11 - Kryptosystem plecakowy

Thursday, 20 June 2024 17:27

Subset-Sum

$V = \{v_1, \dots, v_n\}$, liczba s

Znaleźć $A \subseteq V$: $\sum A = s$

NP-zupełny, chyba, że ciąg jest nadrosnący:

$v_k > v_1 + \dots + v_{k-1}$

Weźmy nadrosnący ciąg V i bosową liczbę $M > \sum v_i$

oraz a względnie pierwsze z M.

Niech $(w_1, \dots, w_n)$: $w_i = a \cdot v_i \pmod M$

- $E = (w_1, \dots, w_n)$ $D = (a, m)$

Zaszyfrowanie n-bitowej liczby B: $s = \sum B_i \cdot w_i$

Żeby odszyfrować wystarczy przemnożyć przez a^{-1}
i otrzymujemy nadrosnący subset-sum.

Dla tej klasy ciągów, subset-sum jest prosty :)