Algoritma RSA

Pendahuluan

- Algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya.
- Ditemukan oleh tiga peneliti dari *MIT* (*Massachussets Institute of Technology*), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.
- Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Properti Algoritma RSA

1. p dan q bilangan prima (rahasia)
2. $n = p \cdot q$ (tidak rahasia)
3. $\phi(n) = (p - 1)(q - 1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)

   Syarat: PBB(e, $\phi(n)$) = 1
5. d (kunci dekripsi) (rahasia)

   d dihitung dari $d \equiv e^{-1} \bmod (\phi(n))$
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Pembangkitan pasangan kunci

1. Pilih dua bilangan prima, a dan b (rahasia)
2. Hitung $n = a\,b$. Besaran n tidak perlu dirahasiakan.
3. Hitung $\phi(n) = (a - 1)(b - 1)$.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relatif prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi, d, melalui $ed \equiv 1$ (**mod** m) atau $d \equiv e^{-1} \bmod (\phi(n))$

Hasil dari algoritma di atas:

- Kunci publik adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

Catatan: n tidak bersifat rahasia, namun ia diperlukan pada perhitungan enkripsi/dekripsi.

Enkripsi

1. Nyatakan pesan menjadi blok-blok plainteks: m_1, m_2, m_3, … (harus dipenuhi persyaratan bahwa nilai m_i harus terletak dalam himpunan nilai 0, 1, 2, …, $n - 1$ untuk menjamin hasil perhitungan tidak berada di luar himpunan)
2. Hitung blok cipherteks c_i untuk blok plainteks p_i dengan persamaan

$$c_i = m_i^e \textbf{ mod } n$$

yang dalam hal ini, e adalah kunci publik.

Dekripsi

1. Proses dekripsi dilakukan dengan menggunakan persamaan

$$m_i = c_i^d \textbf{ mod } n,$$

yang dalam hal ini, d adalah kunci privat.

- **Contoh 21.** Misalkan $a = 47$ dan $b = 71$ (keduanya prima), maka dapat dihitung:

  $n = a \times b = 3337$

  $\phi(n) = (a - 1) \times (b - 1) = 3220$.

- Pilih kunci publik $e = 79$ (yang relatif prima dengan 3220 karena pembagi bersama terbesarnya adalah 1).

- Nilai e dan n dapat dipublikasikan ke umum.

- Selanjutnya akan dihitung kunci privat d dengan kekongruenan:

$$e \times d \equiv 1 \pmod{m}$$

$$d = \frac{1 + (k \times 3220)}{79}$$

Dengan mencoba nilai-nilai k = 1, 2, 3, …, diperoleh nilai d yang bulat adalah 1019. Ini adalah kunci privat (untuk dekripsi).

- Misalkan plainteks M = HARI INI
  atau dalam ASCII: 726582733273873

Pecah M menjadi blok yang lebih kecil (misal 3 digit):

$m_1 = 726$ $m_4 = 273$

$m_2 = 582$ $m_5 = 787$

$m_3 = 733$ $m_6 = 003$

(Perhatikan, m_i masih terletak di dalam antara 0 sampai $n - 1$)

- *Enkripsi setiap blok:*

  $c_1 = 726^{79} \bmod 3337 = 215$

  $c_2 = 582^{79} \bmod 3337 = 776$

  dst

  Chiperteks *C* = 215 776 1743 933 1731 158.

- *Dekripsi (menggunakan kunci privat d = 1019)*

  $m_1 = 215^{1019} \bmod 3337 = 726$

  $m_2 = 776^{1019} \bmod 3337 = 582$

  dst untuk sisi blok lainnya

  Plainteks *M* = 726582733273873

  yang dalam ASCII karakternya adalah HARI INI.

Kekuatan dan Keamanan RSA

- Kekuatan algoritma *RSA* terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $n = a \times b$.

- Sekali n berhasil difaktorkan menjadi a dan b, maka $\phi(n) = (a - 1)\times(b - 1)$ dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan $ed \equiv 1 \pmod{n}$.

- Penemu algoritma *RSA* menyarankan nilai *a* dan *b* panjangnya lebih dari 100 digit. Dengan demikian hasil kali $n = a \times b$ akan berukuran lebih dari 200 digit.

- Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun! (dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik).

Contoh RSA 512 bit ≈ $1{,}3.10^{154}$

(dikutip dari Sarwono Sutikno, EL)

- Modulus *n* = 81 5a d0 b9 0a ac 9f 4c da cc 57 6e ca a7 6a c3 46 92 a7 81 68 ec 08 ec 77 dd 40 c2 ec 97 52 cb 3b 34 2c b6 a6 e2 76 3a ed 42 84 fa 55 ac 0d 6c 10 39 a2 7e a3 09 be 40 35 38 04 7d 06 43 1f 6f
- *e* = 29 40 70 02 50 db 19 6b b1 f4 8a a7 b4 59 6c 4b 66 b5 94 f6 15 ae e4 69 44 95 23 f3 d0 fc ea 84 19 7c 55 e0 27 40 2d 19 18 15 08 05 51 ac f5 98 91 f0 98 5f c4 17 05 eb 3b e8 a3 04 32 d4 20 2f
- *d* = 59 f1 2f 29 73 d0 bc 8e 13 6e 2a 21 53 2c b7 4d 69 82 c9 54 92 6c 64 43 0d 69 15 83 e9 44 a6 de 5e 30 e9 ae 48 f9 c8 84 a4 16 44 4d df 50 f2 0e 96 3e 24 df a4 f4 ec 3d c6 db 61 a7 e6 dc ea cf

- Tahun 1977, 3 orang penemu *RSA* membuat sayembara untuk memecahkan cipherteks dengan menggunakan RSA di majalah *Scientific American*.
- Hadiahnya: $100
- Tahun 1994, kelompok yang bekerja dengan kolaborasi internet ebrhasil memecahkan cipherteks hanya dalam waktu 8 bulan.

Panjang desimal *n*	Panjang *n* dalam bit (perkiraan)	Perolehan Data	MIPS-Year
100	332	April 1991	7
110	365	April 1992	75
120	398	June 1993	830
129	428	April 1994	5000
130	431	April 1996	500

Ket: *MIPS-Year = million instructions-per-second processor running for one year*, setara dengan eksekusi 3 x 10^{13} instruksi
Prosesor Pentium 200 MHz setara dengan mesin 50-MIPS