

## 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.

Appeler l'examineur pour lui montrer l'écran du logiciel après remplissage.

☞ On s'assurera que la connaissance des fonctions requises n'est pas un obstacle, et on fournira, le cas échéant, des indications pour le remplissage du tableau afin de pouvoir continuer.

- (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.

☞ Le début du message codé a l'allure suivante :

B	O	N	J	O	U	R	@	A	@	T	O	U	S
26	20	22					0						
Z	F	T					@						

Appeler l'examineur pour validation des résultats.

☞ La fonction « reste de division » a un nom variable selon les langages de programmation, ce peut être `mod( , )` ou encore `irem( , )` etc.  
La réponse attendue (sous forme de lettres) est : **ZFTVFCR@M@QFCD**

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`.

Appeler l'examineur pour vérification du résultat.

☞ On laissera ici à l'élève l'initiative de construire seul le décodage en s'appuyant sur la technique ayant permis le codage à la question précédente.  
On pourra se contenter de la liste d'entiers 2,15,14,10,15,21,18,0,1,0,20,15,21,19.

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 ?

Appeler l'examineur pour lui proposer une réponse éventuelle à cette question.

☞ On valorisera la réponse  $\text{mod}(25n + 16; 27)$  (qui peut être trouvée de diverses manières), et plus encore le nouveau codage qui est GNACNKZHUYHYNKL.

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  $13(n - p)$ .

☞ La démonstration est évidemment plus simple si on utilise les propriétés des congruences.

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

☞ Ici le théorème de Gauss est attendu (ainsi que la maîtrise des contraposées)

☞ Si le candidat présente une certaine aisance dans les démonstrations, l'examineur pourra pour le valoriser lui proposer la démonstration du décodage : montrer que pour tout entier  $n$  on a  $13 \times (25n) \equiv n \text{ modulo } 27$  et expliquer pourquoi la fonction D, qui associe à  $k$  le reste de la division de  $25k$  par 27, assure le décryptage attendu.

## 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.

## Cryptage et décryptage d'un message

**Nom:****Prénom:****Note:**

On ne cherchera pas à noter chacune des compétences. Pour établir la note finale on prendra en compte les performances globales du candidat en respectant la grille de lecture suivante:

- La capacité à expérimenter (qui prend en compte de façon dialectique les performances dans l'utilisation des outils et la faculté de proposer des conjectures) doit représenter les trois quarts de la note initiale.
- La capacité à rendre compte des résultats établis à partir de cette expérimentation (démonstration, argumentation, etc.) représentera le quart restant.
- La capacité à prendre des initiatives et à tirer profit des échanges avec l'examineur sera globalement pris en compte de façon substantielle.

Il n'est pas nécessaire qu'une compétence soit totalement maîtrisée pour être considérée comme acquise. Les exemples ci-dessous ne sont pas exhaustifs.

<i>Compétences évaluées</i>	<i>Éléments permettant de situer l'élève (à remplir par l'examineur)</i>
<i>L'élève comprend l'énoncé et est capable de faire quelques essais à la main ou avec sa calculatrice.</i>	
<i>L'élève est capable, avec une aide éventuelle, d'écrire une procédure utilisant les itérations dans le langage de programmation choisi.</i>	
<i>En utilisant son programme, l'élève est capable d'émettre des conjectures.</i>	
<i>L'élève tire profit des indications éventuellement données à l'oral ; ces indications peuvent être des aides logicielles nécessaires pour réaliser ce qu'il ou elle a prévu.</i>	
<i>Suite à un éventuel questionnement oral, l'élève est capable d'exposer sa démarche pour la démonstration.</i>	
<i>L'élève propose une résolution correcte de l'exercice, en tirant profit des résultats observés.</i>	

**Remarques complémentaires :**