MAT309
2020-2021

Université Grenoble Alpes

Partiel du 12/11/2020

Ordinateurs et portables interdits. Calculatrice autorisée. Feuille recto-verso A4 manuscrite autorisée.
Toutes les réponses doivent être justifiées et la qualité de la rédaction sera prise en compte.
Certaines réponses aux exercices 1 et 2 doivent être reportées sur la feuille de réponse.
Le barême tiendra compte de la longueur du sujet.

Tableau de correspondance

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercice n° 1 Un décalage de César d'ordre k où $0 \leq k \leq 25$ est la méthode de chiffrement consistant à décaler chaque lettre de l'alphabet de k positions en suivant une permutation circulaire des lettres.

1. Chiffrer le mot **DLST** en utilisant un décalage de César d'ordre 9.
2. Déchiffrer le mot **PYEBSOB** sachant que le mot initial a été chiffré par un décalage d'ordre 10.
3. Les chiffrements précédents étant trop simples à casser, on propose le chiffrement suivant. On choisit une clé qui sera dans notre cas le mot **COVID**.

   La première lettre du texte à chiffrer sera modifiée en utilisant le décalage de César qui envoie A sur C (où C est la première lettre de la clé COVID), la deuxième par le décalage de César qui envoie A sur O, la troisième par le décalage de César qui envoie A sur V, la quatrième par le décalage de César qui envoie A sur I, la cinquième par le décalage de César qui envoie A sur D, la sixième par le décalage de César qui envoie A sur C (on recommence au début de la clé), etc, ...

   (a) Chiffrer la phrase **J AIME MON MASQUE LAVABLE** par cette méthode (sans tenir compte des espaces).

   (b) On note `T[i]` l'entier donné par le tableau de correspondance pour la lettre d'indice i du texte à chiffrer, `C[i]` l'entier donné par le tableau de la lettre d'indice i de la clé et `CH[i]` l'entier donné par le tableau de la lettre d'indice i du texte chiffré. On utilise des indices commençant à 0.

   Comment obtient-on la liste des `CH[i]` à partir de la liste des `T[i]` et de la liste `[C[0],C[1],···,C[4]]` ?

   (c) Combien de chiffrements différents peut-on obtenir avec des clés de 5 lettres ?

   (d) Quelle(s) méthode(s) peut-on utiliser pour casser un tel chiffrement si on ne connait pas la clé ?

   (e) Écrire un algorithme en langage naturel qui à un texte (composé uniquement des lettres A à Z) et une clé associe le texte chiffré par la méthode précédente. On supposera que
   — le caractère d'indice i d'une chaine de caractère `s` est `s[i]`, avec des indices commençant à 0,
   — la fonction `len(s)` renvoie la longueur de la chaine `s`
   — la fonction `ord(c)` convertit un caractère `c` en entier
   — la fonction `chr(n)` convertit un entier `n` en caractère

Exercice n° 2
On rappelle qu'en base 16 les chiffres sont donnés par `0,1,···9,A,B,C,D,E,F`.

1. Convertir tous les nombres du tableau de correspondance en base 2.
2. On décide alors de coder un texte en remplaçant chacune de ses lettres par le nombre correspondant écrit en base deux.

   Ainsi par exemple **INF** devient `1000 1101 101`

   En enlevant les espaces, on obtient un entier écrit en base 2, ici `0b10001101101`, que l'on recode en base 16, soit ici `0x46D`.

   Chiffrer de cette manière le mot **COVID**.

   Proposer un autre mot ayant le même chiffrement.

3. Pour corriger le défaut de la méthode précédente on écrit tous les nombres de 0 à 25 en base 2 avec 5 bits (en ajoutant des 0 au début si nécessaire). On le convertit ensuite en base 16.
   Chiffrer de cette manière le mot **COVID**.
4. Notons n le chiffrement du mot COVID obtenu à la question précédente. Donner le quotient et le reste, en base 16, de la division euclidienne de n par 6. On utilisera l'algorithme de la potence. Pour s'aider, on pourra écrire la table de multiplication par 6 en base 16.

Exercice n° 3

1. Montrer que 2020 et 33 sont premiers entre eux et donner l'identité de Bézout. On détaillera les calculs en utilisant l'algorithme d'Euclide étendu.
2. Déterminer tous les couples d'entiers (x, y) tels que $2020x - 33y = 3$.
3. Existe t-il des entiers x positifs et plus petit que 20000 tels que le reste de la dision euclidienne de x par 33 soit 1 et le reste de la dision euclidienne de x par 2020 soit 4 ? Si oui, donner toutes les solutions.

Exercice n° 4

1. Déterminer le reste de la division euclidienne de 2020^{873} par 14. La méthode doit être explicitée.
2. Donner la liste des inversibles de $\mathbb{Z}/14\mathbb{Z}$.
3. Résoudre l'équation dans $\mathbb{Z}/14\mathbb{Z}$, $\overline{11}x = \overline{3}$.

Exercice n° 5 On considère l'équation suivante :

$$(*) \qquad x^2 - 13y^2 = 7$$

. On suppose dans les questions 1 et 3 que (x, y) est un couple d'entiers vérifiant $(*)$.

1. Montrer que $x^2 + y^2 \equiv 0$ [7]
2. Calculer les carrés de tous les éléments de $\mathbb{Z}/7\mathbb{Z}$.
3. En déduire que x et y sont multiples de 7.
4. $(*)$ a-t-elle des solutions ? Indication : si c'est le cas, il existe des entiers a et b tels que :

$$x = 7a, y = 7b$$