ALGORITMA RSA
(RIVEST-SHAMIR-ADLEMAN)

Pertemuan ke 7

Mata Kuliah : Kriptografi

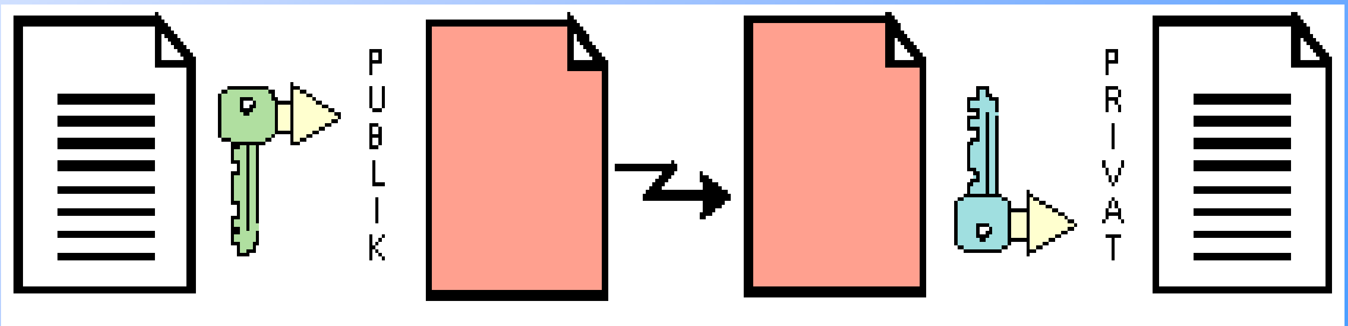
Teknik Informatika UAD

Asal Mula

- tahun 70-an Whitfield Diffie dan Martin Hellman menemukan teknik enkripsi asimetrik yang merevolusi dunia kriptografi
- tahun 1977 tiga orang peneliti, yaitu R.L. Rivest, A. Shamir, dan L. Adleman, menemukan RSA

Apa Itu RSA ?

- Merupakan salah satu teknik kripto, dimana kunci untuk meng-enkrip dan untuk –men-dekrip berbeda
- Contoh metode lain : ElGamal, Rabin, Elliptic Curve Cryptosistem (ECC), Diffie-Helman, LUC



Apa itu RSA ?

- Orang yang mempunyai kunci publik dpt meng-enkripsi tapi yang dapat men-dekripsi cuma yang th kunci privat
- Kuci publik dpt dimiliki oleh sembarang orang,tapi kunci privat cuma orang tertentu atau bahkan hanya seorang.

Dasarnya?

- Algoritma ini dibuat berdasarkan fakta bahwa dalam perhitungan dengan komputer, untuk menemukan suatu bilangan prima yang besar sangat mudah, namun untuk mencari faktor dari perkalian dua bilangan prima yang besar sangat sulit, bahkan hampir tidak mungkin.

Prosesnya ?

Pengirim

- Menerima kunci Publik
- Meng-enkrispi Plaintek dengan kunci publik
- Mengirimkan cipherteks

Penerima

- Membangkitkan kunci publik dan kunci privat
- Mengirimkan kunci Publik
- Mendekripsi Cipherteks dengan kunci provat

Algoritmanya?

Proses enkripsi : $C = M^e \bmod n$

Proses dekripsi : $M = C^d \bmod n$

Dimana :

M : bilangan integer yang merepresentasikan pesan

C : bilangan integer yang merepresentasikan pesan tersandi

e : kunci enkripsi (publik)

d : kunci dekripsi (pribadi)

n : modulus (publik)

Bilangan e dan n adalah kunci publik yg dapat diketahui umum

M dan C berupa Integer ?

- Bila seorang pengguna A ingin mengirimkan pesan rahasia ke seorang pengguna B yang memiliki suatu sistem kriptografi RSA, langkah pertama yang harus dilakukan oleh pengguna A adalah merepresentasikan pesannya (yang biasanya berupa teks) dalam bentuk deretan bilangan integer nonnegatif dalam suatu basis tertentu. Konversi pesan teks ke bentuk deretan bilangan integer ini dapat dilakukan menggunakan berbagai teknik, pada umumnya adalah standar ASCII 8-*bit* atau yang lainnya

Menghitung Nilai *e, d,* dan *n* :

1. ambil secara random dua bilangan prima p dan q yang besar dan berbeda, namun ukuran keduanya (jumlah digitnya dalam basis bilangan yang dipergunakan) haruslah sama.
2. Hitung *modulus n* dan fungsi *Euler's Totient* $\phi(n)$:
3. $n = p.q$,
4. $\Phi(n) = (p-1)(q-1)$
5. Pilih suatu bilangan integer *e* dimana :
6. $1 < e < \phi(n)$ dan $gcd\ (e, \phi(n)) = 1$
7. Hitung nilai integer d dimana $1 < d < \phi(n)$ sedemikian hingga :
8. $d = e-1 \ mod\ \phi(n)$ atau $e.d = 1\ (mod\ \phi\ (n))$
9. dengan menggunakan algoritma *Euclidean* yang diperluas
10. *Public-key* dari sistem ini adalah *n* dan *e*, sedangkan *private-key*-nya adalah *d*

Kondisi Enkripsi

Ada kondisi yang harus dipenuhi dalam proses Enkripsi : ($C = M^e \bmod n$)

- Bilangan *e* harus lebih kecil dari *n*, demikian juga bilangan *M* harus lebih kecil dari *n*
- Bilangan *M* harus lebih kecil dari *n* untuk menjamin terjadinya trasformasi satu-satu dengan *domain* dan *range* yang identik

Verifikasi ?

Setelah menerima pesan tersandi *C*, penerima Cipherteks kemudian mendapatkan kembali pesan *M* semuila dengan melakukan penghitungan :

$M' = Cd \bmod n$

Proses dekripsi ini dapat diverifikasi sebagia berikut :

- $M' = (Me \bmod n)d \bmod n$
- $M' = Med \bmod n$

Karena $e.d = k.\ \Phi(n) + 1$ untuk suatu integer *k* tertentu :

- $M' = Mk(\Phi(n) + 1) \bmod n$
- $M' = (M\ \Phi(n))k.\ M \bmod n$

Jika $gcd(\Phi(n),n) = 1$, maka teorema *Eulier* menjamin bahwa $M'=M$,

Contoh

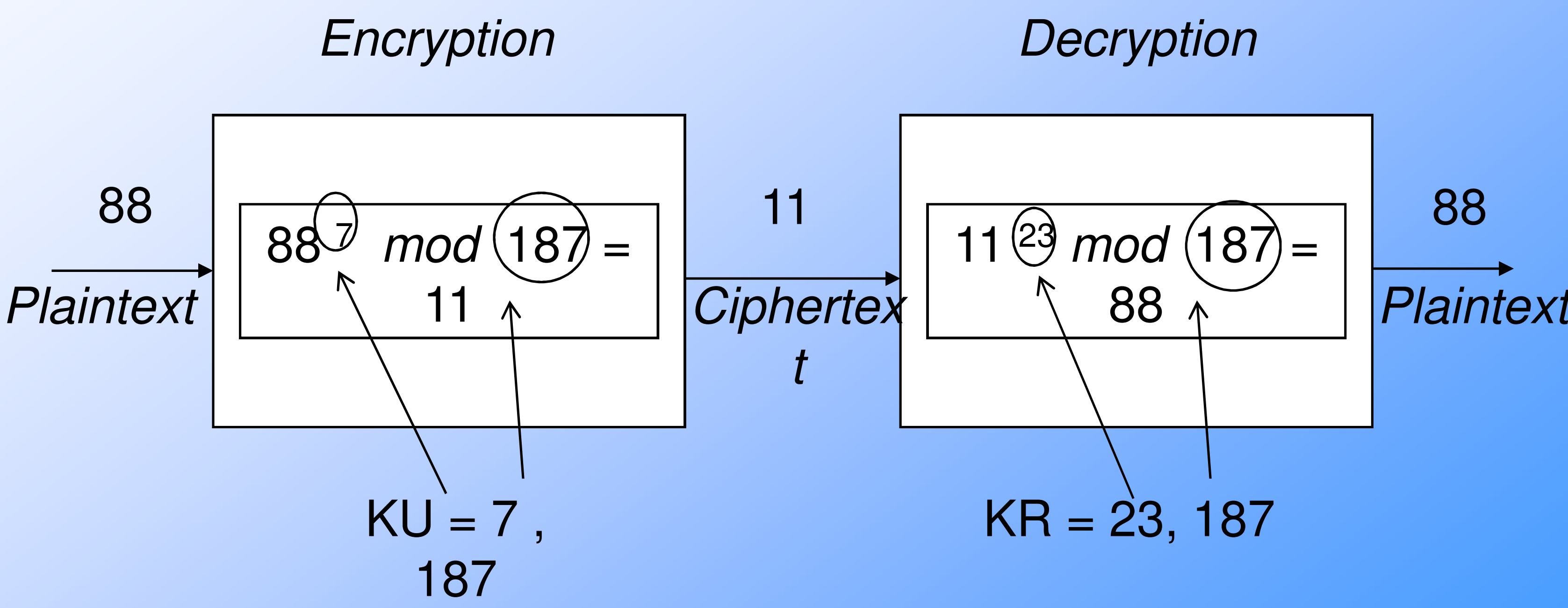
Membangkitkan Kunci

- Membuat 2 bilangan prima lebar p dan q, dimana $p \neq q$. Misalnya $p = 17$ dan $q = 11$
- Hitung $n = pq = 17 \times 11 = 187$
- Hitung $\phi(n) = (p - 1)(q - 1) = (17-1)\times(11-1) = 16 \times 10 = 160$
- Menentukan bilangan terkecil e yang merupakan *coprime* $\phi(n) = 160$, dengan syarat $gcd(e, \phi(n)) = 1$, dimana $1 < e < \phi(n)$, misalnya $e = 7$
- Menghitung $d = e-1 \ mod\ \phi(n)$ dimana $d * 7 = 1\ mod\ 160$ dan $d < 160$. Harga yang benar adalah $d = 23$ karena $23 \times 7 = 161 = 1 \times 160 + 1$, d dapat dihitung menggunakan *euclid's algorithm*
- Dari hasil perhitungan diatas didapatkan bahwa kunci publik ($KU = \{7, 187\}$), dimana $e = 7$ dan *modulus* $n = 187$
- Sedangkan kunci privat ($KR = \{23, 187\}$), dimana $d = 23$ dan $n = 187$.

Contoh

- Akan dienkripsikan planteks huruf “X”
- Maka huruf ini kita konversikan lebih dulu ke suatu nilai integer, misalnya kode ASCI-nya berarti 88

- Sebagai contoh yang menunjukkan penggunaan kunci ini pada pemasukan *plaintext* untuk $M = 88$



Enkripsinya ?

- Untuk enkripsi, dapat dihitung dengan syarat *plaintext* $M < n$, dan
- *ciphertext* $C = Me \ (mod\ n)$, dimana $C = 88^7 \ mod\ 187$.
- $88^7 \ mod\ 187 = ((88^4 \ mod\ 187) \times (88^2 \ mod\ 187) \times (88^1 \ mod\ 187)) \ mod\ 187$
- $88^1 \ mod\ 187 = 88$
- $88^2 \ mod\ 187 = 7744 \ mod\ 187 = 77$
- $88^4 \ mod\ 187 = 59.969.536 \ mod\ 187 = 132$
- $88^7 \ mod\ 187 = (88 \times 77 \times 132) \ mod\ 187 = 894.432 \ mod\ 187 = 11$

Dekripsinya?

- Dekripsi dapat dihitung dengan *ciphertext C*, dan

plaintext M = Cd (mod n), dimana $M = 11^{23}$ *mod* 187

- 11^{23} *mod* 187 = ((11^{1} *mod* 187) x (11^{2} *mod* 187) x (11^{4} *mod* 187) x
- (11^{8} *mod* 187) x (11^{8} *mod* 187)) *mod* 187
- 11^{1} *mod* 187 = 11
- 11^{2} *mod* 187 = 121
- 11^{4} *mod* 187 = 14.641 *mod* 187 = 55
- 11^{8} *mod* 187 = 214.358.881 *mod* 187 = 33
- 11^{23} *mod* 187 = (11 x 121 x 55 x 33 x 33) *mod* 187
- = 79.720.245 *mod* 187 = 88
- Proses ini akan menghasilkan pesan *plaintext* semula.