T experts

Devoir pour le mercredi 6 janvier 2021

Numéro : ….. **Prénom et nom :** ……..…… **Note : ….. / 20**

Cet exercice met en œuvre sur de petits nombres le premier système de cryptage asymétrique appelé Merkle-Hellman (MH), défini par Ralph Merkle et Martin Hellman en 1978.
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 entiers naturels premiers entre eux : $p = 78$ et $q = 95$.
Justifier que les entiers p et q sont premiers entre eux.

……..

……..

……..

……..

2°) La personne destinataire choisit cinq entiers naturels $b_1 = 45$, $b_2 = 22$, $b_3 = 13$, $b_4 = 4$, $b_5 = 2$.
La clé de cryptage est le quintuplet $(a_1, a_2, a_3, a_4, a_5)$ d'entiers naturels où a_i désigne le reste de la division euclidienne de $b_i \times q$ par p pour tout $i \in \{1, 2, 3, 4, 5\}$.
Par exemple, pour déterminer a_1, on calcule $b_1 \times q = 45 \times 95 = 4275$ puis on détermine le reste de la division euclidienne de 4275 par p (c'est-à-dire 78). On trouve 63 (on peut par exemple utiliser la calculatrice) donc $a_1 = 63$.
Calculer les quatre 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 deux sur 5 bits ; on obtient ainsi 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 : $\overline{9}^{(10)} = 8 + 1 = \overline{01001}^{(2)}$ puis 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 ».

……..

……..

……..

……..

Ralph Merkle (né en 1952) est un cryptographe américain et chercheur en nanotechnologie.
Martin Hellman (né en 1945) est un cryptologue américain, connu pour ses travaux sur la cryptographie asymétrique.
Le système MH est basé sur le problème du sac à dos (Knapsack problem en anglais).
Il n'est plus utilisé actuellement puisque ce chiffre, ainsi que de nombreuses variantes, a été cassé au début des années 1980 par Adi Shamir.

On peut ajouter le nom de Whitfield Diffie (né le 5 juin 1944), cryptologue américain, qui est avec Martin Hellman et Ralph Merkle, l'un des pionniers de la cryptographie asymétrique (utilisant une paire de clés publique et privée).

Petit résumé sur les clés du chiffrage :

Le destinataire choisit au départ sa clé privée constituée :
- des entiers naturels p et q ;
- du quintuplet $(b_1, b_2, b_3, b_4, b_5)$

Il détermine ensuite sa clé publique constituée du quintuplet $(a_1, a_2, a_3, a_4, a_5)$ dont les éléments sont calculés à partir de la clé privée.

Corrigé du devoir pour le 6-1-2021

Partie A

1°)
Les diviseurs positifs de p sont 1, 2, 3, 6, 13, 26, 39, 78.
Les diviseurs positifs de q sont 1, 5, 19, 95.
Le seul diviseur positif commun à p et q est 1 donc p et q sont premiers entre eux.

On peut aussi considérer la combinaison linéaire $28p - 23q$.
Il s'agit d'une combinaison linéaire de p et q à coefficients entiers relatifs qui est égale à 1 donc p et q sont premiers entre eux.

2°)

$a_1 = 63$
$b_2 \times q = 22 \times 95 = 2090$ donc $a_2 = 62$ (par division euclidienne par 78).
$b_3 \times q = 13 \times 95 = 1235$ donc $a_3 = 65$.
$b_4 \times q \equiv 4 \times 95 = 380$ donc $a_4 = 68$.
$b_5 \times q = 2 \times 95 = 190$ donc $a_5 = 34$.

On $a_2 = 62$, $a_3 = 65$, $a_4 = 68$ 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 deux sur 5 bits : $\overline{10111}^{(2)}$.

On calcule $\sigma = 1 \times 63 + 0 \times 62 + 1 \times 65 + 1 \times 68 + 1 \times 34 = 230$.

La lettre « W » est donc cryptée par l'entier 230.

Problème du sac à dos
À ne pas rendre (mais je conseille de le faire)

Le problème du sac à dos consiste à empiler des objets dans un sac, de manière à atteindre (si possible) un poids total fixé.
Plus formellement, étant donnés des poids entiers naturels P_1, ..., P_n et un but T, il s'agit de trouver b_1, ..., b_n, valant 0 ou 1, tels que $T = b_1P_1 + b_2P_2 + ... + b_nP_n$.
Si la suite des poids P_1, ..., P_n est supercroissante (chaque poids est strictement supérieur à la somme de tous les précédents), alors il existe une méthode de résolution simple (algorithme glouton) :

Algorithme glouton

Pour *i* allant de *n* à 1 **Faire**
  Si $T \geqslant P_i$
    Alors $T \leftarrow T - P_i$ et $b_i \leftarrow 1$
    Sinon
      $b_i \leftarrow 0$
  FinSi
FinPour

Si $T = 0$
  alors $\{b_1, ..., b_n\}$ est solution
  sinon il n'y a pas de solution.
FinSi

Vérifier qu'avec la suite de poids supercroissante $P_1 = 2$, $P_2 = 3$, $P_3 = 6$, $P_4 = 12$ et $T = 15$ on obtient la solution $b_1 = 0$, $b_2 = 1$, $b_3 = 0$, $b_4 = 1$.
Au contraire, si la suite des poids n'est pas supercroissante, le seul algorithme connu consiste à essayer successivement toutes les solutions $(b_1, b_2, ..., b_n)$ possibles. Si la suite est suffisamment longue, c'est un algorithme impraticable.