Licence d'informatique. I23, Mathématiques discrètes

Première session 2006-2007.

Université du Sud Toulon-Var.

lundi 18 juin 2007, 14h00-16h15

Les documents sont interdits. Seule la calculatrice est autorisée. Le barème est approximatif et donné à titre indicatif.

Exercice 1. [6pts] Soit $\sigma \in \mathfrak{S}_9$ la permutation définie par :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 1 & 8 & 4 & 2 & 6 & 9 & 5 \end{pmatrix}$$

1. [2pts] Quel est le cardinal ω du groupe symétrique $\mathfrak{S}_9$? Déterminer, sans division euclidienne, $\omega \mod 11$.

2. [3pts] Décomposer la permutation σ en produit de cycles à supports disjoints. On rappelle que l'ordre d'une permutation σ est le *plus petit* entier non nul m tel que $\sigma^m = e$, où e désigne l'identité. Déterminer l'ordre de cette permutation, puis calculer σ^4 et σ^{64}.

3. [1pt] Calculer la signature de σ.

Exercice 2. [4pts] MM. Aubry et Zanotti surveillent l'examen de I23 qui se déroule de 14h à 16h15. M. Aubry, qui a trop forcé sur le vin au déjeuner, somnole quelques secondes toutes les 28 minutes tandis que M. Zanotti regarde sa montre tous les quarts d'heure car les surveillances d'examens l'ennuient. Les étudiants ont vu M. Aubry bailler à 14h08 la première fois, alors que M. Zanotti a regardé sa montre dès 14h02.

1. [1pt] Si t désigne le temps écoulé en minutes depuis le début de l'épreuve, quelle congruence satisfait t pour correspondre aux moments d'inattention de M. Aubry ? De M. Zanotti ?

2. [1pt] Justifier, sans faire de calculs, l'existence de solutions au système de congruences ci-dessus.

3. [2pts] A quelle(s) heure(s) les étudiants peuvent-ils espérer communiquer entre-eux sans être remarqués par les examinateurs ?

Exercice 3. [8pts] Alice et Bob sont tombés amoureux en cours de I23 et profitent des TP de C pour échanger des mots doux, mais redoutent que leurs messages soient interceptés par leurs camarades facétieux. Leur grande passion durant les cours les ayant empêché de se concentrer sur les subtilités du protocole RSA, ils décident d'utiliser le protocole à clef secrète suivant, moins ambitieux, dans lequel un texte subit 4 opérations avant d'être transmis :

(1) *Filtrage :* on retire les accents des lettres accentuées et on efface tous les symboles du texte qui ne font pas partie des 26 lettres de l'alphabet $A, B, \ldots, Z$. Par exemple le texte *à mon amour* devient $AMONAMOUR$;

(2) *Codage :* chaque lettre du message est codée avec le code naturel suivant : $A \to 0, B \to 1, \ldots, Z \to 25$;

(3) *Chiffrement :* on chiffre chaque entier x de la séquence codée avec la fonction de chiffrement $e : \mathbf{Z}/26\mathbf{Z} \to \mathbf{Z}/26\mathbf{Z}$ définie par

$$e(x) = a.x + b.$$

où $(a, b) \in (\mathbf{Z}/26\mathbf{Z})^2$ constitue la clef secrète fixée par Alice et Bob au préalable dans un endroit discret.

(4) *Décodage :* les entiers obtenus sont décodés.

Exemple : avec la clef $(a, b) = (7, 5)$, le symbole *é* suit la séquence :

$$é \xrightarrow[\text{filtre}]{\text{filtrage}} E \xrightarrow[\text{code}]{\text{codage}} 4 \xrightarrow[(7.x+5) \bmod 26]{\text{chiffrement}} 7 \xrightarrow[\text{code}]{\text{décodage}} H$$

On s'intéresse au déchiffrement à présent.

1. [1pt] Combien y-a-t-il de clefs (a, b) distinctes possibles ?

2. [1pt] Quel message chiffré reçoit Bob si Alice lui envoie le message *à mon amour* avec la clef secrète $(7, 5)$?

3. [2pts] Quels sont les chiffrés des lettres K et X avec la clef $(a, b) = (6, 1)$? La fonction e est-elle injective ? Quel problème poserait ce résultat à Bob ?

4. [2pts] Calculer $\varphi(26)$ à l'aide des propriétés de la fonction indicatrice d'Euler. Énumérer les entiers qui admettent un inverse dans $\mathbf{Z}/26\mathbf{Z}$?

5. [1pt] Bob dispose d'un chiffré y. Donner une condition suffisante sur la clef (a, b) pour que Bob puisse déchiffrer y d'une seule façon ?

6. [1pt] Déduire de la question précédente le nombre de clefs qui assurent l'unicité du déchiffrement.

Exercice 4. [4pts] Soit C le code linéaire binaire de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

1. [1pt] Déterminer la longueur n et la dimension k du code C.

2. [2pts] Combien y a-t-il de mots dans le code C ? Enumérer les mots du code et en déduire la distance minimale d du code C et sa capacité de correction.

3. [1pt] Quels sont les bits de redondance si l'on veut envoyer le message $u = (1, 1, 1)$?