

# EP 019 - 2007 : Cryptographie

Auteur du corrigé : Alain Soléan

TI-Nspire™ /TI-Nspire™ CAS

**Avertissement** : ce document a été réalisé avec la version 1.4 ; il est disponible dans sa version la plus récente sur notre site <http://education.ti.com/france>, menu Ressources pédagogiques.

**Fichier associé** : EP019\_2007\_Cryptographie.tns

## 1. Le sujet

### Sujet 019 de l'épreuve pratique 2007– Arithmétique : Cryptographie

#### 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 américain, 1913 – 1983).

#### I - 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.

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

Compléter le tableau réalisé en 1.a), en y ajoutant à la ligne 3, les restes  $\mathcal{C}(n)$  correspondant à chaque code 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	D	a	n	s		l	'	a	r	i	t	h	m
2	Codage ASCII	68	97	110	115	32	108	39	97	114	105	116	104	109
3	Message codé	220	167	2	37	224	244	17	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 17 223 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  $\mathcal{D}$  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.

## II – 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 **I- 1.b**) code deux nombres  $n$  et  $p$  distincts, compris entre 0 et 255, par deux nombres distincts.

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

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

### 2. Explication du décodage

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

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

## Production demandée

- Partie I : Ecrire le message codé de la première partie de la citation et le message décodé de la fin de la citation.
- Partie II : rédaction des justifications demandées.

## Compétences évaluées

- **Compétences TICE**
  - Utiliser les fonctions du tableur (reste d'une division euclidienne, codes ASCII, ...);
  - Réaliser une feuille de calcul adaptée à la situation.
- **Compétences mathématiques**  
Utiliser les propriétés du programme d'arithmétique :
  - congruences,
  - division euclidienne,
  - nombres premiers entre eux.

*Remarque : dans le texte original, les apostrophes (codés ASCII 39) étaient remplacés par des blancs (codés ASCII 32).*

## 2. Corrigé

*Remarques :*

1. Pour des raisons de taille et de lisibilité, le tableau demandé en lignes sera réalisé en colonnes.
2. La fonction renvoyant le code ASCII est **ord** sur TI-Nspire.

### I - Expérimentation

1) a) Ouvrir une page **Tableur & listes**.

Dans la colonne A : taper le texte, une lettre par cellule et en respectant les espaces. Ne pas oublier les " avant chaque caractère. Pour les blancs, taper " suivi d'un espace.

*Remarque : Avec le logiciel, sur la calculatrice ou l'ordinateur, les guillemets de « fermeture » sont placés automatiquement, dès l'ouverture.*

Dans la colonne B : dans la cellule grisée, en haut, inscrire = ord(a).

On obtient ainsi les codes ASCII des caractères.

b) Pour coder le texte, inscrire dans la cellule grisée de la colonne C : = mod(7.b,256).

On obtient le message crypté :

220 167 2 37 224 244 17 167 30 223 44 216  
 251 95 44 223 23 51 195 224 188 195 224  
 244 17 167 251 9 51 30 52 224 51 2 224 16  
 244 51 37 224 51 2 224 95 209 167 244

	A	B	C
		=ord(a[])	=mod(7*b[],256)
1	D	68	220
2	a	97	167
3	n	110	2
4	s	115	37
5		32	224
6		108	244

2. Dans la colonne D : taper les nombres constituant le cryptage de la fin de la citation.

Dans la cellule grisée en haut de la colonne E, inscrire la formule : = char(mod(183\*d,256)).

On obtient le message décrypté : **l'infini et deux moins un égal zéro.**

D'où la citation complète de Mignon McLaughlin :

**Dans l'arithmétique de l'amour, un plus un égal l'infini et deux moins un égal zéro.**

	C	D	E
	=ord(a[])	=mod(7*b[]	=char(mod(183*d,256))
1	68	220	244 l
2	97	167	224
3	110	2	223 i
4	115	37	2 n
5	32	224	202 f

## II – Justifications

1. Justification du codage

a) Si  $\mathcal{C}(n) = \mathcal{C}(p)$ , alors  $7n \equiv 7p \pmod{256}$  donc  $7(n - p) \equiv 0 \pmod{256}$ .

b) Comme 7 est premier avec 256, si  $7(n - p) \equiv 0 \pmod{256}$ , alors  $n - p \equiv 0 \pmod{256}$ .  
 Et si  $n - p \equiv 0 \pmod{256}$  alors  $n = p$  car  $n$  et  $p$  sont deux entiers appartenant à  $[0 ; 255]$ .

On peut déduire de ce qui précède que :

$$\mathcal{C}(n) = \mathcal{C}(p) \Leftrightarrow n = p \text{ pour tout } n, \text{ pour tout } p, \text{ entiers de l'intervalle } [0 ; 255].$$

Le codage est donc bien valide.

2. Explication du décodage

a) On vérifie facilement que  $183 \times 7 \equiv 1 \pmod{256}$  ( $183 \times 7 = 1281$  et  $1281 = 5 \times 256 + 1$ ).  
 Donc, pour tout entier  $n$  de l'intervalle  $[0 ; 255]$ , on a :  $183 \times 7n \equiv n \pmod{256}$ .

b) Soit le caractère " $n$ ", soit  $A_n$  son code ASCII et soit  $\mathcal{C}(n)$  son codage. On a, d'après ce qui précède :

$$\begin{aligned} \mathcal{C}(n) &\equiv 7 A_n \pmod{256} ; \\ 183 \times \mathcal{C}(n) &\equiv 183 \times 7 A_n \pmod{256} ; \\ 183 \times \mathcal{C}(n) &\equiv A_n \pmod{256} ; \\ \text{d'où } D(183 \times \mathcal{C}(n)) &= \text{char}(A_n) = "n". \end{aligned}$$

Le décodage est bien valide.