Corrigé du devoir 2.

Le problème du sac à dos est le suivant: on dispose d'un sac à dos vide et de n objets de poids respectifs $a_1, ..., a_n$. Quels objets doit-on mettre dans le sac à dos pour obtenir un poids total égal à k, i.e., existe-t-il une suite $(x_1, ..., x_n)$ de valeurs booléennes telles que $\sum_{i=1}^{n} x_i a_i = k$?

C'est un problème très difficile à résoudre sauf dans le cas où la suite $(a_1, ..., a_n)$ et supercroissante, i.e., si pour tout entier $1 \leq i \leq n$, on a

$$\sum_{j=1}^{i} a_j < a_i$$

1) Vérifier que la suite $(1, 3, 6, 13, 28, 63, 142, 290, 601, 1231, 2543, 5100)$ est supercroissante.
$1 < 3$
$1 + 3 = 4 < 6$
$1 + 3 + 6 = 10 < 13$
$1 + 3 + 6 + 13 = 23 < 28$
$1 + 3 + 6 + 13 + 28 = 51 < 63$
$1 + 3 + 6 + 13 + 28 + 63 = 114 < 142$
$1 + 3 + 6 + 13 + 28 + 63 + 142 = 256 < 290$
$1 + 3 + 6 + 13 + 28 + 63 + 142 + 290 = 546 < 601$
$1 + 3 + 6 + 13 + 28 + 63 + 142 + 290 + 601 = 1147 < 1231$
$1 + 3 + 6 + 13 + 28 + 63 + 142 + 290 + 601 + 1231 = 2378 < 2543$
$1 + 3 + 6 + 13 + 28 + 63 + 142 + 290 + 601 + 1231 + 2543 = 4921 < 5100$

2) Montrer qu'il y a une unique solution au problème du sac à dos pour $k = 2931$.
On cherche une suite $(x_1, ..., x_{12})$ de valeurs booléennes ($x_i \in \{0, 1\}$) telle que
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 + 28 \times x_5 + 63 \times x_6 + 142 \times x_7 + 290 \times x_8 + 601 \times x_9 + 1231 \times x_{10} + 2543 \times x_{11} + 5100 \times x_{12} = 2931$.
Comme $2931 < 5100$, on doit avoir $x_{12} = 0$,
Comme $1+3+6+13+28+63+142+290+601+1231 = 2378 < 2931$ et $2543 < 2931$, on doit avoir $x_{11} = 1$ et on est ramené au problème suivant: trouver une suite $(x_1, ..., x_{10})$ telle que:
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 + 28 \times x_5 + 63 \times x_6 + 142 \times x_7 + 290 \times x_8 + 601 \times x_9 + 1231 \times x_{10} = (2931 - 2543) = 388$
Comme $388 < 601$ et $388 < 1231$, on doit avoir $x_9 = x_{10} = 0$.
Comme $1 + 3 + 6 + 13 + 28 + 63 + 142 = 256 < 388$ et $290 < 388$, on doit avoir $x_8 = 1$ et on est ramené au problème suivant: trouver une suite $(x_1, ..., x_7)$ telle que:
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 + 28 \times x_5 + 63 \times x_6 + 142 \times x_7 = (388 - 290) = 98$.
Comme $98 < 142$, on doit avoir $x_7 = 0$.
Comme $1 + 3 + 6 + 13 + 28 = 51 < 98$ et $63 < 98$, on doit avoir $x_6 = 1$ et on est ramené au problème suivant: trouver une suite $(x_1, ..., x_5)$ telle que:
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 + 28 \times x_5 = (98 - 63) = 35$.
Comme $1+3+6+13 = 23 < 35$ et $28 < 35$, on doit avoir $x_5 = 1$ et on est ramené au problème suivant: trouver une suite $(x_1, ..., x_4)$ telle que:
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 = (35 - 28) = 7$.
ce problème a un unique solution qui est $(1, 0, 1, 0)$.

Donc, il existe une unique solution au problème du sac à dos pour 2931 et pour la suite de la question 1), cette solution est: $2931 = 1 + 6 + 28 + 63 + 290 + 2543$.

3) Montrer qu'il n'y a pas de solution pour $k = 3090$.
On cherche une suite $(x_1, ..., x_{12})$ de valeurs booléennes ($x_i \in \{0, 1\}$) telle que
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 + 28 \times x_5 + 63 \times x_6 + 142 \times x_7 + 290 \times x_8 + 601 \times x_9 + 1231 \times x_{10} + 2543 \times x_{11} + 5100 \times x_{12} = 3090$.
Comme $3090 < 5100$, on doit avoir $x_{12} = 0$,
Comme $1+3+6+13+28+63+142+290+601+1231 = 2378 < 3090$ et $2543 < 3090$, on doit avoir $x_{11} = 1$ et on est ramené au problème suivant: trouver une suite $(x_1, ..., x_{10})$ telle que:
$1 \times x_1 + 3 \times x_2 + 6 \times x_3 + 13 \times x_4 + 28 \times x_5 + 63 \times x_6 + 142 \times x_7 + 290 \times x_8 + 601 \times x_9 + 1231 \times x_{10} = (3090 - 2543) = 547$
Mais, alors comme $547 < 601$ et $547 < 1231$, on doit avoir $x_9 = x_{10} = 0$.
Mais, par ailleurs, on a $1 + 3 + 6 + 13 + 28 + 63 + 142 + 290 = 546 < 547$. Donc, il n'existe pas de telle suite $(x_1, ..., x_{10})$. Le problème du sac à dos pour 3090 et pour la suite de la question 1) n'a pas de solution.

4) Donner un algorithme de résolution du problème du sac à dos lorsque $(a_1, ..., a_n)$ est supercroissante.

On commence par comparer les valeurs de k et de a_n :
si $k < a_n$, on pose $x_n = 0$.
sinon, on doit poser $x_n = 1$: en effet, comme la suite est supercroissante, on a alors $\sum_{i=1}^{n-1} a_i < k$ et si on veut écrire k comme la somme des a_i on est obligé de prendre a_n. Il suffit alors de résoudre le problème du sac à dos pour la suite $(a_1, ..., a_{n-1})$, et pour l'entier naturel $k - a_n$.

5) a) Montrer que la suite supercroissante qui ait les plus petits termes a_i est définie par $a_i = 2^{i-1}$.

On considère la suite $(a_i)_{i \in \mathbb{N}^*}$ définie par $a_i = 2^{i-1}$, c'est bien un suite supercroissante: pour tout $k \in \mathbb{N}^*$, on a $\sum_{i=1}^{k-1} a_i = 1 + 2 + 2^2 + ... + 2^{k-1} = 2^k - 1 = a_k - 1$, d'où, $\sum_{i=1}^{k-1} a_i < a_k$.

Soit $(a_i)_{i \in \mathbb{N}}$ la suite supercroissante qui ait les plus petits termes $a_i \in \mathbb{N}^*$, alors vérifions par récurrence sur i que $a_i = 2^{i-1}$ pour tout $i \in \mathbb{N}^*$:
$a_1 = 1$,
a_2 est le plus petit entier k tel que $k > a_1$ donc, $a_2 = 2$,
a_3 est le plus petit entier k tel que $k > a_1 + a_2 = 3$ donc $a_3 = 4 = 2^2$,
Supposons que pour $i \geq 3$, on ait $a_j = 2^{j-1}$ pour tout $j \leq i$, alors a_{i+1} est le plus petit entier k tel que $k > \sum_{j=1}^{i} a_j = \sum_{j=1}^{i} 2^{j-1} = 2^i - 1$, donc $a_{i+1} = 2^i$. En appliquant le principe de récurrence, on conclut que $a_i = 2^{i-1}$ pour tout $i \in \mathbb{N}^*$.

b) Montrer que si la suite supercroissante $(a_1, ..., a_n)$ est définie par $a_i = 2^{i-1}$, alors le problème du sac-à-dos a une solution pour tout entier $k \leq \sum_{i=1}^{n} a_i$ et que ce n'est plus le cas pour les autres suites supercroissantes.
On considère la suite supercroissante $(a_1, ..., a_n)$ définie par $a_i = 2^{i-1}$. Soit k un entier tel que $0 \leq k \leq \sum_{i=1}^{n} a_i < 2^i$. Alors, l'écriture de k dans la base 2 fournit une solution au problème de sac-à-dos.

Si $(b_1, ..., b_n)$ est une suite supercroissante différente de $(a_1, ..., a_n)$, alors:
- soit $b_1 \neq 1$ et il n'y a pas de solution pour le problème du sac-à-dos pour la suite $(b_1, ..., b_n)$ et l'entier $k = 1$.
- soit $b_1 = 1$, mais il existe $i \in \{1, ..., n-1\}$ tel que $b_{i+1} > b_1 + b_2 + ... + b_i + 1$ et il n'y a pas de solution pour le problème du sac-à-dos pour la suite $(b_1, ..., b_n)$ et l'entier $k = b_1 + b_2 + ... + b_i + 1$.

Le cryptosystème de Merkle et Hellman (1978) est basé sur le problème du sac à dos:
Alice choisit une suite supercroissante $(a_1, ..., a_n)$ et un entier $N > \sum_{i=1}^{n} a_i$,
Alice choisit au hasard un entier d compris entre 1 et $N-1$ et premier avec N (et non avec $N-1$, erreur d'énoncé!!),
Alice choisit au hasard une permutation de l'ensemble $\{1, ..., n\}$,
Alice calcule $b_i = a_{\sigma(i)} d \bmod N$ pour tout $i \in \{1, ..., n\}$:
Clé publique d'Alice: $(b_1, ..., b_n)$,
Clé privée d'Alice: $((N, d, \sigma, (a_1, ..., a_n))$.
5) Bob veut envoyer à Alice un message qui est une suite $x_1, ..., x_n$ de n bits. Comment va-t-il s'y prendre pour chiffrer ce message? Pourquoi le message chiffré est-il difficile à déchiffrer?

Bob calcule l'entier $c = \sum_{i=1}^{n} x_i b_i$ et l'envoie à Alice. Comme la suite $(b_1, ..., b_n)$ n'est pas supercroissante, le problème de sac à dos pour cette suite et pour l'entier k est difficile à résoudre. Donc, il est difficile de retrouver $x_1, ..., x_n$.

6) Alice reçoit le message chiffré c. Quels calculs fait-elle pour déchiffrer le message?

Alice a reçu $c = \sum_{i=1}^{n} x_i b_i = \sum_{i=1}^{n} x_i a_{\sigma(i)} d \bmod N$.
Or d est inversible modulo N car il est premier à N, soit $e = d^{-1} \bmod N$.
Alice calcule $k = ec \bmod N = \sum_{i=1}^{n} x_i a_{\sigma(i)} \bmod N = \sum_{i=1}^{n} x_i a_{\sigma(i)}$ car $N > \sum_{i=1}^{n} a_i$.
Ensuite Alice résout le problème de sac-à-dos pour la suite $(a_1, ..., a_n)$ et l'entier k. Elle obtient une suite booléenne $(y_1, ..., y_n)$ telle que $\sum_{i=1}^{n} x_i a_{\sigma(i)} = \sum_{i=1}^{n} y_i a_i$. Donc, elle retrouve la suite x_i car $x_i = y_{\sigma(i)}$ pour tout $i \in \{1, ..., n\}$.

7) Application numérique:

$n = 5$, $(a_i) = (2, 5, 11, 23, 55)$, $N = 113$, $d = 27$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$.

Quelle est la clé publique d'Alice?
On peut remarquer que 27 et 113 sont premiers entre eux et que $2+5+11+23+55 = 96 < 113$.

Alice calcule la suite $(b_1, ..., b_5)$ de la façon suivante:
$b_1 = a_{\sigma(1)} \times 27 \bmod 113 = a_2 \times 27 \bmod 113 = 5 \times 27 \bmod 113 = 22$
$b_2 = a_{\sigma(2)} \times 27 \bmod 113 = a_5 \times 27 \bmod 113 = 55 \times 27 \bmod 113 = 16$
$b_3 = a_{\sigma(3)} \times 27 \bmod 113 = a_3 \times 27 \bmod 113 = 11 \times 27 \bmod 113 = 71$
$b_4 = a_{\sigma(4)} \times 27 \bmod 113 = a_1 \times 27 \bmod 113 = 2 \times 27 \bmod 113 = 54$
$b_5 = a_{\sigma(5)} \times 27 \bmod 113 = a_4 \times 27 \bmod 113 = 23 \times 27 \bmod 113 = 56$
Donc la clé publique d'Alice est $(22, 16, 71, 54, 56)$.

Bob veut envoyer le message $m = (10101)$. Calculer c.
$c = b_1 + b_3 + b_5 = 22 + 71 + 56 = 149$.

Vérifier en faisant les mêmes calculs qu'Alice, qu'elle retrouve bien m.

Tout d'abord, Alice calcule $e = d^{-1} \bmod 113$ en utilisant l'algorithme d'Euclide:
$113 = 27 \times 4 + 5$, $27 = 5 \times 5 + 2$, $5 = 2 \times 2 + 1$,
On obtient l'identité de Bezout suivante: $113 \times 11 - 27 \times 46 = 1$ donc $e = -46 \bmod 113 = 67 \bmod 113$.

Alice calcule $k = e \times c \bmod 113 = 67 \times 149 \bmod 113 = 39$.

Alice cherche ensuite une solution au problème de sac-à-dos pour $k = 39$ et la suite supercroissante $(2, 5, 11, 23, 55)$.
On cherche une suite $(y_1, y_2, y_3, y_4, y_5)$ de valeurs booléennes ($y_i \in \{0, 1\}$) telle que
$2 \times y_1 + 5 \times y_2 + 11 \times y_3 + 23 \times y_4 + 55 \times y_5 = 39$.

Comme $39 < 55$, on doit avoir $y_5 = 0$,
Comme $2 + 5 + 11 = 18 < 39$ et $23 < 39$, on doit avoir $y_4 = 1$ et on est ramené au problème suivant: trouver une suite (y_1, y_2, y_3) telle que:
$2 \times y_1 + 5 \times y_2 + 11 \times y_3 = (39 - 23) = 16$, $(0, 1, 1)$ est une solution.

On obtient donc $(y_1, y_2, y_3, y_4, y_5) = (0, 1, 1, 1, 0)$. Et on retrouve $(x_1, x_2, x_3, x_4, x_5)$ de la façon suivante:
$x_1 = y_{\sigma(1)} = y_2 = 1$
$x_2 = y_{\sigma(2)} = y_5 = 0$
$x_3 = y_{\sigma(3)} = y_3 = 1$
$x_4 = y_{\sigma(4)} = y_1 = 0$
$x_5 = y_{\sigma(5)} = y_4 = 1$
D'où, $(x_1, x_2, x_3, x_4, x_5) = (1, 0, 1, 0, 1)$.

Le cryptosystème de Merkle et Hellman a été cassé par Shamir en 1982.