Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Probabilités et Entropie

Exercice 1 : [Probabilités conditionnelles]

1. Déterminer la loi de probabilité du jet d'un dé à 6 faces et d'un dé polyédrique à 5 faces.
2. Déterminer la probabilité que la somme soit égale à 8.
3. Déterminer la probabilité que la somme soit paire.
4. Déterminer la probabilité que sortent des nombres différents et que leur somme soit paire.
5. Déterminer la probabilité que la somme soit égale à 8, sachant que le premier dé vaut 5.
6. Déterminer la probabilité que la somme soit paire, sachant que le premier dé vaut 5.
7. Déterminer la probabilité que le premier dé soit 5, sachant que la somme est paire.

Exercice 2 : Quelle est la probabilité de trouver un mot de passe constitué de 5 caractères alphanumériques en moins de deux minutes par une machine testant 1 million de possibilités par seconde? Que devient cette probabilité, si on est sûr que le dernier caractère est un chiffre?

Exercice 3 : [Paradoxe des anniversaires] Combien faut-il de personnes pour en avoir (au moins) deux avec le même anniversaire ? et avec une probabilité $> 1/2$? (On pourra utiliser l'inégalité $1 + x \leq e^x$ pour faire une majoration)

Exercice 4 : Calculer l'entropie d'un lancer de dé et d'un lancer de pièce (pile ou face).

Exercice 5 : Soit X la variable aléatoire qui suit le nombre d'occurrences des lettres d'un texte en Français. Calculer l'entropie de ce texte.

Exercice 6 : [Stinson Ex 2.10] Montrer que $H(X,Y) = H(Y) + H(X|Y)$. Comme corollaire, montrer que $H(X|Y) \leq H(X)$ avec égalité si et seulement si X et Y sont indépendants.

Exercice 7 : [Stinson Ex 2.11] Montrer que $Pr(x|y) = Pr(x)$ pour tout $x \in \mathcal{P}$ et tout $y \in \mathcal{C}$ si et seulement si $H(M) = H(M|C)$.

Exercice 8 : Montrer que le chiffrement de Vernam est un système cryptographique parfait.

Exercice 9 : Montrer que le chiffrement de César n'est pas un système cryptographique parfait.

Exercice 10 : Soit un système cryptographique dans lequel $\mathcal{M} = \{a, b, c\}$, $\mathcal{C} = \{1, 2, 3, 4\}$ et $\mathcal{K} = \{k_1, k_2, k_3\}$, les opérations de chiffrement/déchiffrement étant données par la matrice :

	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

En supposant que les clés sont équiprobables, que le choix de la clé est indépendant du clair à chiffrer et que la distribution de probabilité sur les clairs est définie par $Pr_{\mathcal{M}}(a) = 1/2$, $Pr_{\mathcal{M}}(b) = 1/3$ et $Pr_{\mathcal{M}}(c) = 1/6$, calculez $H(M)$, $H(K)$, $H(C)$, $H(K|C)$ et $H(M|C)$.

Exercice 11 : Montrez que, pour n'importe quel cryptosystème, $H(K|C) \geq H(M|C)$. Montrez que, dans le cas d'un système est à confidentialité parfaite (c'est-à-dire $H(M|C) = H(M)$), on a $H(K) \geq H(C)$ et $H(K) \geq H(M)$. Quelle est la signification de cette dernière inégalité ?