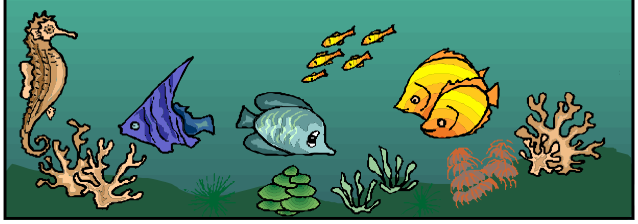
Algoritma RSA



- Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman.
- Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Besaran-besaran yang digunakan pada algoritma RSA:

1.	p dan q bilangan prima	(rahasia)
2.	$r = p \cdot q$	(tidak rahasia)
3.	$m = (p - 1)(q - 1)$	(rahasia)
4.	*PK* (kunci enkripsi)	(tidak rahasia)
5.	*SK* (kunci dekripsi)	(rahasia)
6.	*X* (plainteks)	(rahasia)
7.	*Y* (cipherteks)	(tidak rahasia)

Prosedur Membuat Pasangan Kunci

Key generation :

1. Hasilkan dua buah integer prima besar, p dan q Untuk memperoleh tingkat keamanan yang tinggi pilih p dan q yang berukuran besar, misalnya 1024 bit.
2. Hitung m = (p-1)*(q-1)
3. Hitung n = p*q
4. Pilih d yg relatively prime terhadap m e relatively prime thd m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut gcd(e,m) = 1. Untuk mencarinya dapat digunakan algoritma Euclid.
5. Cari d, sehingga e*d = 1 mod (m), atau d = (1+nm)/e Untuk bilangan besar, dapat digunakan algoritma extended Euclid.
6. Kunci publik : e, n Kunci private : d, n

Kasus 1

Misalkan

p = 3

q = 11 (keduanya prima).

Selanjutnya, hitung nilai

$n = p \cdot q = 33$

dan

$m = (p – 1)(q – 1) = 20$.

Pilih d yg relatively prime terhadap m

→ gcd(e,m) = 1

→ gcd(e, 20) = 1

e = 2 => gcd(e, 20) = 2 (tidak)

e = 3 => gcd(e, 20) = 1 (ya)

e = 5 ➔ gcd(5,20) =1 (tidak)

e = 7 ➔ gcd(7,20) =1 (ya)

Asumsi dipilih e =3

Cari nilai d

e*d = 1 mod (m)

3*d = 1 mod 20

3*d mod 20 = 1 → 21 mod 20 =1

81 mod 20 =1

misal dipilih d=7

Public key : (3, 33)

Private key : (7, 33)

Enkripsi

B mengenkripsi message M untuk A Yg harus dilakukan B :

1. Ambil kunci publik A yg otentik (n, e)
2. Representasikan message sbg integer M dalam interval [0,n-1]
3. Hitung C = M ^ e (mod n)
4. 4. Kirim C ke A

dekripsi

- Untuk mendekripsi, A melakukan : Gunakan kunci pribadi d untuk menghasilkan

  M = C^(d) (mod n)

message "2"

Enkripsi

C = 2 ^ 3 (mod 33) = 8

= 8 mod 33 = 0 sisa 8

Dekripsi

M = 8 ^ 7 (mod 33)

= 2097152 (mod 33)

= 2

Kasus 2

Misalkan

p = 47

dan *q* = 71 (keduanya prima).

n= *p* · *q* = 3337

m = (*p* – 1)(*q* – 1) = 3220

mencari d

gcd(e,3337)

misal dipilih = 79

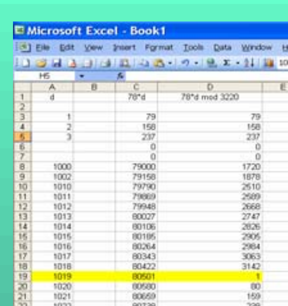
Hitung d

e*d = 1 mod (m)

79 * d = 1 mod 3220

79 * d mod 3220 = 1

→ 1019



	A	B	C	D	E
1	d		78*d	78*d mod 3220	
2					
3	1		79	79	
4	2		158	158	
5	3		237	237	
6			0	0	
7			0	0	
8	1000		79000	1720	
9	1002		79158	1878	
10	1010		79790	2510	
11	1011		79869	2589	
12	1012		79948	2668	
13	1013		80027	2747	
14	1014		80106	2826	
15	1015		80185	2905	
16	1016		80264	2984	
17	1017		80343	3063	
18	1018		80422	3142	
19	1019		80501	1	
20	1020		80580	80	
21	1021		80659	159	
22	1022		80738	238	

Kunci publik : e, n Kunci private : d, n

Private key : (1019, 3337)

Public key : (79, 3337)

Misalkan plainteks yang akan dienkripsikan adalah

X = HARI INI

Dalam sistem desimal (pengkodean ASCII) adalah

H	A	R	I	(SPASI)	I	N	I
72	65	82	73	32	73	78	73

- Pecah *X* menjadi blok yang lebih kecil, misalnya *X* dipecah menjadi enam blok yang berukuran 3 digit:
- $x1 = 726$ $x4 = 273$
- $x2 = 582$ $x5 = 787$
- $x3 = 733$ $x6 = 003$ (ditambah 0)

Proses pemecahan melihat dalam interval [0,n-1] → interval [0, 3336]

Blok-blok plainteks dienkripsikan sebagai berikut:

726^79 mod 3337 = 215 = $y1$

582^79 mod 3337 = 776 = $y2$

733^79 mod 3337 = 1743 = $y3$

273^79 mod 3337 = 933 = $y4$

787^79 mod 3337 = 1731 = $y5$

003^79 mod 3337 = 158 = $y6$

Jadi, cipherteks yang dihasilkan adalah

Y = 215 776 1743 933 1731 158.

- 72 65 82 73 32 73 78 73 → ASLI

- 215 776 1743 933 1731 15.
  cf62b7c1b3169329d516ee6a13d3016c hash asli
- cf64ec4a3febd3642a29107c99e8e993 hash naskah

- hash
- 72 65 82 73 32 73 78 73 → dekripsi
- H A R I

Dekripsi dilakukan dengan menggunakan kunci rahasia

Blok-blok cipherteks didekripsikan sebagai berikut:

215^1019 mod 3337 = 726 = $x1$

776^1019 mod 3337 = 582 = $x2$

1743^1019 mod 3337 = 733 = $x3$

- …

Blok plainteks yang lain dikembalikan dengan cara yang serupa. Akhirnya kita memperoleh kembali plainteks semula

P = 7265827332737873

yang dalam karakter ASCII adalah

P = HARI INI.

Kekuatan RSA

- Keamanan algoritma *RSA* terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $r = p \times q$.

- Sekali r berhasil difaktorkan menjadi p dan q, maka $\phi(r) = (p - 1)(q - 1)$ dapat dihitung. Selanjutnya, karena kunci enkrispi *PK* diumumkan (tidak rahasia), maka kunci dekripsi *SK* dapat dihitung dari persamaan $PK \cdot SK \equiv 1 \pmod{\phi(r)}$.

- Penemu algoritma *RSA* menyarankan nilai p dan q panjangnya lebih dari 100 digit. Dengan demikian hasil kali $r = p \times q$ akan berukuran lebih dari 200 digit. Menurut Rivest dan kawan-kawan, uasaha 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).

- Terima Kasih