

# Hátizsák rendszerek

## 1. A hátizsák probléma

Adott egy  $V$  térfogatú hátizsák, valamint adott  $k$  csomag, melyek térfogata rendre  $v_0, v_1, \dots, v_{k-1}$ . A csomagok közül szeretnénk néhányat kiválasztani, hogy telepakoljuk vele a hátizsákot (feltételezzük, hogy a pakolás hézagmentesen elvégezhető). Azaz keressünk egy olyan  $k$ -bites  $M = (\varepsilon_{k-1}\varepsilon_{k-2}\dots\varepsilon_1\varepsilon_0)_2$  számot (tehát  $\varepsilon_i \in \{0, 1\}$ ), melyre

$$\sum_{i=0}^{k-1} \varepsilon_i v_i = V.$$

A megoldáshoz sajnos nem áll rendelkezésünkre "igazán jó" algoritmus, pontosabban fogalmazva a használt eljárások gyakorlatilag az összes eset végignézését jelentik. Ebből következik, hogy nagy  $k$  és  $V$  értékek esetén belátható időn belül nem lehet megoldáshoz jutni.

## 2. Szupernövekvő hátizsák probléma

Vizsgáljuk most meg az alapfeladat egy olyan variánsát, melynek megoldása módszerében és hatékonyságában is eltér az alapfeladattól. Ezen a különbségen fog alapulni a hátizsákos nyilvános kulcsú titkosítási rendszer.

**Definíció.** A  $v_0, v_1, \dots, v_{k-1}$  sorozat szupernövekvő, ha minden elem nagyobb mint az összes őt megelőző elem összege, azaz bármely  $s = 1, \dots, k-1$  esetén

$$\sum_{i=0}^{s-1} v_i < v_s.$$

**Példa.** A 2, 3, 6, 15, 30 sorozat szupernövekvő, mert  $3 > 2$ ,  $6 > 2 + 3$ ,  $15 > 2 + 3 + 6$  és  $30 > 2 + 3 + 6 + 15$ .

Könnyű előállítani szupernövekvő sorozatot egy tetszőleges pozitív tagú segédsorozat felhasználásával. Éppen a segédsorozat tagjai szolgáltatják a különbséget az első néhány tag összege és a következő tag között. Jelölje  $a_0, a_1, \dots, a_{k-1}$  a segédsorozatot.

Legyen  $v_0 = a_0$ , továbbá  $v_1 = v_0 + a_1$ ,  $v_2 = v_0 + v_1 + a_2$ , és így tovább, míg végül  $v_{k-1} = v_0 + v_1 + \dots + v_{k-2} + a_{k-1}$ . Világos, hogy az  $a_0, a_1, \dots, a_{k-1}$  sorozat pozitivitása miatt a fenti módon gyártott  $v_0, v_1, \dots, v_{k-1}$  sorozat szupernövekvő.

**Példa.** Legyen 3, 1, 2, 1, 2, 4 az előre adott segédsorozat. Ekkor

$$\begin{aligned} v_0 &= \boxed{3}, \\ v_1 &= 3 + \boxed{1} = 4, \\ v_2 &= 3 + 4 + \boxed{2} = 9, \\ v_3 &= 3 + 4 + 9 + \boxed{1} = 17, \\ v_4 &= 3 + 4 + 9 + 17 + \boxed{2} = 35, \\ v_5 &= 3 + 4 + 9 + 17 + 35 + \boxed{4} = 72. \end{aligned}$$

A bekeretezett számok a segédsorozat tagjainak felhasználását emelik ki, míg a dőlttel szedett számok a végeredményt, azaz a szupernövekvő sorozat tagjait mutatják.

Tegyük most fel, hogy a csomagok térfogatai egy szupernövekvő sorozat tagjai. Vegyük észre, hogy ebben a speciális esetben a hátzísák probléma megoldása nagyon könnyűvé válik. Rendezzük térfogatuk szerint csökkenő sorrendbe a csomagokat:  $v_{k-1} > v_{k-2} > \dots > v_0$ , és kezdjük el betenni őket a hátzísákba.

- Ha a soron következő  $v_i$  térfogatú csomag nem fér bele, akkor vegyük az utána következő  $v_{i-1}$  térfogatú csomagot;
- Ha soron következő  $v_i$  térfogatú csomag belefér, akkor őt kötelező beletenni, hiszen az utána következő összes többi csomag térfogata együttesen is kevesebb  $v_i$ -nél, tehát  $v_i$  mellőzése esetén biztosan nem telik meg a hátzísák.

Végül vagy megtelik a hátzísák vagy elfogynak a csomagok anélkül, hogy tele tudnánk rakni a hátzísákat.

### 3. MERKLE-HELLMAN rendszer

Legyenek az elküldendő üzenet egységei  $k$ -bites számként ábrázolva.

1. A felhasználók mindegyike választ magának egy  $k + 1$  elemű szupernövekvő sorozatot. Legyen például az  $\mathcal{A}$  felhasználó sorozata  $v_0, v_1, \dots, v_{k-1}, m = v_k$ .
2. Ezután  $\mathcal{A}$  egyszerű próbálgatással keres egy  $m$ -hez relatív prím  $a$  számot, tehát  $\gcd(a, m) = 1$ .
3. Majd  $\mathcal{A}$  meghatározza  $a$  multiplikatív inverzét modulo  $m$ , jelölje ezt  $b$ , azaz  $a \cdot b \equiv 1 \pmod{m}$ .
4. Legyen minden  $i = 0, 1, \dots, k - 1$  esetén  $w_i \equiv a \cdot v_i \pmod{m}$ , ahol  $0 \leq w_i < m$ . A  $w_0, w_1, \dots, w_{k-1}$  sorozat nem lesz szupernövekvő, kivéve néhány extrém esetet.

$\mathcal{A}$  nyilvános kulcsa a  $\{w_i\}_{i=0}^{k-1}$  sorozat lesz, a többi adat titkos.

**Üzenetküldés.** Ha valaki szeretne  $\mathcal{A}$  számára egy üzenetet küldeni, akkor kikeresi a nyilvánántartásból  $\mathcal{A}$  nyilvános kulcsát. Legyen a nyílt üzenet  $M = (\varepsilon_{k-1}\varepsilon_{k-2} \dots \varepsilon_0)_2$ , amelyből a nyilvános kulcs segítségével

$$V = \sum_{i=0}^{k-1} \varepsilon_i w_i.$$

A  $V$  titkos üzenetet egy kommunikációs csatornán eljuttatják  $\mathcal{A}$ -nak. Amennyiben valaki  $V$  birtokába jut, akkor  $\{w_i\}$  ismeretében egy hátzísák problémát kellene megoldania az üzenet megfejtéséhez, ami túlonatúl időigényes.

**Az üzenet megfejtése.** Miután  $\mathcal{A}$  megkapja a  $V$  titkos üzenetet, előveszi  $b$  és  $m$  titkos kulcsát, majd kiszámítja a  $b \cdot V \pmod{m}$  számot. Mivel

$$bV = b \sum_{i=0}^{k-1} \varepsilon_i w_i = \sum_{i=0}^{k-1} b\varepsilon_i w_i \equiv \sum_{i=0}^{k-1} \varepsilon_i \overbrace{b a}^{\equiv 1} v_i \equiv \sum_{i=0}^{k-1} \varepsilon_i v_i \pmod{m},$$

így ahhoz, hogy  $\mathcal{A}$  megfejtse a kapott üzenetet, csak egy szupernövekvő hátizsák problémát kell megoldania, ami nem okoz számára problémát. Tehát a  $\sum_{i=0}^{k-1} \varepsilon_i v_i$  szám, valamint a  $\{v_i\}_{i=0}^{k-1}$  szupernövekvő sorozat ismeretében  $\mathcal{A}$  kiszámolja az

$$\varepsilon_{k-1}, \varepsilon_{k-2}, \dots, \varepsilon_0$$

együtthatókat, ahonnan  $M = (\varepsilon_{k-1}\varepsilon_{k-2}\dots\varepsilon_0)_2$ .

**Példa.** Legyen  $k = 5$ ,  $\{v_i\} : 2, 3, 7, 15, 31$ . Legyen továbbá  $m = 61$  és  $a = 17$ . Az Euklideszi algoritmus alkalmazásával könnyen megkaphatjuk, hogy  $b = 18$ .

$$(w_0, w_1, w_2, w_3, w_4) = (34, 51, 58, 11, 39) \equiv (17 \cdot 2, 17 \cdot 3, 17 \cdot 7, 17 \cdot 15, 17 \cdot 31) \pmod{61}.$$

Az elküldendő üzenet  $M = (10110)_2$ . Ekkor  $51 + 58 + 39 = 148 = V$  lesz a titkosított üzenet. Ha a címzett megkapja, akkor kiszámolja, hogy  $148 \cdot 18 \equiv 41 \pmod{61}$ . Végül  $41 = 31 + 7 + 3$ , amelyből  $M = (10110)_2$ .

**Megjegyzés.** SHAMIR 1982-ben megmutatta, hogy bár  $\{w_i\}$  nem szupernövekvő, de az üzenet feltöréséhez jól ki lehet használni azt a tényt, hogy szupernövekvő sorozatból származik. Ezért úgy tesz biztonságosabbá a rendszert, hogy az  $(m, a)$  pár alkalmazása helyett dupla titkosítást használnak valamely  $(m_1, a_1)$  és  $(m_2, a_2)$  párokat felhasználva.

#### 4. Részletesen kidolgozott mintapélda

A mintapélda a *mintafeladatok.pdf* fileban található.