Université de Caen Normandie, UFR des Sciences — Année 2017/2018
Licence 3 - Informatique et Mathématiques — 2nde session

Module "Sécurité Informatique et Protection de données"
Session 2, 29 juin 2018 ;
durée : 1h30
Documents de cours, de TD et de TP sont autorisés.
La calculatrice est autorisée.
Le barème est indicatif.

Le logarithme utilisé dans les calculs d'entropie sera le logarithme en base 2.

Exercice 1 (6pts) :

On considère une source à trois éléments $S = \{a, b, c\}$ avec

$$p_a = 0.1, \qquad p_b = 0.2, \qquad p_c = 0.7.$$

1. Donnez l'entropie de S.
2. On considère le code $C = \{0, 0010, 0001100\}$ pour S où $a \mapsto 0$, $b \mapsto 0010$, $c \mapsto 0001100$. Donnez sa longueur moyenne.
3. Le code C est-il préfixe ?
4. Décomposer la séquence 0001000000110000100 en une séquence de mots de C.
5. Le code $C = \{0, 0010, 0001100\}$ est-il uniquement décodable ?
   Rappel : un code est uniquement décodable si toute séquence de bits est décomposable en au plus une séquence de mots.
6. Montrez que le code $C' = \{0, 0010, 000100\}$ n'est pas uniquement décodable : vous donnerez une séquence qui peut être décomposée de deux manières différentes.

Exercice 2 (5pts) :

On considère une source à deux symboles $S = \{a, b\}$ avec pour probabilité $p_a = 0.1$ et $p_b = 0.9$.

1. Calculer l'entropie de la source et trouver un code optimal dont vous donnerez la longueur moyenne pour cette source.
2. On considère maintenant la source $S' = S \times S \times S$ formée de triplets de symbole de S Les probabilités sont données par $p_{xyz} = p_x p_y p_z$ pour $(x, y, z) \in S^3$.
   Calculer les probabilités de chaque triplet et en déduire l'entropie de la source.
3. Appliquer l'algorithme de Huffman pour déterminer un code optimal pour S'. Vous déterminerez sa longueur moyenne ainsi que la longueur moyenne en bit pour encoder un symbole de S.

Exercice 3 (4pts) :

1. Donnez les éléments inversibles modulo 21.
2. Combien y a t'il d'éléments inversibles dans $\mathbb{Z}/3150\mathbb{Z}$?

3. Calculez l'inverse modulaire de 13 modulo 3150.
4. Calculez $3^{4363} \mod 55$.

Exercice 4 (5pts) :
Considérons un protocole RSA dont la clé publique est $(N, e) = (55, 3)$.

1. Calculez le chiffré de $m = 4$.
2. Calculez la clé de déchiffrement.
3. Déchiffrez le message $c = 2^3 = 8$.
4. Décrivez sur quel problème difficile repose la sécurité du protocole RSA ?
5. Décrivez un autre problème difficile en cryptographie.