Examen du mardi 7 janvier 2020, de 9h à 11h.

Sont autorisés : une calculatrice et résumé de cours manuscrit format A4 recto-verso.
Autres documents et portables interdits.
Le sujet comporte 2 pages. Le barême est indicatif.

1. PARTAGE DE SECRET (8 POINTS)

Un informaticien dispose d'un coffre avec un code secret s à 11 chiffres en base 10 ($0 \leq s < 10^{11}$). Il veut transmettre s à ses trois heritiers en partageant s en trois parties (afin de s'assurer de l'accord des trois héritiers pour l'ouverture du coffre). Comme il affectionne les entiers 16 bits, il décide d'écrire s en base $b = 2^{16}$

$$s = \sum_{i=0}^{n} s_i b^i$$

et donne la valeur de s_0 au premier héritier, s_1 au deuxième héritier et s_2 au troisième héritier.

(1) Justifier que $n = 2$ (on rappelle que $0 \leq s < 10^{11}$).

(2) Déterminer s en base 16 et en base 10 sachant que $s_0 = 0, s_1 = 0, s_2$=`0x17` en base 16 (i.e. $s_2 = 23$ en base 10).

(3) Le deuxième et le troisième héritier souhaiteraient ouvrir le coffre sans le premier héritier (donc en connaissant s_1 et s_2, mais pas s_0). Combien d'essais de code devront-ils faire ?

(4) Le premier héritier et le deuxième héritier souhaiteraient ouvrir le coffre sans le troisième héritier (donc en connaissant s_0 et s_1, mais pas s_2). Combien d'essais de code devront-ils faire ?

(5) Pourrait-on adapter la méthode de partage pour être moins inéquitable ?

(6) Un mathématicien conseille à notre informaticien de partager s en donnant aux héritiers les valeurs r_0, r_1, r_2 des restes de la division euclidienne de s par trois nombres premiers $p_0 = 4643$, $p_1 = 4649$ et $p_2 = 4651$. Calculer r_0, r_1 et r_2 pour s du (1).

(7) Justifier que les trois héritiers peuvent reconstituer s à partir de r_0, r_1, r_2.

(8) Le partage du mathématicien est-il équitable ? Justifier.

2. CRYPTOGRAPHIE (12 POINTS)

Les caractères de a à z sont représentés par les entiers de 10 à 35 (a=10, b=11, ..., z=35), l'espace par 36 et les entiers de 0 à 9 par eux-mêmes. On a 37 caractères possibles, on travaille dans la suite dans $\mathbb{Z}/p\mathbb{Z}$ pour $p = 37$.

2.1. **Codage linéaire.** Ici, on code un message caractère par caractère en utilisant la correspondance précédente et l'application φ définie dans $\mathbb{Z}/p\mathbb{Z}$ par :

$$\varphi(n) = an + b \pmod{p}, \quad a = 10,\ b = 3$$

(1) 10 est-il inversible modulo 37 ? Si oui, calculer l'inverse de 10 modulo 37.

(2) φ est-elle bijective ? Si oui, déterminer son application réciproque.

(3) Coder le mot janvier.

(4) Décoder le message [25,35,17,32,14].

(5) Expliquez une méthode que pourrait utiliser un attaquant ne connaissant pas les entiers a et b utilisés dans la définition de la fonction φ pour déchiffrer un message suffisamment long.

2.2. **Cryptographie de Hill.** Soit $p = 37$ et la matrice à coefficients dans $\mathbb{Z}/p\mathbb{Z}$

$$A = \begin{pmatrix} 1 & 5 \\ 7 & 8 \end{pmatrix} \ [37]$$

(1) Montrer que A est inversible et calculer son inverse.

(2) On groupe les caractères par paires, chaque paire de caractères est considérée comme un vecteur v de $(\mathbb{Z}/37\mathbb{Z})^2$. On code un vecteur v en envoyant Av. Comment décode-t-on un message codé ?

(3) Coder le message composé des 4 chiffres 2020

(4) Décoder le message suivant
`[20,10],[27,12],[9,16],[14,32],[19,14],[9,16],[2,14],[2,14]`

(5) Ce codage est-il plus résistant à une attaque que celui de la section précédente ? Comment pourrait-on le rendre plus résistant ?

(6) Donner un algorithme permettant de coder un message, prenant en argument une matrice `A` (sous forme d'une liste de 2 listes ayant 2 éléments) et un message `m` sous forme d'une liste d'entiers compris entre 0 et 36 et renvoyant un message codé sous forme d'une liste d'entiers compris entre 0 et 36. Indiquer comment adapter cet algorithme pour votre codage plus résistant de la question (5).