EP 139 - 2009 : Cryptage - Décryptage

Auteur du corrigé : Alain SOLEAN **TI-Nspire™ – TI-Nspire™ CAS**

***Avertissement** : ce document a été réalisé avec la version* 1.7

Fichier associé : EP139_2009_Cryptage.tns

1. Le sujet

Sujet 139 de l'épreuve pratique 2009 – Cryptage et décryptage d'un message

Énoncé

***Préliminaire :** on se réfère dans ce sujet à un langage de programmation capable de traiter des nombres entiers et des caractères, ce qui est le cas de la plupart des langages y compris ceux que fournissent certaines calculatrices programmables. En informatique, le code ASCII consiste à associer à chaque caractère un code numérique qui est un entier compris entre* 0 *et* 255*. Ainsi, le code de @ vaut* 64*, celui de A est* 65*, etc.*
***Questions de syntaxe :** dans la plupart des langages de programmation il existe une fonction appelée chr() ou char() ou car() et qui renvoie un caractère à partir de son code ASCII. On entre donc par exemple chr(*65*) pour obtenir la lettre A. La fonction réciproque est souvent nommée asc() ou ord(), de sorte qu'on tape ord("A") ou asc('A') (selon le langage) pour obtenir le nombre* 65*.*
Pour simplifier ce qui suit, nous conviendrons de nous limiter à un sous-alphabet formé des lettres majuscules de A à Z et du caractère @ pour marquer les espaces. Dans ces conditions, la formule ord(c)-64 *renvoie un nombre compris entre* 0 *et* 26 *si la variable c contient une lettre de notre mini-alphabet.*

1. **Codage.**

a) En utilisant le codage décrit ci-dessus, coder le message suivant :

BONJOUR@A@TOUS

On définira un tableau pour ranger les lettres et un autre pour le codage du message.

b) On va crypter (*chiffrer*) le message au moyen de la fonction C qui, à tout n entier appartenant à [0 ; 26] associe le reste $C(n)$ de la division de $13n$ par 27. Adapter la procédure réalisée en **1.a** pour obtenir les restes $C(n)$ correspondant à chaque code n, puis en déduire la lettre correspondante.

2. **Décodage.** Notons D la fonction qui, à tout entier k appartenant à [0 ; 27], associe le reste de la division de $25k$ par 27. À partir des nombres cryptés trouvés précédemment, retrouver le message originel en utilisant la fonction D.

3. **Amélioration.** Le codage proposé ci-dessus est rudimentaire, notamment parce que le caractère d'espacement @ est invariant. On modifie donc la fonction C ainsi : $C(n)$ = reste de la division de $13n + 8$ par 27. Comment faut-il modifier la fonction D ?

4. **Justification du codage.** Pour le codage ASCII, deux lettres de l'alphabet sont codées par deux nombres distincts. Il faut donc s'assurer que le cryptage choisi au **1.b** code deux nombres n et p distincts, compris entre 0 et 26, par deux nombres distincts.

a) Montrer que, si $C(n) = C(p)$ alors 27 divise $13(n – p)$.

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

Production demandée

- Écrire le message codé et le message décodé.
- Justifications demandées aux questions **4.a** et **4.b**.

Compétences évaluées

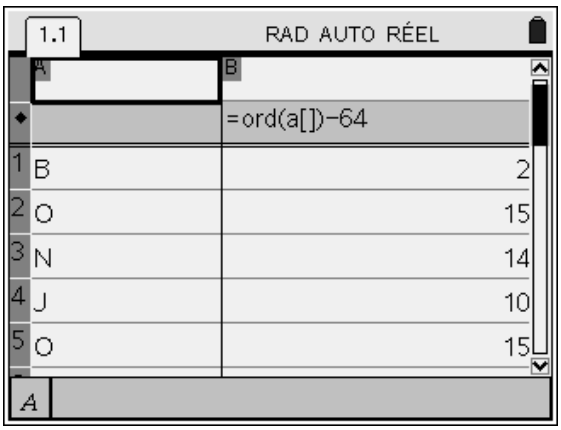
- Utiliser quelques fonctions d'un langage de programmation (reste d'une division euclidienne, etc.).
- Remplir un tableau à une dimension avec des valeurs entières ou des caractères.

- Utiliser les propriétés sur les congruences, la division euclidienne, les nombres premiers entre eux.

2. Corrigé

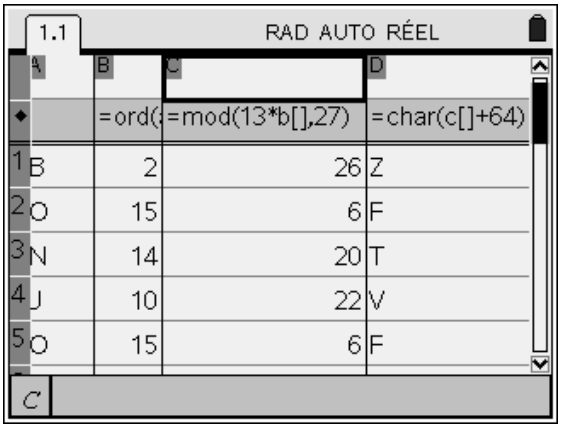
1) Ouvrir une page **Tableur & listes**.

a)Dans la colonne **A**, écrire le texte proposé. Puis dans la cellule grisée de la colonne **B** écrire la formule : **=ord(a[]) – 64** donnant le codage demandé.



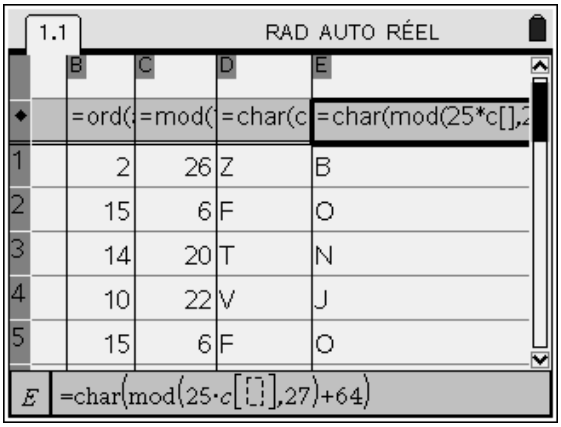
b) Pour crypter le message, écrire dans la cellule grisée de la colonne **C** la formule : **=mod(13*b[],27)** qui va nous donner le codage crypté, puis dans la cellule grisée de la colonne **D** écrire la formule : **=char(c[]+64)** qui nous rend le message crypté suivant :

ZFTVFCR@M@QFCD.

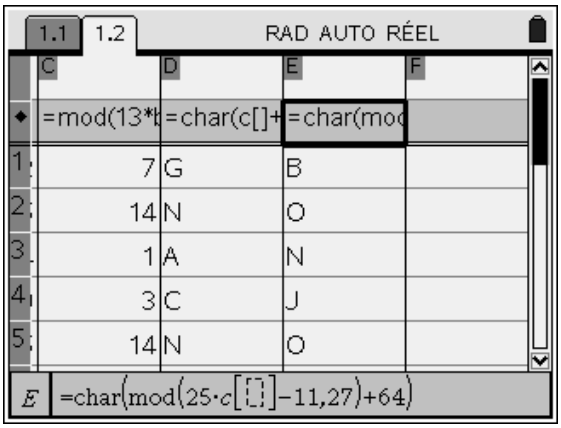


2) Pour décoder le message crypté, il suffit d'écrire dans la cellule grisée de la colonne **E** la formule :

=char(mod(25*c[],27)+64).



3) Si on améliore le codage en modifiant la fonction C avec $C(n)$ = reste de la division de $13n + 8$ par 27 alors il faut modifier la fonction D qui doit devenir $D(k)$ = reste de la division de $25k - 11$ par 27.
L'écran ci-contre le confirme, les formules dans les cellules grisées des colonnes **C** et **E** ayant été modifiées.
Prouvons-le :
Soit le code n on a : $13n + 8 \equiv k \pmod{27}$
d'où : $25(13n + 8) \equiv 25k \pmod{27}$
or $25 \times 13 \equiv 1 \pmod{27}$ et $25 \times 8 \equiv 11 \pmod{27}$
donc : $n + 11 \equiv 25k \pmod{27}$
et enfin : $n \equiv 25k - 11 \pmod{27}$.



4)
a) $C(n) = C(p) \Leftrightarrow 13n \equiv 13p \pmod{27}$
$C(n) = C(p) \Leftrightarrow 13(n - p) \equiv 0 \pmod{27}$
donc 27 divise $13(n - p)$.

b) Comme 13 est premier avec 27 d'après le théorème de Gauss 27 divise $n - p$; les entiers n et p appartenant à l'intervalle [0 ; 26], il s'ensuit que $n - p = 0$.
On a donc $C(n) = C(p) \Leftrightarrow n = p$; le codage est donc bien valide.