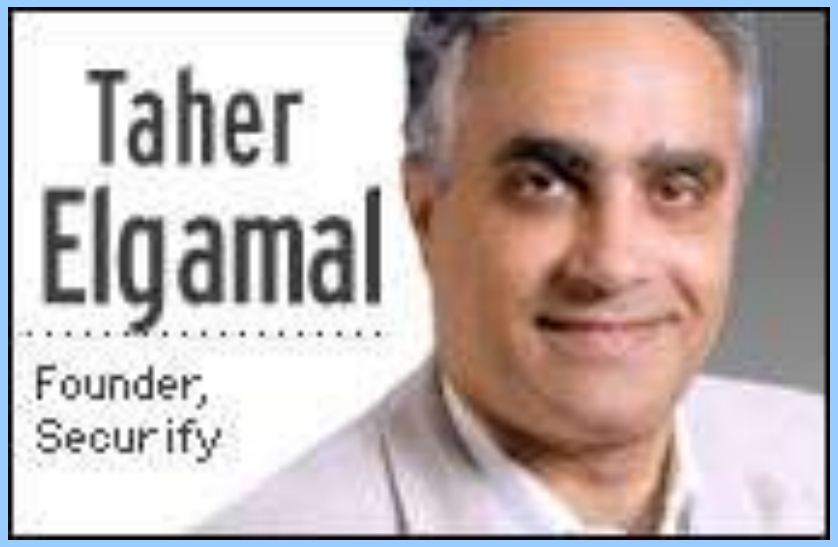
Algoritma ElGamal

Bahan Kuliah

IF3058 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 α dan β adalah sembarang bilangan bulat. carilah *d* sedemikian sehingga

$$\alpha^d \equiv \beta \pmod{p}$$

- Atau $\beta = \alpha^d \mod p$

Properti algoritma = ElGamal:

1. Bilangan prima, p (tidak rahasia)
2. Bilangan acak, α ($\alpha < p-1$) (tidak rahasia)
3. Bilangan acak, d ($d < p-2$) (rahasia, kc. privat)
4. $\beta = \alpha^x \bmod p$ (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 $\beta = \alpha^d \mod p$.

Hasil dari algoritma ini:

- Kunci publik: tripel (α , β, p)
- Kunci privat: pasangan (d, 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

   $a = \alpha^k \bmod p$

   $b = \beta^k \, m \bmod p$

   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 $(a^d)^{-1}$, yaitu I yang berlaku hubungan

   $$I \times a^d \bmod p = 1$$

1. Hitung plainteks *m* dengan persamaan:

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

   $$= b\,I \bmod p$$

Contoh:

(a) Pembangkitan kunci (Oleh Alice)

Misal $p = 2357$, $\alpha = 2$, dan $d = 1751$.

Hitung: $\beta = \alpha^x \bmod p = 2^{1751} \bmod 2357 = 1185$

Hasil: Kunci publik: ($\alpha = 2$, $\beta = 1185$, $p = 2357$)

Kunci privat: ($d = 1751$, $p = 2357$).

(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

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

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

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

Bob mengirim cipherteks ini ke Alice.

(c) Dekripsi (Oleh Alice)

$1/a^x = (a^x)^{-1} = 872$ ➔ dicari dengan trial error

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