Lab 4 (Knapsack)

18 February 2022 13:13

Knapsack ① 1st key generation algorithm

② Asymm. key encryption

③ Developed by Ralph Merkle & Martin Hellman

Public key = Hard K.s

Private key = ~~Private~~ Easy K.s

Algorithm:

I select a random set of Private keys denoted as D

$$D = \{1, 2, 4, 10, 20, 40\}$$

Ascending order

II a. Select value of a variable M such that it should be greater than sum of all elements in D

$$M = 110$$

b Select value of variable n such that there should not be common factor of M.

$$n = 3$$

III Calculate the public key denoted as E

$$E = (D_i * n \bmod M)$$

eg $E = 1 * 3 \bmod 110 = 3$ $= 10 * 3 \bmod 110 = 30$

$= 2 * 3 \bmod 110 = 6$ $= 20 * 3 \bmod 110 = 60$

$= 4 * 3 \bmod 110 = 12$ $= 40 * 3 \bmod 110 = 10$

$E \{3, 6, 12, 30, 60, 10\}$ $D = \{1, 2, 4, 10, 20, 40\}$

eg Plain text = { 110010 101011 }

C.T 1: 1 1 0 0 1 0

E : 3 6 12 30 60 10

$3 + 6 + 0 + 0 + 60 + 0 = 69$

C.T 2: 1 0 1 0 1 1

E : 3 6 12 30 60 10

$3 + 0 + 12 + 0 + 60 + 10 = 85$

$\frac{3 + 6 + 0 + 0 + 60 + 0}{3 + 0 + 12 + 0 + 60 + 10} = \frac{69}{85}$

Ciphertext (69, 85)

eg Ciphertext (69, 85)

Decryption $n^{-1} \bmod m = 1$ → $n^{-1} \cdot x \cdot \bmod m = 1$

$\therefore 3 \cdot x \bmod 110 = 1$

$x = 37$

$CT_1 = 69 \times 37 \bmod 110 = 23$

$CT_2 = 85 \times 37 \bmod 110 = 65$

$D = \{1, 2, 4, 10, 20, 40\}$

$PT_1 = \{1\ 0\ 0\ 1\ 0\}$

$PT_2 = \{1\ 0\ 1\ 0\ 1\ 1\}$

$P.T = \{1\ 1\ 0\ 0\ 1\ 0 \quad 1\ 0\ 1\ 0\ 1\ 1\}$

$PT. = 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0$

$E = \{1, 6, 8, 15, 24\}$

Convert this into C.T.