Exercice :

Cet exercice met en œuvre sur de petits nombres le premier système de cryptage asymétrique. Dans ce système, une personne destinataire qui veut recevoir des informations confidentielles publie une clé permettant à quiconque de lui envoyer des messages sous forme cryptée. Cependant, seule la personne destinataire peut décrypter les messages à l'aide d'une autre clé connue d'elle seule.

Partie A - Détermination de la clé publique servant au cryptage

1°) Dans tout l'exercice, on choisit deux nombres premiers entre eux : $p = 78$ et $q = 95$.
Justifier que les entiers p et q sont premiers entre eux.

2°) La personne destinataire choisit 5 entiers $b_1 = 45$, $b_2 = 22$, $b_3 = 13$, $b_4 = 4$, $b_5 = 2$.
La clé de cryptage est formée des 5 nombres entiers $(a_1,\ a_2,\ a_3,\ a_4,\ a_5)$ ainsi calculés :
pour tout $i \in \{1,\ 2,\ 3,\ 4,\ 5\}$, $0 \leqslant a_i \leqslant 77$ et $b_i \times q \equiv a_i \pmod{p}$.
Exemple : Pour le calcul de a_1, on calcule $b_1 \times q = 45 \times 95 = 4275$.
Or $4275 \equiv 63 \pmod{p}$, et 63 est bien compris entre 0 et 77. Donc $a_1 = 63$.
Calculer les 4 autres entiers de la clef.

Partie B - Cryptage d'un message

Cette clé, publiée par la personne destinataire, permet à quiconque de lui envoyer un message crypté.
Cette partie va expliquer comment on crypte le message.
On associe d'abord à chaque lettre son rang dans l'alphabet, selon la correspondance suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Pour crypter une lettre :
- on détermine son rang à l'aide du tableau de correspondance précédent ;
- on écrit ce nombre en base 2 sur 5 bits ; on ainsi obtient 5 chiffres $(m_1,\ m_2,\ m_3,\ m_4,\ m_5)$, chaque chiffre étant égal à 0 ou à 1 ;
- on détermine alors la valeur cryptée, égale à la somme $\sigma = a_1m_1 + a_2m_2 + a_3m_3 + a_4m_4 + a_5m_5$.

On remarque qu'une lettre est ainsi cryptée par un nombre entier.

• On veut crypter la lettre « I ».

- Le rang de I est 9 (en base dix) ;
- on écrit ce nombre en base deux sur 5 bits : $\overline{9}^{(10)} = 8 + 1 = \overline{01001}^{(2)}$;
- on calcule la somme $\sigma = 0 \times a_1 + 1 \times a_2 + 0 \times a_3 + 0 \times a_4 + 1 \times a_5 = \ldots$ (écrire le calcul correspondant).

Par quel entier la lettre « I » est-elle cryptée.

• Crypter la lettre « W ».

Réponses :

Partie A 2°) $a_2 = 62$, $a_3 = 65$, $a_4 = 68$ et $a_5 = 34$.
La clé de cryptage est donc $(a_1, a_2, a_3, a_4, a_5) = (63, 62, 65, 68, 34)$.

Partie B

$\sigma = 0 \times 63 + 1 \times 62 + 0 \times 65 + 0 \times 68 + 1 \times 34 = 96$

La lettre « I » est donc cryptée par l'entier 96.

Le rang de W est 23 et $23 = 16 + 4 + 2 + 1$.
23 s'écrit donc en base 2 sous la forme de 5 bits : 10111.
On calcule $\sigma = 1 \times 63 + 0 \times 62 + 1 \times 65 + 1 \times 68 + 1 \times 34 = 230$.
W est crypté par l'entier 230.

Source : Services informatiques aux organisations
épreuve obligatoire
2 13 mai 2019Brevet de technicien supérieur Métropole A. P. M. E. P.