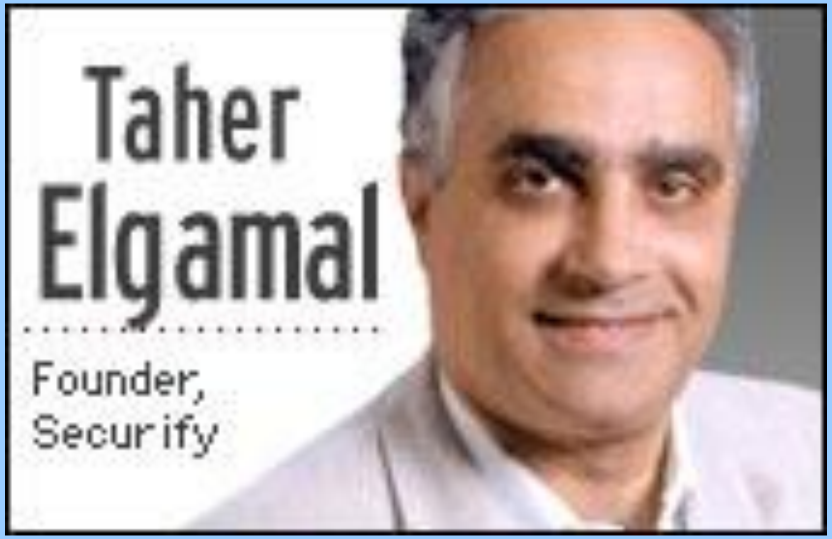
Algoritma ElGamal

Bahan Kuliah

IF4020 Kriptografi

Pendahuluan

- Dibuat oleh Taher Elgamal (1985). Pertama kali dikemukakan di dalam makalah berjudul "*A public key cryptosystem and a signature scheme based on discrete logarithms*"



- Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit.

- *Masalah logaritma diskrit*: Jika p adalah bilangan prima dan g dan y adalah sembarang bilangan bulat. carilah x sedemikian sehingga

$$g^x \equiv y \pmod{p}$$

Properti algoritma ElGamal:

1. Bilangan prima, p (tidak rahasia)
2. Bilangan acak, g ($g < p$) (tidak rahasia)
3. Bilangan acak, x ($x < p$) (rahasia, kc. privat)
4. $y = g^x \bmod p$ (tidak rahasia, kc. publik)
5. m (plainteks) (rahasia)
6. a dan b (cipherteks) (tidak rahasia)

Algoritma Pembangkitan Kunci

1. Pilih sembarang bilangan prima p (p dapat di-*share* di antara anggota kelompok)
2. Pilih dua buah bilangan acak, g dan x, dengan syarat $g < p$ dan $1 \leq x \leq p - 2$
3. Hitung $y = g^x \bmod p$.

Hasil dari algoritma ini:

- Kunci publik: tripel (y, g, p)

- Kunci privat: pasangan (x, p)

Algoritma Enkripsi

1. Susun plainteks menjadi blok-blok m_1, m_2, …, (nilai setiap blok di dalam selang [0, p – 1].
2. Pilih bilangan acak k, yang dalam hal ini $1 \leq k \leq p - 2$.
3. Setiap blok m dienkripsi dengan rumus

   $$a = g^k \bmod p$$

   $$b = y^k m \bmod p$$

   Pasangan a dan b adalah cipherteks untuk blok pesan m. Jadi, ukuran cipherteks dua kali ukuran plainteksnya.

Algoritma Dekripsi

1. Gunakan kunci privat x untuk menghitung $(a^x)^{-1} = a^{p-1-x} \bmod p$
2. Hitung plainteks m dengan persamaan:

$$m = b/a^x \bmod p = b(a^x)^{-1} \bmod p$$

Contoh:

(a) Pembangkitan kunci (Oleh Alice)

Misal p = 2357, g = 2, dan x = 1751.

Hitung: $y = g^x \bmod p = 2^{1751} \bmod 2357 = 1185$

Hasil: Kunci publik: (y = 1185, g = 2, p = 2357)

Kunci privat: (x = 1751, p = 2357).

(b) Enkripsi (Oleh Bob)

Misal pesan m = 2035 (nilai m masih berada di dalam selang [0, 2357 – 1]).

Bob memilih bilangan acak k = 1520 (nilai k masih berada di dalam selang [0, 2357 – 1]).

Bob menghitung

$a = g^k \bmod p = 2^{1520} \bmod 2357 = 1430$

$b = y^k m \bmod p = 1185^{1520} \cdot 2035 \bmod 2357 = 697$

Jadi, cipherteks yang dihasilkan adalah (1430, 697).

Bob mengirim cipherteks ini ke Alice.

(c) Dekripsi (Oleh Alice)

$1/a^x = (a^x)^{-1} = a^{p-1-x} \bmod p = 1430^{605} \bmod 2357 = 872$

$m = b/a^x \bmod p = 697 \cdot 872 \bmod 2357 = 2035$