EISTI Ecole Internationale des Sciences du Traitement de l'Information	**Cycle préparatoire 1 ère année** **Devoir surveillé n ° 2**
Nombre de pages : 3	Mathématiques appliquées
Durée : 2 heures	Date : 9 mai 2019

Appareils électroniques et documents interdits.

Il sera tenu compte de la qualité de la rédaction et de la précision des justifications.

Le sujet comporte trois exercices. L'ordre dans lequel ceux-ci sont traités n'est pas imposé.

Si vous êtes amené à repérer ce qui peut vous sembler être une erreur d'énoncé, vous la signalerez sur votre copie et devrez poursuivre votre composition en expliquant les raisons des initiatives que vous êtes amené à prendre.

◇◇

EXERCICE 1 (Chiffrement affine – 6 points) Afin de coder un message, chaque lettre de l'alphabet est associée à un nombre entier comme indiqué dans le tableau ci-dessous :

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

Table 1: Correspondance entre l'alphabet et les chiffres

Soit x le nombre associé à la lettre à coder, le chiffrement affine consiste à coder le chiffre x par le chiffre y qui est le reste de la division euclidienne de $f(x)$ par 26, f est une fonction affine

$$f(x) = ax + b$$

avec a et b premiers entre eux.

1. Vérifier que $19 \times 11 \equiv 1 \bmod (26)$ et que $-152 \equiv 4 \bmod (26)$.
2. En utilisant le chiffrement à l'aide de $f(x) = 11x + 8$, coder la lettre L.
3. (a) Soit k un entier relatif. Montrer que si $k \equiv 11x \bmod (26)$ alors $19k \equiv x \bmod (26)$.
   (b) Démontrer la réciproque de l'implication précédente.
   (c) En déduire que $y \equiv 11x + 8 \bmod (26)$ équivaut à $x \equiv 19y + 4 \bmod (26)$.
   (d) À l'aide de la question précédente, décoder la lettre F.

EXERCICE 2 (Chiffrement de Vigenère – 4 points)

1. Rappeler le principe de codage et de décodage du Vignère.
2. (a) Trouver la clé de codage de quatre lettre, avec seul indice
   - *"Mon premier est le féminin de il."*
   - *"Mon second est une expression permettant de faire avancer un cheval."*
   - *"Mon troisième est la première lettre du prénom de votre enseignante des maths appliquées."*
   - *"La poule pond nos quatrièmes."*
   - *"Mon tout est un satellite naturel de la Terre, qui l'éclaire la nuit."*

   (b) En utilisant la clé trouvée ci-dessus, décoder le message suivant: WUUEFNRYC

EXERCICE 3 (Chiffrement RSA – 10 points) Les questions 1 et 2 sont des questions préparatoires aux questions 3 et 4. La question 3 aborde le cryptage avec le système RSA et la question 4 aborde le décryptage avec le même système.

1. Calcul du reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.
   (a) Vérifier que $8^2 \equiv 9 \bmod 55$ et que $8^7 \equiv 2 \bmod 55$.

(b) En déduire que le reste dans la division euclidienne par 55 du nombre 8^{21} est 8.

(c) Déduire le reste dans la division euclidienne par 55 de 8^{23}.

2. On considère l'équation (E): $23x - 40y = 1$, dont les solutions sont des couples (x, y) d'entiers relatifs.

(a) Justifier le fait que l'équation (E) admet au moins un couple solution.

(b) Donner un couple, solution particulière de l'équation (E).

(c) Rappeler la division de l'inverse d'un entier relatif a modulo un entier naturel non nul n.

(d) Déterminer l'unique inverse d de 23 modulo 40 tel que $0 \leq d < 40$.

3. Cryptage dans le système RSA.

Une personne A choisit deux nombres premiers p et q, puis calcule les produits

$$n = pq, \ \ \varphi(n) = \big(p-1\big)\big(q-1\big).$$

Elle choisit également un entier naturel c premier avec $\varphi(n)$. La personne A publie le couple (n, c) qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté. Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et n-1.

Pour crypter un entier a de cette suite, on calcule le reste b dans la division euclidienne par n du nombre a^c et le nombre crypté est l'entier b.

Dans la suite, on considère $p = 5$, $q = 11$ et $c = 23$.

(a) Calculer les nombres n et $\varphi(n)$, puis justifier que la valeur de c vérifie la condition voulue.

(b) Un émetteur souhaite envoyer à la personne A le nombre $a = 8$. Déterminer la valeur du nombre crypté b.

4. Décryptage dans le système RSA.

La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions

$$0 \leq d < n \ \text{ et } \ cd \equiv 1 \bmod \big(\varphi(n)\big).$$

Elle garde secret ce nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique. Pour décrypter un nombre crypté b, la personne A calcule le reste a dans la division euclidienne par n du nombre b^d, et le nombre en clair est le nombre a.

(a) Quelle est la valeur de d?

(b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.