

Cryptographie : séance 2

Groupe 1 : Mardi 8 Novembre

Le but de cette séance est le cryptage et le décryptage d'un message utilisant le « chiffrement à clef secrète ». On utilisera le codage informatique des lettres avec le code ASCII (American Standard Code for Information Interchange) . Comme exemple, le message choisi est une citation de Georg Cantor (mathématicien allemand 1845 – 1918). Ensuite vous décrypterez les deux messages codés sur les papiers retrouvés sur le lieu du crime.

I) Le cryptage

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

Par exemple, le code de A est 65, celui de a est 97, celui de l'espace est 32 Le code utilisé est un entier n tel que

$$0 \leq n \leq 255.$$

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. Code ASCII

a) Vous allez ouvrir une page de tableur afin de coder le message suivant :

L'essence des mathématiques, c'est la liberté.

Vous écrirez le message dans la ligne 1 à partir de la cellule B1 en ne mettant qu'une seule lettre par cellule et vous n'oublierez pas de taper un espace pour séparer les mots. Vous ferez apparaître le message codé avec le code ASCII sur la ligne 2 à partir de la cellule B2. Pour cela écrire dans la formule B2 la formule =code(B1) puis à l'aide du petit carré noir dans le coin en bas à droite de la cellule, étirer cette formule sur la ligne et jusqu'à la fin de votre phrase.

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
1	Message	L		e	s	s	e	n	c	e
2	Codage ASCII (n)	76								

	A	B	C	D	E	F	G	H	I	J
1	Message	L		e	s	s	e	n	c	e
2	Codage ASCII (n)	76		101	115	115	101	110	99	101

b) Le code ASCII ne constituant pas un message bien secret, nous allons dans la ligne 3 du tableur crypter le code ASCII en utilisant le cryptage suivant :

On note f la fonction de cryptage qui, à tout entier n (le code ASCII) appartenant à $[0 ; 255]$ associe le reste de la division euclidienne de $7 \times n$ par 256. On note $f(n)$ ce reste.

La fonction du tableur qui renvoie le reste dans une division euclidienne est « mod(nombre;diviseur) ».

Ecrire dans la cellule B3 la formule =MOD(7*B2;256) puis à l'aide du petit carré noir dans le coin à droite de la cellule, étirer cette formule sur la ligne et jusqu'à la fin de votre phrase.

	A	B	C	D	E	F	G	H	I	J
1	Message	L		e	s	s	e	n	c	e
2	Codage ASCII (n)	76		101	115	115	101	110	99	101
3	Message codé f(n)	20		195	37	37	195	2	181	195

2. Justification du cryptage

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.

On veut donc démontrer que : "si $n \neq p$ alors" Pour fixer les idées, on suppose que $n > p$

- Explique pourquoi pour tout n du code ASCII, il existe un entier k tel que $7n = 256 \times k + f(n)$
- Montrer que si $f(n) = f(p)$ alors 256 divise $7(n - p)$.
- On admet le résultat suivant :

Théorème de Gauss

Si un nombre divise un produit de deux facteurs entiers sans diviser l'un des facteurs, alors il divisera l'autre facteur.

A l'aide de ce résultat, en déduire que $n = p$. Justifier alors que le codage est valide.

II) Le décryptage

1. Expérimentation

Le premier message crypté dans la poche de **Mme NARIENAYFAIRE**:

```

6 195 37 167 223 37 9 207 224 37 9 2 44 58 9 37
202 223 244 244 195 37 23 51 195 58 9 51 37 167 58 195 86
251 223 37 195 167 51 251 9 2 188 195 244 195 94 129
251 167 223 87 143 136 80 199 244 244 195 30 181 216 195 86
27 90 255 227 213 41 83 62 76 227 87 94 16 244 167 181 195
90 195 30 188 51 2 32 241 30 195 2 9 174 244 195 244 195
230 195 51 188 223 115 69 195 16 44 195 251 174 30 195
58 195 30 37 87 122 216 80 80
90 9 37 202 223 244 244 195 37 79 37 195 30 9 2 44 231
27 251 195 199 2 44 223 16 51 181 195

```

Le deuxième message crypté dans la poche de **M VIECOURTE** :

```

213 216 195 30 6 195 167 2 90 255 227 213 41 83 62 76 227
58 9 51 37 167 244 244 195 86 167 58 9 223 30 51 2 195
174 195 244 244 195 37 51 30 16 30 223 37 195 244 195
115 37 195 16 44 195 251 174 30 195 181 216 195 86 58 9 51 37
6 195 37 16 195 30 195 23 51 195 58 9 51 37
167 51 30 195 86 16 244 51 37 188 195 181 9 51 30 167 209 195
188 195 58 167 2 44 58 9 37 202 223 244 244 195 37
195 44 58 9 44 30 195 202 195 251 251 195
34 9 51 174 244 223 195 86 16 167 37 58 9 44 30 195
202 223 244 37 16 9 51 30 51 2 195 202 9 223 37
255 244 2 95 44 167 223 44 16 9 51 30 44 167 2 44
16 167 37 44 30 88 37 244 9 223 2 188 195 44 9 223
199 44 30 195 37 174 223 195 2 44 172 44 150 59 31

```

Pour décrypter ces deux messages, on note g la fonction de décryptage qui, à tout entier k appartenant à $[0 ; 255]$, associe le reste de la division de $183k$ par 256. On note $g(k)$ ce reste.

Rentrer sur une nouvelle feuille de tableur, les restes $g(k)$ en ligne en commençant à A1. Puis sur une nouvelle ligne, rentrer la formule correspondant à la fonction g pour décrypter les messages.

	A	B	C	D	E
1	Message Codé f(n)	195	1	4	23
2	183*f(n)	35685	183	732	4209
3	Reste par 256	101	183	220	113
4	Lettre	e	·	Û	q

2. Justification du décryptage

- Vérifier que le reste de la division euclidienne de 183×7 par 256 est 1.
- En déduire que le reste de la division euclidienne de $183 \times 7n$ par 256 est n (Si $n < 256$).
- Le but de cette question est d'expliquer pourquoi la fonction g , qui à k associe $g(k)$ le reste de la division euclidienne de $183k$ par 256, assure le décryptage attendu.
 - Par rapport à la partie I), que représente k ?
 - Quelle égalité faut-il donc démontrer ?
 - En utilisant le fait que $f(n)$ est le reste de la division de $7n$ par 256, démontrer alors l'égalité et conclure.