Cryptographie : la méthode des empilements, dite du « sac à dos »

Dans l'exemple du codage affine, connaître la méthode de codage permet de déterminer la façon de décoder le message. Si une entreprise voulait correspondre de façon secrète avec ses clients, elle devrait donc avoir un codage différent pour chacun d'eux... Ce qui est impensable. Ce problème a été réglé par l'invention en 1976 de la cryptographie à clé publique : la méthode de codage est connue de tous, mais on ne peut pas en déduire la façon de décoder les messages malgré l'utilisation d'ordinateurs performants (pour un temps de calcul raisonnable).
Nous allons étudier un système de codage à clé publique appelé **méthode des empilements** ou **méthode du sac à dos**. Un autre système très connu de cryptage à clé publique est le système RSA (qui sera vu plus tard).

Partie A. Des empilements

On considère cinq boîtes de hauteurs : $b_1 = 13$, $b_2 = 45$, $b_3 = 183$, $b_4 = 315$ et $b_5 = 802$.
On souhaite former une pile de hauteur $H = 511$ en empilant certaines de ces boîtes.

1°) Peut-on prendre la boîte de hauteur 802 ?

2°) Peut-on prendre celle de hauteur 315 ? Peut-on ne pas la prendre ?

3°) Déterminer comment former cette pile. Y-a-t-il plusieurs solutions ?

4°) Décrire en quelques mots l'algorithme utilisé.

5°) En déduire la liste $(x_1, x_2, x_3, x_4, x_5)$ de chiffres 0 ou 1 tels que : $H = x_1b_1 + x_2b_2 + x_3b_3 + x_4b_4 + x_5b_5$.

6°) Quelle particularité de la liste $(b_1, b_2, b_3, b_4, b_5)$ assure l'unicité de cette liste ?

Remarque : cet algorithme peut être programmé sur une calculatrice.

Partie B. Cryptage

Pour coder dans un mot, il faut savoir coder chacune de ses lettres. Nous repérerons chaque lettre par son rang dans l'alphabet (de 1 à 26), rang écrit en base 2. On fera alors correspondre à chaque lettre une liste $m = (m_1, m_2, m_3, m_4, m_5)$ de cinq chiffres 0 ou 1.
Par exemple H, la huitième lettre, correspond à $m = (0,\ 1,\ 0,\ 0,\ 0)$ car huit s'écrit $\overline{1000}$ (ne pas oublier la « barre » au dessus des chiffres) en base 2, c'est-à-dire $8 = 1\times 2^3 + 0\times 2^2 + 0\times 2^1 + 0\times 2^0$.

1°) Choisir une lettre et déterminer la liste *m* associée.

2°) On ne peut pas envoyer directement *m* comme lettre codée, cette suite de 0 et de 1 faisant clairement penser à un codage binaire. On va donc coder *m* de la façon suivante : l'entreprise a rendu publique sa clé de codage. Il s'agit de la liste : $(a_1,\ a_2,\ a_3,\ a_4,\ a_5) = (1837,\ 945,\ 3567,\ 1095,\ 2398)$.
Le message codé est alors $M = a_1m_1 + a_2m_2 + a_3m_3 + a_4m_4 + a_5m_5$.

Calculer M pour la lettre choisie à la question 1°).