FIGURE 5.11
Subset sum problem

Problem Instance $I = (s_1, \ldots s_n, T)$, where $s_1, \ldots s_n$ and T are positive integers. The s_i's are called *sizes* and T is called the *target sum*.

Question Is there a 0-1 vector $\mathbf{x} = (x_1, \ldots, x_n)$ such that

$$\sum_{i=1}^{n} x_i s_i = T?$$

superincreasing

$$s_j > \sum_{i=1}^{j-1} s_i$$

FIGURE 5.13
Merkle-Hellman Knapsack Cryptosystem

Let $\mathbf{s} = (s_1, \ldots, s_n)$ be a superincreasing list of integers, let $p > \sum_{i=1}^{n} s_i$ be prime, and let $1 \leq a \leq p-1$. For $1 \leq i \leq n$, define

$$t_i = as_i \bmod p,$$

and denote $\mathbf{t} = (t_1, \ldots, t_n)$. Let $\mathcal{P} = \{0,1\}^n$, $C = \{0, \ldots, n(p-1)\}$, and let

$$\mathcal{K} = \{(\mathbf{s}, p, a, \mathbf{t})\},$$

where $\mathbf{s}$, p, a, and $\mathbf{t}$ are constructed as described above. $\mathbf{t}$ is public, and p, a and $\mathbf{s}$ are secret.

For $K = (\mathbf{s}, p, a, \mathbf{t})$, define

$$e_K(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i t_i.$$

For $0 \leq y \leq n(p-1)$, define $z = a^{-1}y \bmod p$ and solve the subset problem $(s_1, \ldots, s_n, z)$, obtaining $d_K(y) = (x_1, \ldots, x_n)$.

FIGURE 5.12
Algorithm for solving a superincreasing instance of the subset sum problem

```
1.  for i = n downto 1 do
2.      if T ≥ s_i then
3.          T = T − s_i
4.          x_i = 1
5.      else
6.          x_i = 0
7.  if T = 0 then
8.      X = (x_1, ..., x_n) is the solution
9.  else
10.     there is no solution.
```

$$\mathbf{s} = (2, 5, 9, 21, 45, 103, 215, 450, 946)$$

is the secret superincreasing list of sizes. Suppose $p = 2003$ and $a = 1289$. Then the public list of sizes is

$$\mathbf{t} = (575, 436, 1586, 1030, 1921, 569, 721, 1183, 1570).$$

Now, if Alice wants to encrypt the plaintext $x = (1, 0, 1, 1, 0, 0, 1, 1, 1)$, she computes

$$y = 575 + 1586 + 1030 + 721 + 1183 + 1570 = 6665.$$

When Bob receives the ciphertext y, he first computes

$$\begin{aligned} z &= a^{-1}y \bmod p \\ &= 317 \times 6665 \bmod 2003 \\ &= 1643. \end{aligned}$$

Then Bob solves the instance $I = (\mathbf{s}, z)$ of the **Subset Sum** problem using the algorithm presented in Figure 5.12. The plaintext $(1, 0, 1, 1, 0, 0, 1, 1, 1)$ is obtained. □