

CRYPTOGRAPHIE

Terminale S spécialité

Séance informatique

Énoncé

Le but de cet exercice est le cryptage et décryptage d'un message utilisant le « chiffrement à clef secrète ». On utilisera le codage informatique des lettres avec le code ASCII. Le message choisi est une citation de Mignon McLaughlin (journaliste et écrivain américaine, 1913-1983).

1. Expérimentation

Préliminaire : En informatique, le code ASCII consiste à associer à chaque caractère (lettre de l'alphabet, chiffre, signe de ponctuation, ...) un code numérique que l'on appelle son code ASCII.

Par exemple, le code de A est 65, celui de B est 66, celui de a est 97, celui de l'espace est 32... Le code utilisé est un entier n tel que $0 \leq n \leq 255$.

Syntaxe : Dans la plupart des tableurs, la fonction «code» renvoie le code ASCII. La fonction réciproque est notée « CAR ». On entre « = CODE("A") » pour obtenir le nombre 65 et on entre « =CAR(65) » pour obtenir la lettre A.

1) Cryptage

a) En utilisant le code ASCII, coder le message suivant :

Dans l'arithmétique de l'amour, un plus un égal...

Dans la zone de saisie du message, on ne mettra qu'une seule lettre par cellule et on n'oubliera pas de taper un espace pour séparer les mots. La zone de saisie du message est la ligne 1 à partir de la cellule B1. Le message codé avec le code ASCII apparaîtra sur la ligne 2 à partir de la cellule B2.

Appeler l'examineur.

b) Le code ASCII ne constituant pas un codage bien secret, la ligne 3 consiste à crypter le code ASCII en utilisant le cryptage suivant :

On note C la fonction de cryptage qui, à tout n entier appartenant à $[0 ; 255]$ associe le reste de la division de $7n$ par 256. Soit $C(n)$ ce reste.

Compléter le tableau réalisé en 1) a), en y ajoutant à la ligne 3, les restes $C(n)$ correspondant à chaque code n de la ligne 2.

Le tableau ci-dessous donne le début de la phrase et du codage à obtenir :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	message	<i>D</i>	<i>a</i>	<i>n</i>	<i>s</i>		<i>l</i>		<i>a</i>	<i>r</i>	<i>i</i>	<i>t</i>	<i>h</i>	<i>m</i>	
2	codage ASCII	68	97	110	115	32	108	32	97	114	105	116	104	109	
3	message codé	220	167	2	37	224	244	224	167	30	223	44	216	251	

2) Décryptage à l'aide de la clef secrète

La fin de la citation de Mignon McLaughlin est cryptée par :

244 224 223 2 202 223 2 223 224 195 44 224 188 195 51 72 224
251 9 223 2 37 224 51 2 224 95 209 167 244 224 86 95 30 9

Pour décrypter la fin de cette citation, on note D la fonction de décryptage qui, à tout entier k appartenant à $[0 ; 255]$, associe le reste de la division de $183k$ par 256.

Entrer en ligne les nombres cryptés ci-dessus, puis sur une nouvelle ligne, utiliser la fonction D pour lire la fin de la citation de Mignon McLaughlin.

Appeler l'examineur.

2. Justifications

1) Justification du codage : pour le codage ASCII, deux lettres de l'alphabet sont codées par deux nombres distincts.

Il faut s'assurer que le cryptage choisi au **1. 1) b)** code deux nombres n et p distincts, compris entre 0 et 255, par deux nombres distincts.

a) Montrer que, si $C(n) = C(p)$ alors $7(n - p) \equiv 0 \pmod{256}$.

b) En déduire que $n = p$. Justifier alors que le codage est valide.

2) Explication du décodage

a) Vérifier que $183 \times 7 \equiv 1 \pmod{256}$ et en déduire que $183 \times (7n) \equiv n \pmod{256}$.

b) Expliquer pourquoi la fonction D , qui associe à k le reste de la division de $183k$ par 256, assure le décryptage attendu.

Production demandée.

- Partie 1. : Écrire le message codé de la première partie de la citation et le message décodé de la fin de la citation.
- Partie 2. : Rédaction des justifications demandées.