TP02 : Cryptographie (DM09)

Enoncé :
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)

Partie 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 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 $0 \leq n \leq 255$

1. **Cryptage**
   a. En utilisant le code ASCII, coder le message suivant :
   Dans les mathématiques 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 apparaitra 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 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.
2. **Décryptage à l'aide de la clef secrète.**
   La fin de la citation de Mignon McLaughlin est crypté 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.

Partie II : Justifications
1. Justification du codage.
   Pour le codage ASCII, deux lettres de l'alphabet sont codées par deux nombres distincts. Sil 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 $C(n)=C(p)$ alors $7(n-p) \equiv 0 \quad [256]$
   b. En déduire que $n=p$. Justifier alors que le codage est valide.
2. Explication du décodage.
   a. Vérifier que $183 \times 7 \equiv 1 \quad [256]$ et en déduire que $183 \times 7n \equiv n\,[256]$
   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 :
1. Envoyer le fichier tableur par mail : vincent.obaton **at** ac-grenoble.fr
2. Rédiger les justifications demandées de la partie II sur une feuille à rendre.

Date :

A rendre pour le **Mardi 12 Mars**.

Tableur

=code("A")

Renvoie le code ASCII de la lettre A majuscule

=car(65)

Renvoie le caractère qui est défini par le code ASCII 65.