Université de Caen Normandie, UFR des Sciences — Année 2021/2022
Licence 3 - Informatique et Mathématiques — session 1

Module "Sécurité Informatique et Protection de données"
Session 1, novembre 2021 ;
durée : 1h30
Documents de cours, de TD et de TP sont autorisés.
La calculatrice est autorisée.
Le barème (sur 22 donc avec 2 points de bonus) est indicatif.

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

Exercice 1 - Arithmétique (4pts) :

1. Donnez les éléments inversibles modulo 33.
2. Combien y a t'il d'éléments inversibles dans $\mathbb{Z}/17640\mathbb{Z}$?
3. Calculez l'inverse modulaire de 11 modulo 17640.
4. Calculez $3^{4419} \mod 221$.

Exercice 2 - RSA (3pts) : Alice dispose d'une clé publique RSA (n_A, e_A) et d'une clé privée associée d_A.
Eve intercepte un message c chiffré envoyé par Bob à Alice via le protocole RSA. Afin de déchiffrer c, Eve procède de la manière suivante :

— Eve choisit un entier $0 < r < n_A$ au hasard et calcule $x = r^{e_A} \mod n_A$;
— Eve calcule $y = xc \mod n_A$;
— Eve demande à Alice de **signer** y avec sa clé et Alice retourne u à Eve.

Exprimez u en fonction de y et la clé d'Alice. Montrez que Eve peut facilement découvrir le message m émis par Bob. Qu'en déduisez-vous sur l'usage des clés ?

Exercice 3 - codage de source (4pts) :

On considère une source sans mémoire qui produit un bit par unité de temps selon la distribution $p_0 = 0.4$ et $p_1 = 0.6$. On souhaite faire passer ce flot de bit à travers un canal qui ne peut faire passer que 0.99 bits par unité de temps (ou de manière équivalente, 99 bits toutes les 100 unités de temps).

Trouvez un code de Huffman qui permet de compresser le flot de la source afin qu'il puisse passer par le canal (il faudra considérer des blocs de bits).

Exercice 4 - Canal (4pts) :

On considère une source X sur l'alphabet à trois symboles $\{a, b, c\}$ avec pour probabilités $p_a = 0.2$, $p_b = 0.3$ et $p_c = 0.5$.

On considère le canal $\mathcal{C}$, dont l'alphabet d'entrée et de sortie est aussi $\{a, b, c\}$ et dont la matrice de transition $\mathcal{M}$ est donnée par :

$$\begin{array}{c} \begin{array}{ccc} \mathsf{a} & \mathsf{b} & \mathsf{c} \end{array} \\ \begin{pmatrix} 3/4 & 1/8 & 1/8 \\ 1/8 & 3/4 & 1/8 \\ 1/8 & 1/8 & 3/4 \end{pmatrix} \begin{array}{c} a \\ b \\ c \end{array} \end{array}$$

On note Y la source à la sortie du canal lorsque X est à l'entrée.

1. Donnez la loi conjointe de (X, Y). En déduire la loi de Y.
2. Quelle est l'entropie de X et de Y ? Quelle est l'entropie conjointe de (X, Y) ?
3. En déduire l'information mutuelle $I(X, Y)$ et les entropies conditionnelles $H(X|Y)$ et $H(Y|X)$.
4. Donnez la capacité du canal $\mathcal{C}$.

Exercice 5 - Algorithmes probabilistes (7pts) :

L'exercice qui suit a été commencé en cours mais non terminé.

Un problème de décision $\mathcal{D}$ est un problème dont la réponse est binaire : 0 ou 1 (ou oui/non, vrai ou faux, ...). Pour un problème de décision $\mathcal{D}$, les instances positives (resp. négative) sont celles dont la réponse est 1 (resp. 0).

Définition. 1 *Un problème de décision est dit dans la classe RP (random polynomial-time) s'il existe un algorithme probabiliste $\mathcal{A}$ tel que*

$$\begin{aligned} x \text{ est une instance positive} &\Rightarrow Pr\left[\mathcal{A}(x) = 1\right] \geq \frac{1}{2} \\ x \text{ est une instance négative} &\Rightarrow Pr\left[\mathcal{A}(x) = 1\right] = 0 \end{aligned}$$

Q1. Pour les problèmes dans RP, quelle réponse (0 ou 1) ne donne lieu à aucune erreur ? Justifiez.

Définition. 2 *Un problème de décision est dit dans la classe $co - RP$ (complementary random polynomial-time) s'il existe un algorithme probabiliste $\mathcal{A}$ tel que*

$$\begin{aligned} x \text{ est une instance positive} &\Rightarrow Pr\left[\mathcal{A}(x) = 1\right] = 1 \\ x \text{ est une instance négative} &\Rightarrow Pr\left[\mathcal{A}(x) = 0\right] \geq \frac{1}{2} \end{aligned}$$

Q2. Pour les problèmes dans $co - RP$, quelle réponse (0 ou 1) ne donne lieu à aucune erreur ? Justifiez.

La valeur 1/2 dans les définitions précédentes n'a aucune importance. Il suffit d'utiliser une probabilité $p \in]0, 1[$.

Définition. 3 *Pour un problème de décision $\mathcal{D}$ et une instance x du problème, on note $\chi_{\mathcal{D}}(x)$ la réponse (1=positive ou 0=négative) au problème. Un problème de décision $\mathcal{D}$ est dit dans la classe ZPP (Zero error probability) s'il existe un algorithme probabiliste $\mathcal{A}$, de complexité (dans le pire des cas) polynomiale, retournant 0, 1 ou $FAIL$ tel que*

$$\begin{aligned} &\forall x, && Pr\left[\mathcal{A}(x) = FAIL\right] \leq \frac{1}{2} \\ &\forall x && Pr\left[\mathcal{A}(x) = \chi_{\mathcal{D}}(x) \quad ou \quad \mathcal{A}(x) = FAIL\right] = 1 \end{aligned}$$

Q3. Considérons un problème dans ZPP et un algorithme probabiliste $\mathcal{A}$ pour le résoudre. Construire un algorithme $\mathcal{B}$ qui n'échoue jamais et qui retourne toujours la bonne réponse.

Q4. A quelle famille d'algorithmes appartient l'algorithme $\mathcal{B}$?

Q5. Montrez que $ZPP \subseteq RP$.

Aide : considérez un problème dans ZPP et un algorithme $\mathcal{A}$ qui respecte la définition 3 (ZPP). Construisez ensuite un algorithme $\mathcal{B}$ qui respecte la définition 1 (RP) pour le même problème.

Q6. Montrez que $ZPP \subseteq co - RP$ et en déduire que $ZPP \subseteq RP \cap co - RP$.

Q7. Montrez que $ZPP = RP \cap co - RP$.