$ est $O(\log b)$, c'est-à-dire qu'il existe une constante $C > 0$ telle que, si $N(a, b)$ désigne le nombre d'étapes dans l'évaluation de la fonction $\text{euclide}(a, b)$, on a :

$$N(a, b) \leq C \log b.$$

Exercice 5 (théorème de Cauchy). Soit G un groupe d'ordre divisible par p premier, d'élément neutre e . En étudiant l'action de $\mathbb{Z}/p\mathbb{Z}$ sur $X = \{(x_1, \dots, x_p) \in G \times \dots \times G : x_1 \dots x_p = e\}$ définie par

$$1 \cdot (x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1}),$$

montrer que G admet un élément d'ordre p .