EISTI. **Année scolaire 2010-2011**

DÉPARTEMENT "INFORMATIQUE"

THÉORIE DE L'INFORMATION

Série d'exercices N°2

PARTIE I. ENTROPIE : UN JEU D'ESPION !

Le chiffrement de César consiste à décaler l'alphabet de k positions de façon cyclique et de remplacer chaque lettre d'un massage clair par une lettre correspondante de l'alphabet décalé. La clé secrète de ce chiffre est un entier $1 \leq k \leq 25$ qui représente le décalage de l'alphabet. Nous allons dans un premier temps étudier la sécurité de ce chiffre et ensuite apprendre la méthode d'analyse des fréquences qui a permis de la casser.

Exercice 1 (Rendons à César ce qui est à César : son chiffre !)**.**

1. Montrer que pour les messages de longueur $l = 1$ le chiffre de César est parfaitement sûr au sens de Shannon. Pour cela montrez que

$$\forall m \in \mathcal{M},\ \ \forall c \in \mathcal{C},\ \ P[M = m|C = c] = P[M = m]$$

2. Montrer que pour les messages de longueur $l \geq 2$ le chiffre n'est plus parfaitement sûr. Pour cela analysez l'exemple suivant. Soient le message $m = AB$ et le chiffré $c = DM$. Montrer que $P[M = m|C = c] = 0$ tandis que $P[M = m] \neq 0$.

Exercice 2 (Cryptanalyse du chiffre de César)**.** La méthode d'analyse des fréquences a été inventé par le savant arabe AL-Kindi au IX-ème siècle. On suppose que l'on connaît la langue du texte clair et que l'on dispose du message chiffré. Dans le ca de chiffre de César on cherche à déterminer le paramètre k, clé du chiffre. La méthode consiste à comparer l'histogramme d'occurrences des caractères du chiffré avec la table des fréquences d'occurrence des caractères de la langue du texte clair. Voici la table des fréquences de la langue française.

Lettre	Fréquence %	Lettre	Fréquence %
A	8.4	N	7.13
B	1.06	O	5.26
C	3.03	P	3.01
D	4.18	Q	0.99
E	17.26	R	6.55
F	1.12	S	8.08
G	1.27	T	7.07
H	0.92	U	5.74
I	7.34	V	1.32
J	0.31	W	0.04
K	0.05	X	0.45
L	6.01	Y	0.3
M	2.96	Z	0.12

1. Votre mission, si vous l'acceptez, consiste à déchiffrer le message secret de votre binôme. Chacun de vous va composer un message de son choix. Pour le chiffrer, utiliser `http://www.bibmath.net/crypto/substi/cryptcesar.php3`l'applet java sur ce site. Envoyez le chiffré obtenu à votre voisin (par e-mail ou chat). Ensuite chacun cherchera à trouver la clé et le message clair par analyse fréquentielle.
2. Et maintenant, déchiffrez ceci :

UHGCHNK. GHNL OHNL IKHIHLHGL MKHBL PTZHGL IHNK ITKMBK TN STGBSBUTK. OHMKX TOBHG OT ITKMBK ET HN OHNL OHNEXS. NG OKTB OTNMHNK OXNM MHNCHNKL OHEXK ATNM IHNK OHBK LT IKHBX. NG SHFUB FTKVATBM XG SBZSTZTGM LNK ET KHNMX.

PARTIE II. ENTROPIE ET ARBRES DE DÉCISION

Exercice 3 (Le jeu de la fausse pièce)**.** On considère un jeu de n pièces, toutes d'apparence identiques. On sait qu'une seule pièce est fausse. Elle a un poids différent des autres mais on ne sait pas si elle plus légère ou plus lourde.

On dispose d'une balance à deux plateaux. À chaque pesée la balance peut se trouver dans l'une des trois configurations :

G Elle penche vers la gauche.

D Elle penche vers la droite.

E Elle reste à l'équilibre.

L'objectif est de déterminer avec le moins de pesées possible la fausse pièce et si elle plus légère ou plus lourde.

1. Soit $n = 8$.
   (a) Combien de réponses possibles il y a dans ce problème ?
   (b) Combien de possibilités différentes peut on obtenir avec 2 pesées ? Avec 3 pesées ? Conclusion sur la faisabilité de détermination de la fausse pièce en 2 ou en 3 pesées.
   (c) Est-il intéressant de peser deux lots de 4 pièces chacun ? Pourquoi ? Combien d'information nous apporterait une telle pesée ?
   (d) A l'aide du programme java à l'adresse `http://nlvm.usu.edu/fr/nav/frames_asid_139_g_4_t_2.html` Élaborer une stratégie de pesée permettant de déterminer la fausse pièce en 3 pesées dans tous les cas. Voici quelques conseils qui peuvent être utiles
      i. Essayez, pour commencer, de diviser l'ensemble de vos pièces en trois lots, de taille à peu près égale. Pour 8 pièces vous pouvez tester les décompositions $8 = 3 + 3 + 2$ ou $8 = 2 + 2 + 4$;
      ii. Lorsque l'on compare le même lot de pièces $L1$ à deux lots différents $L2$ et $L3$ on peut interpréter les résultats de façon suivante : si les deux résultats de comparaison sont identiques, la fausse pièce est dans le lot 1 et nous avons le sens de la différence de poids ($+$ ou $-$) ; il n'est pas possible que l'un des résultats soit G et l'autre D.

(e) Essayez de représenter votre stratégie sous forme d'arbre de décision. Les feuilles de l'arbre doivent représenter toutes les réponses possibles. La profondeur de cet arbre indique alors le nombre maximal de pesées.

2. A l'aide du même programme java élaborer une stratégie pour $n = 9, 10, 12$.