Konsep Enkripsi dan Dekripsi Berdasarkan Kunci Tidak Simetris

Oleh: Benfano Soewito – Faculty member Graduate Program Universitas Bina Nusantara

Dalam tulisan saya pada bulan Agustus lalu telah dijelaskan bagaimana prinsip dari enkripsi dan dekripsi dengan menggunakan kunci simetris. Pada tulisan saya bulan ini saya akan melanjutkan tentang enkripsi dan dekripsi dengan menggunakan kunci tidak simetris atau *asymmetric key*.

Seiring dengan banyaknya aplikasi digital dan bertambahnya pengguna internet, maka informasi yang disimpan dalam data digital juga bertambah. Setiap aplikasi yang baru diperkenalkan di internet biasanya selalu ada celah keamanan, maka semakin banyak aplikasi diinternet, maka makin banyak juga celah celah yang terbuka bagi orang orang yang ingin berbuat jahat. Oleh karena itu faktor keamanan menjadi suatu hal yang serius dalam semua applikasi yang ada di internet, terutama aplikasi aplikasi yang berhubungan dengan keuangan. Salah satu cara untuk melindungi atau mencegah data kita dibaca oleh orang orang yang tidak bertanggung jawab adalah dengan mengenkrip data tersebut.

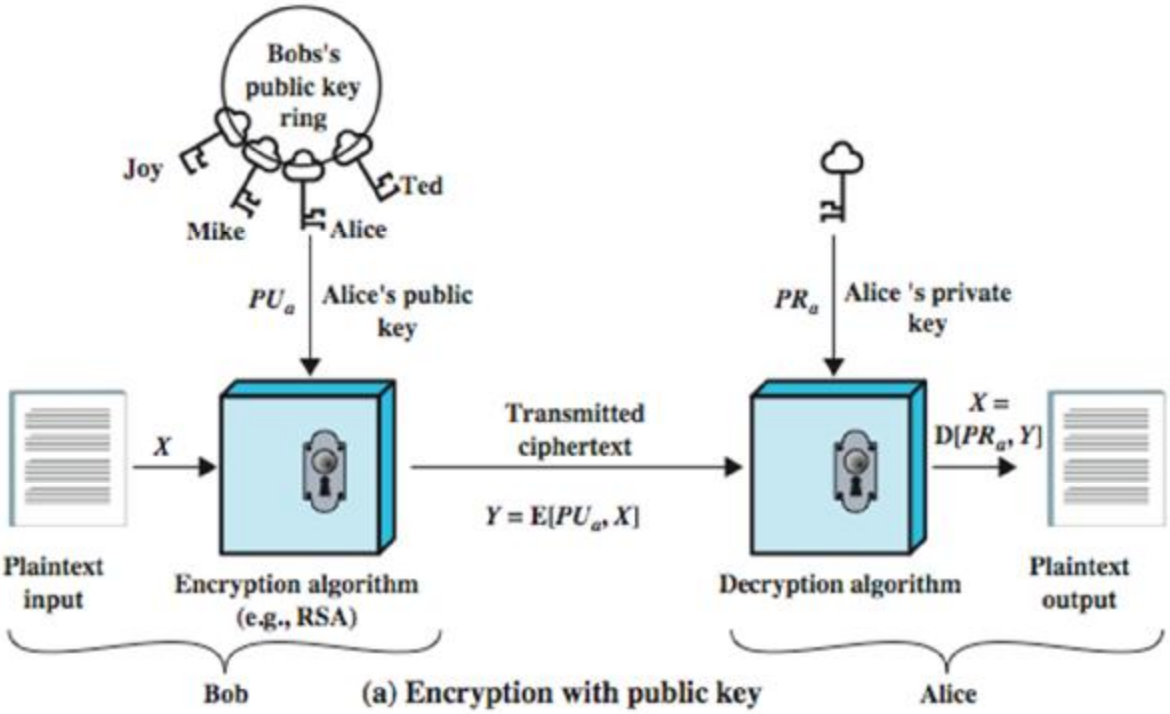
Enkripsi adalah suatu proses untuk merubah sebuah pesan, data atau informasi (biasa disebut plaintext), sehingga informasi tersebut tidak dapat dibaca oleh orang yang tidak bertanggung jawab (ciphertext). Jadi plaintext adalah informasi yang dapat dimengerti dan ciphertext adalah informasi yang tidak dapat dimengerti atau dibaca. Enkripsi adalah bagian dari sebuah ilmu yang disebut kriptologi atau kriptografi. Kriptografi adalah sebuah ilmu yang mempelajari teknik untuk membuat sebuah pesan atau informasi tidak dapat dibaca oleh orang yang tidak berhak. Ada dua teknik yang cukup terkenal dalam kriptografi yaitu: symmetric key encryption dan public key encryption.

Symmetric-key encryption atau enkripsi dengan menggunakan kunci simetris sudah ssaya bahas pada bulan Agustus lalu. Pada tulisan ini saya akan membahas enkripsi dengan menggunakan kunci tidak simetris. Ada beberapa kelemahan dari enkripsi dengan menggunakan kunci simetris, yaitu:

1. Distribusi kunci, pada kenyataannya cara atau media untuk memberikan kunci menjadi masalah, sebab apabila data yang sudah dienkrip dan dikirim ke pihak lain, maka kita juga perlu mengirimkan juga kuncinya.

2. Terlalu banyak kunci, setiap kita berkomunikasi atau mengirim data kepada orang yang berbeda, kita juga harus menyediakan kunci yang berbeda beda pula. Ini menimbulkan masalah dalam mengingat atau menyimpan kunci kunci tersebut.
3. Tidak dapat dijamin apakah informasi berasal dari orang yang benar atau tidak apabila kunci tercuri.

Oleh karena itu untuk mengatasi masalah tersebut maka diciptakanlah enkripsi dengan cara kunci asimetrik. Pada enkripsi asimetrik dibutuhkan dua buah kunci, yaitu: *public key* dan *private key* atau kunci umum dan kunci pribadi. Kunci umum memang kunci yang dibuat untuk disebarkan kepada public. Kunci umum ini digunakan oleh siapa saja yang ingin mengirim data atau pesan kepada orang yang mempunyai kunci umum tersebut. Sedangkan kunci pribadi harus dijaga kerahasiaannya dan digunakan untuk mengdekrip data atau pesan yang diterima. Hal ini dapat dijelaskan pada gambar 1.



Gambar 1. Enkripsi dengan kunci umum (diambil dari buku Cryptography and Network Security oleh Stallings)

Salah satu algoritma enkripsi dengan kunci asimetrik yang terkenal adalah Algoritma RSA. Algoritma RSA ini 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. Algoritma ini menghasilkan sepasang kunci yang mana salah satu kunci dapat dijadikan kunci umum dan kunci yang lainnya menjadi kunci pribadi. Faktor yang menyebabkan tingginya tingkat keamanan adalah sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima dimana pemfaktoran ini dilakukan untuk mentukan kunci private.

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) (tidakrahasia)
5. SK (kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia)

Cara untuk membuat kunci:

1. Tentukan 2 bilangan integer prima besar misal nya kita sebut **p** dan **q**.
   Pilihlah **p** dan **q** dengan ukuran besar agar tingkat keamanan semakin besar.misal nya 1024 bit.
2. Tentukan n, dimana **n = p*q**
3. Tentukan m, dimana **m = (p-1)*(q-1)**
4. Pilih **e** yang relatively prime terhadap **m** . Dimana **e** relatively prime terhadap **m** artinya faktor pembagi terbesar keduanya adalah **1**, secara matematis disebut **gcd(e,m) = 1.**
   (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**

Cara untuk enkripsi:

Misal B mengenkripsi message M untuk A. Yang 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. Kirim C ke A

Cara untuk dekripsi:

Untuk mendekripsi A maka yang harus kita lakukan adalah Gunakan kunci pribadi d untuk menghasilkan M = C^(d) (mod n)

Contoh enkripsi dan dekripsi dengan kunci umum dan kunci pribadi:

Misalkan plainteks yang akan dienkripsikan adalah X = HARI INI
Jika dibuat dalam sistem desimal (pengkodean ASCII) adalah

H A R I (SPASI) I N I

72 65 82 73 32 73 78 73

Solusi :

Pecah X menjadi blok yang lebih kecil, misalnya X dipecah menjadi enam blok yang berukuran 3 digit:

- x1 = 726
- x2 = 582
- x3 = 733
- x4 = 273
- x5 = 787
- x6 = 003 (ditambah 0)

Proses pemecahan melihat dalam interval

[0,n-1) **à** 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.

Deskripsi :

215^1019 mod 3337 = 726 = x1

776^1019 mod 3337 = 582 = x2

1743^1019 mod 3337 = 733 = x3

933^1019 mod 3337= 273= x4

1731^1019 mod 3337= 787= x5

158^1019 mod 3337= 003= x6

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.