Assignment-2
Cryptography Network Security

B192589
P. Anjali
Roll No: 58
class: CS 214

Knapsack algorithm

It is given by Hellman

Asymmetric key Cryptography

eg: weights = (1, 6, 8, 15 and 24)

In general knapsack, we select weights to achieve a sum. if we want sum = 30

we select 1, 6, 8 and 15

Let plaintext = 1 0 0 1 1

× × × × ×

(*) 1 6 8 15 24

1 + 0 + 0 + 15 + 24

↓

⇒ 40

1 1 0 1 0

× × × × ×

1 6 8 15 24

1 + 6 + 0 + 15 + 0

↓

⇒ 22

CT = plan text × corresponding weights

∴ CT = 40 22

* Key Generation: Assymmetric key

1) Public key (Hard knapsack)

2) Private key (easy knapsack)

↓

done first (i.e we find private key first)

eg: {1, 2, 4, 9, 20, 40}

Weights are always in increasing order

1) First, find private key (Assume)

D = {1, 2, 4, 10, 20, 40} → private key

Select (2) number "n" and "m"

Condition:

m > sum of all no.s in sequence

sum = 77 m = 110 let

40}

2 n = select so that it has no common factor with m

∴ let $\boxed{n=31}$

⇒ List out factors of 110, 31 don't have common factor except one (take like that)

now, $\boxed{(D_i \times n) \bmod m}$ ∀ elements in n.

D_i ⇒ First number in list.

$(1\times31) \bmod 110 = 31$ ⇒ {1, 2, 4, 10, 20, 40} initial

$(2\times31) \bmod 110 = 62$ ⇒ {31, 62, 14, 90, 70, 30}

$(4\times31) \bmod 110 = 14$ ↓ public key

$(10\times31) \bmod 110 = 90$

$(20\times31) \bmod 110 = 70$

$(40\times31) \bmod 110 = 30$

* Encryption:

Now Assume PT

let PT = 100100 | 111100 | 10 1110
① ② ③

divide PT into 6-6 parts (no. of elements in sequence = 6)

1st part ⇒ 100100 = 1×31 + 0×62 + 0×14 + 1×90 + 0×70 + 0×30

= 31 + 90 = 121 ⇒ CT

2nd part ⇒ 111100 ⇒ 31 + 62 + 14 + 90 + 0 + 0

= 197 → CT

→ no. of elements in sequence is 6 elements, so divide into 6 parts PT.

part ⇒ 101110 → 31+0+14+90+70+0 → 205 ↓ CT

We multiply with public key with PT instead of private key.

$\therefore CT = [121, 197, 205]$

* Decryption:

① Calculate $5^{-1} = 31^{-1}$

$31x \bmod 110 = 1$ then we get $x = 71$

→ until get 1 continue process

$(CT \times x) \bmod m$ from seq D = {1, 2, 4, 10, 20, 40}
↓ private key

$(121 \times 71) \bmod 110 = 11 \Rightarrow 100100$ (1+10=11)

$(197 \times 71) \bmod 110 = 17 \Rightarrow 111100$ (1+2+4+10=17)

$(205 \times 71) \bmod 10 = 35 \Rightarrow 101110$ (1+4+10+20=35)

in encryption we taken public key

in decryption process we taken private key

⇒ 11 in sequence add any two no's to get it

{1, 2, 4, 10, 20, 40}
1 0 0 1 0 0

(0+1=11 → here put 1 other case put 0.

17 → {1, 2, 4, 10, 20, 40}
1 1 1 1 0 0

we get same PT back 100100 111100 101110

⇒ knapsack encryption algorithm is the first general public key cryptography algorithm.

It is developed by Ralph Merkle and Martin Hellman in 1978.

=> we need two different keys public key & private key

for easy knapsack we will choose a super increasing knapsack problem.

It is a sequence in which every next term is greater than the sum of all preceding terms.