Nama: Nur Hidayatul Mustafit

NIM: 190411100014

KDA B

Algoritma Knapsack (Merkle-Hellman)

I. PRIVATE KEY

Pada algoritma ini untuk menentukan *kunci private adalah berupa barisan superincreasing.* **Barisan superincreasing adalah suatu barisan di mana setiap nilai di dalam barisan lebih besar daripada jumlah semua nilai sebelumnya.**

Contoh:

{2, 3, 6, 13, 27, 52} merupakan barisan superincreasing,

{1, 3, 4, 9, 15, 25} bukan barisan superincreasing

II. PUBLIC KEY

Langkah untuk membuat kunci public adalah:

1. Tentukan barisan superincreasing (private key)
   Misalkan kita ambil : {2, 3, 6, 13}
2. Kalikan setiap elemen di dalam barisan tersebut dengan n (mod m) (*Modulus m seharusnya angka yang lebih besar daripada jumlah semua elemen di dalam barisan,* sedangkan pengali n seharusnya tidak mempunyai faktor persekutuan dengan m atau PBB(n, m) = 1).
   Misalkan kita ambil: m = 105 dan n =31
   $2 \cdot 31 \bmod 105 = 62$
   $3 \cdot 31 \bmod 105 = 93$
   $6 \cdot 31 \bmod 105 = 81$
   $13 \cdot 31 \bmod 105 = 88$
   Maka, kunci publiknya adalah {62, 93, 81, 88}

III. ENKRIPSI

Pada proses enkripsi, jika kita ingin enkripsi huruf (string) maka kita ubah dalam bentuk ASCII kode biner. Berikut adalah proses enkripsi:

- Misal kita akan mengekripsi kata " h ", bentuk binernya (plainteks) adalah: 01101000
- kunci publiknya adalah {62, 93, 81, 88}
- kunci privatenya adalah {2, 3, 6, 13}
- Plainteks dibagi menjadi blok yang panjangnya 4 karena kode ASCII terdiri dari 8 bit biner, kemudian setiap bit di dalam blok dikalikan dengan elemen yang berkorepsonden di dalam kunci public :

Blok plainteks ke-1 : 0110

Kunci publik : 62, 93, 81, 88

Kriptogram : $(0 \times 62) + (1 \times 93) + (1 \times 81) + (0 \times 88) = 174$

Blok plainteks ke-2 : 1000

Kunci publik : 62, 93, 81, 88

Kriptogram : $(1 \times 62) + (0 \times 93) + (0 \times 81) + (0 \times 88) = 62$

Hasil enkripsi (chiperteks) adalah {174, 62}

IV. DEKRIPSI

- Proses dekripsi dilakukan dengan menggunakan kunci privat.
- Mula-mula penerima pesan menghitung n^{-1} , yaitu balikan dari *n* modulo *m*, sedemikian sehingga $n \cdot n^{-1} \equiv 1 \pmod{m}$.
- Kalikan setiap kriptogram dengan n^{-1} , lalu nyatakan hasil kalinya sebagai penjumlahan elemen-elemen kunci privat untuk memperoleh plainteks dengan menggunakan algoritma pencarian solusi superincreasing knapsack.
- Contoh:

  Sesuai contoh dari atas, kunci private {2, 3, 6, 13}. n = 31 dan m = 105.

  $n \cdot n^{-1} \equiv 1 \pmod{m}$ → $31 \cdot n^{-1} \equiv 1 \pmod{105}$ → $n^{-1} = (1 + 105k)/31$, dengan mencoba nilai k = 0, 1, 2, …, dst. Diperoleh $n^{-1} = 61$ (dengan n^{-1} berupa bilangan bulat)

chiperteks dari enkripsi adalah {174, 62}, proses deskripsinya:

$174 \cdot 61 \bmod 105 = 9 = 0 \cdot 2 + 1 \cdot 3 + 1 \cdot 6 + 0 \cdot 13 \rightarrow 0110$

$62 \cdot 61 \bmod 105 = 2 = 1 \cdot 2 + 0 \cdot 3 + 0 \cdot 6 + 0 \cdot 13 \rightarrow 1000$

Plainteksnya adalah 01101000

Jika dikonvert ASCII menjadi huruf “ h ”