EISTI se transforme et devient CY TECH

Département de Mathématiques
Année universitaire 2019-2020

DS2 du 29/05/2020

Filière : **PREPA1 - Pau**
Matière : **Mathématiques appliquées**
Durée : **2h**
Responsable : **BARRAU Nelly ; FORTIN Nisrine**

En cas de problème informatique pendant l'épreuve (connexion internet, ...) : le candidat devra impérativement contacter (avant la fin de l'épreuve/dépôt), l'un des numéros suivants et y déposer un message :

(+33)5 590 590 84 (*Nisrine*) *ou* (+33)5 590 590 96 (*Nelly*)

La communication entre les candidats durant l'épreuve est strictement interdite.
En cas de copies ressemblantes/similaires/identiques/proches : les candidats seront soumis à une évaluation orale (notée).

CONSIGNES *: Évaluation à distance*

1. L'usage d'un ordinateur est autorisé et nécessaire :
   - *récupération du sujet sur AREL,*
   - *scan/photo de votre copie : écrits (**chaque feuille doit être numérotée / nombre total de feuilles**)*
   - *dépôt sur AREL : Archive intitulée Groupe-NOM-Prenom (exemple : P1-FORTIN-Nisrine) et contenant tous vos écrits.*
2. L'usage des supports de cours et TD de mathématiques appliquées est autorisé.
3. L'usage de la calculatrice est autorisé.
4. Le barème est signalé à titre indicatif.
5. La **qualité de la rédaction** sera prise en compte dans la note. Les réponses devront être soigneusement justifiées.
6. Ce DS est composé de 3 exercices indépendants.

Dans tout ce sujet, l'alphabet considéré comporte les 40 caractères ordonnés suivants :

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 À Â Ç É È Ê Ë Î Ï Ô Œ Ù Û Ü

Les signes de ponctuation (' " . , ; : ! ? ...), d'opérations (+ - × ÷) et les chiffres (0 1 2 3 4 5 6 7 8 9) ne sont pas cryptés : ils restent inchangés quelque soit le message (clair ou crypté).

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

À	Â	Ç	É	È	Ê	Ë	Î	Ï	Ô	Œ	Ù	Û	Ü
26	27	28	29	30	31	32	33	34	35	36	37	38	39

TABLE 1 – Correspondance entre l'alphabet et les chiffres

EXERCICE 1 (Chiffrement Vigenère – 7 points) **Toutes vos réponses doivent être soigneusement justifiées.**

1. La clé (de 3 lettres) de cet exercice est donnée dans le "Qui suis-je" suivant :

   Même si on me vide
   en plus d'un tour,
   Vous m'avez à dos ou à main.

2. En expliquant votre raisonnement et votre méthode, **retrouver la clé de 3 lettres** qui a transformé le message

   VŒU DÉJÀ REÇU

   en message crypté

   ÜŒW VÉLE RGGU

3. À l'aide de la clé de la question 1., chiffrer le message suivant en expliquant soigneusement toutes les étapes de votre raisonnement :

   TÊTE BIEN FAITE ET BON CŒUR

4. À l'aide de la clé de la question 1., déchiffrer le message suivant en expliquant soigneusement toutes les étapes de votre raisonnement :

   ÉÀQ PSG ÙRQ ÛVG ÛNG ÜON ËNV HIN WXK ŒTG ÛNE ZEO ÀN

Tournez svp →

Exercice 2 (Chiffrement César – 6 points) **Toutes vos réponses doivent être soigneusement justifiées.**

1. À l'aide de congruences, déterminer x, y, z et t :

   $$42 \equiv x \pmod{40}, \qquad -13 \equiv y \pmod{40}, \qquad -23 \equiv z \pmod{40}, \qquad 54 \equiv t \pmod{40}.$$

2. Chiffrer le message suivant, avec un décalage de 10

   L'ÉPIDÉMIE DU COVID-19

3. Sachant que le décalage est de 25, déchiffrer le message suivant et donner sa réponse

   ÂËÎÈÈCÉC GÜECÉ ACOÛÜÙ (ÇOÂZŒZÊÉ 25)

Exercice 3 (Chiffrement RSA – 7 points) **Toutes vos réponses doivent être soigneusement justifiées.**

Nelly et Nisrine souhaitent communiquer via un chiffrement RSA.

1. Nisrine construit la clé publique $n = 85$ et $e = 3$.
   (a) Déterminer p, q et $\varphi(n)$ la fonction d'Euler.
   (b) Nisrine souhaite crypter le message suivant :

   MAXIMUM.

   Quel est le message crypté que Nelly recevra ?
2. Nelly construit la clé privée d à partir de la clé publique de Nisrine.
   (a) Déterminer la valeur de d. ($d \in \mathbb{N}$)
   (b) Nelly reçoit le message crypté suivant :

   IDAKÂIAIAY !

   Quel est le message que Nisrine a envoyé à Nelly ?

Fin. ♣