

Dasar Kriptografi

Fidens Felix VHS

<http://www.fidens.info>
ikc@fidens.info

Lisensi Dokumen:

Copyright © 2006 IlmuKomputer.Com

*Seluruh dokumen di **IlmuKomputer.Com** dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari **IlmuKomputer.Com**.*

Abstrak:

Kuliah ini dibuat berdasarkan catatan-catatan penulis sewaktu mengikuti kuliah di Universitas Osaka Department Information Science and Technology, tahun 2004.

Keywords: Kriptografi, DES

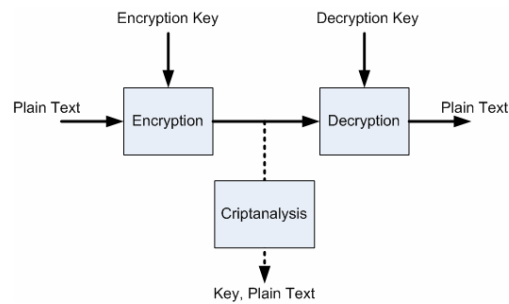
1. Sekilas Kriptografi

Kriptografi adalah ilmu yang berguna untuk mengacak (kata yang lebih tepat adalah *masking*) data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga. Tentu saja data yang diacak harus bisa dikembalikan ke bentuk semula oleh pihak yang berwenang.

Data yang ingin diacak biasanya disebut Plain Teks (*Plain Text*). Data diacak dengan menggunakan Kunci Enkripsi (*Encryption Key*). Proses pengacakan itu sendiri disebut Enkripsi (*Encryption*). Plain Teks yang telah diacak disebut Cipher Teks (*Chiper Text*). Kemudian proses untuk mengembalikan Cipher Teks ke Plain Teks disebut Dekripsi (*Decryption*). Kunci yang digunakan pada tahap Dekripsi disebut Kunci Dekripsi (*Decryption Key*).

Pada prakteknya, selain pihak yang berwenang ada pihak ketiga yang selalu berusaha untuk mengembalikan Cipher Teks ke Plain Teks atau memecahkan Kunci Dekripsi. Usaha oleh pihak ketiga ini disebut Kriptanalisis (*Cryptanalysis*).

Keseluruhan sistem kriptografi dirangkum pada Gambar 1.



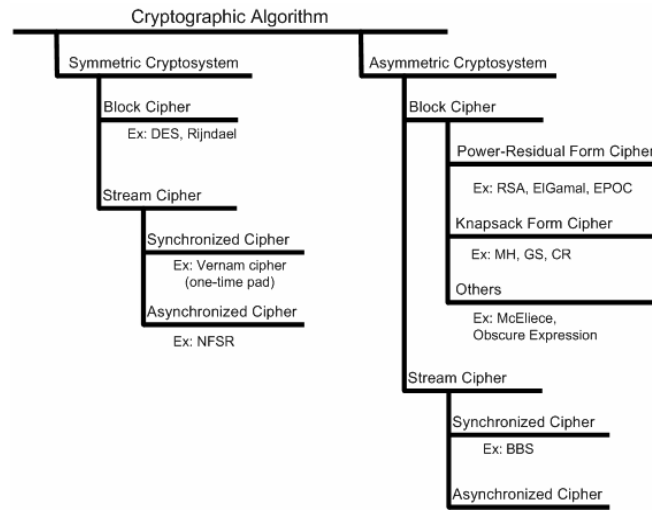
Gambar 1 Sistem Kriptografi

Konsep penggunaan kriptografi antara lain:

1. Kerahasiaan (*Confidentiality*).
Sederhananya, kerahasiaan adalah proses menyembunyikan data dari orang-orang yang tidak punya otoritas.
2. Integritas (*Integrity*)
Proses untuk menjaga agar sebuah data tidak dirubah-rubah sewaktu ditransfer atau disimpan.
3. Penghindaran Penolakan (*Non-repuditation*)
Proses untuk menjaga bukti-bukti bahwa suatu data berasal dari seseorang. Seseorang yang ingin menyangkal bahwa data tersebut bukan berasal darinya, dapat saja melenyapkan bukti-bukti yang ada. Karenanya diperlukan teknik untuk melindungi data-data tersebut.
4. Autentikasi (*Authentication*)
Proses untuk menjamin keaslian suatu data.
5. Tanda Tangan Data (*Data Signature*)
Dapat disebut juga sebagai tanda tangan digital. Berguna untuk menandatangani data digital. Contohnya adalah *Digital Signature Algorithm* (DSA)
6. Kontrol Akses (*Access Control*)
Untuk mengontrol akses terhadap suatu *entity*.

Contoh penggunaan kriptografi di dunia internet antara lain: Secure Shell (SSH), SSL (Secure Socket Layer), Secure Hypertext Transfer Protocol (HTTP), dan lain lain.

2. Pengelompokan Teknik Kriptografi



Gambar 2 Pengelompokan Enkripsi berikut contoh

Teknik kriptografi modern yang ada saat ini dapat dikelompokkan sebagaimana ditunjukkan pada Gambar 1. Kriptosistem Simetrik (*Symmetric Cryptosystem*) atau disebut juga Kunci Pribadi (*Private Key*) adalah metode kriptografi dimana kunci enkripsi bisa diperoleh dari kunci deskripsi atau sebaliknya. Kebalikan dari sistem ini adalah Kriptosistem Asimetrik (*Asymmetric Cryptosystem*) atau disebut juga Kunci Publik (*Public Key*). Kunci Pribadi disini berarti bahwa pemegang kunci enkripsi maupun dekripsi hanyalah pihak-pihak berwenang saja. Karena melihat kembali sifatnya, bila pihak ketiga memperoleh salah satu kunci tersebut maka dia bisa memperoleh kunci yang lain. Kunci Publik berarti Kunci Enkripsi dapat disebarluaskan ke publik sedangkan pihak berwenang cukup menjaga kerahasiaan Kunci Deskripsi.

Berdasarkan dari jenis data yang diolah, teknik kriptografi dapat dibagi menjadi dua bagian: *Block Cipher* dan *Stream Cipher*. Pada Block Cipher, sesuai namanya data Plain Teks diolah per blok data. Di lain pihak, pada Stream Cipher, data Plain Teks diolah per satuan data terkecil, misalnya per bit atau per karakter.

Teknik Kriptografi kemudian dibagi lagi menjadi dua kelompok, yaitu *Synchronized Cipher* dimana Kunci Enkripsi dan Kunci Dekripsi perlu disinkronisasi, dan *Asynchronized Cipher* dimana sinkronisasi tidak diperlukan. Stream Cipher dapat dibagi menjadi dua kelompok ini, sedangkan pada Block Cipher hanya ada *Synchronized Cipher*.

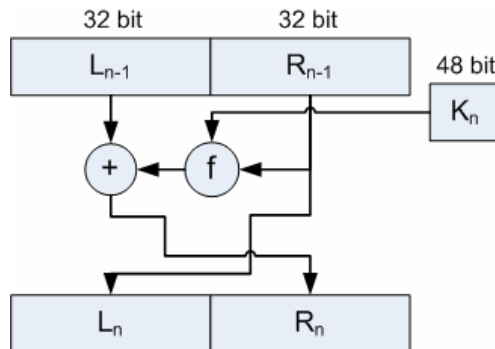
Power-Residual Form Cipher adalah teknik dimana dalam proses enkripsinya menggunakan rumus matematika $X^Y \pmod N$ atau rumus yang mirip seperti itu. *Knapsack Form Cipher* adalah teknik yang menggunakan *Knapsack Problem* yang merupakan problem komputasi kelas NP-Komplit (*NP-Complete/ NP-Hard*).

3. Lebih Detil Dengan Teknik Kriptografi (Studi Kasus DES)

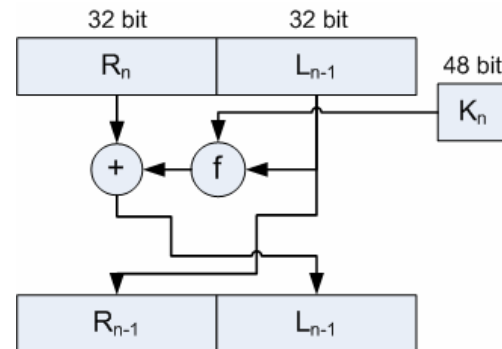
Kriptosistem Asimetrik biasanya menggunakan metode transformasi yang matematikal (biasanya cukup rumit). Ini berbeda dengan Kriptosistem Simetrik yang menggunakan metode seperti substitusi atau transposisi sebagai unsur dasar transformasinya. Substitusi adalah metode dimana huruf pada Plain Teks dirubah menjadi huruf tertentu yang lain. Misalnya: **a** dgn **z**, **b** dgn **y**. Transposisi adalah metode dimana urutan susunan huruf Plain

Teks diubah. Misalnya tiap-tiap 5 huruf yang berurutan dari Plain Teks urutannya dirubah dari 12345 ke 35412.

Contoh Kriptosistem Simetrik yang terkenal adalah DES (*Data Encryption Standard*). DES adalah Block Cipher yang menerima 64 bit data input dan mengeluarkan 64 bit data output. Panjang kunci yang digunakan adalah 64 bit (8 bit untuk *parity*, jadi panjang sebenarnya 56 bit). Proses enkripsi dan dekripsi dari DES digambarkan secara sederhana pada Gambar 3 dan Gambar 4, dimana $n = 0 \dots 15$.



Gambar 3 Proses Enkripsi DES



Gambar 4 Proses Dekripsi DES

Keterangan: Struktur pada Gambar 3 dan Gambar 4, dikenal sebagai Feistel Network.

\oplus = Eksklusif OR (XOR)

Pada proses enkripsi, input dari L_0 dan R_0 masing-masing adalah 32 bit terkiri dan terkanan dari 64 bit data Plain Teks yang telah ditransposisi sebelumnya. Kemudian, output dari L_{15} dan R_{15} adalah 64 bit data Cipher Teks. K_n adalah *Round Key* yang adalah kunci 48 bit yang diperoleh dari kunci 64 bit. Penjelasan proses penggenerasian Round Key, penulis serahkan pada buku-buku referensi. K_n menjadi input dari fungsi $f(R, K)$. Fungsi $f(R, K)$ ini adalah bisa berupa apa saja. Nanti akan dibuktikan bahwa proses enkripsi/dekripsi selalu benar untuk sembarang $f(R, K)$. Sekarang kita dapat merumuskan proses enkripsi sebagai berikut.

$$L_n = R_{n-1} \quad \dots (1)$$

$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n) \quad \dots (2)$$

Struktur proses dekripsi serupa dengan proses enkripsi, hanya input dan outputnya saja yang berbeda. Input dari fungsi f kali ini adalah 32 bit terkiri dari 64 bit data Cipher Teks. Proses dekripsi dirumuskan sebagai berikut.

$$R_n = L_{n-1} \quad \dots (3)$$

$$L_{n-1} = R_n \oplus f(L_n, K_n) \quad \dots (4)$$

Sekarang kita akan membuktikan bahwa dengan sembarang f kita bisa melakukan proses enkripsi-dekripsi.

Bukti:

Dengan melakukan operasi XOR dengan $f(L_n, K_n)$ pada sisi kiri dan kanan persamaan (2) kita memperoleh persamaan berikut.

$$f(R_{n-1}, K_n) \oplus R_n = L_{n-1} \quad \dots (5)$$

Dengan mensubstitusikan persamaan (1), kita peroleh persamaan berikut.

$$f(L_n, K_n) \oplus R_n = L_{n-1}$$

Persamaan ini adalah persamaan (4), yang membuktikan bahwa apapun bentuk f , proses enkripsi-dekripsi tetap berjalan dengan benar.

4. Penutup

Artikel ini telah menjelaskan sekilas tentang apa itu kriptografi dan apa penggunaannya. Kemudian telah dijelaskan pula pembagian teknik-teknik kriptografi yang ada sekarang. Terakhir, telah dijelaskan secara singkat tentang teknik enkripsi dan dekripsi pada kriptosistem DES.

Selama menggunakan fasilitas internet, hampir setiap saat kita bersentuhan dengan penerapan dari teknik kriptografi. Namun hal ini sering kita tidak sadari.

BIOGRAFI PENULIS



Fidens Felix VHS. Lahir di Jakarta, 29 April 1980 dan lulus dari SMU Negeri 8 Jakarta pada tahun 1997. Semasa SMU, penulis aktif mengikuti lomba matematika dan komputer serta terpilih menjadi anggota Tim Olimpiade Komputer Indonesia (TOKI) yang mewakili Indonesia pada Olimpiade Informatika Internasional 1997 di Cape Town. Melanjutkan pendidikannya ke Jepang pada tahun 1998 dengan sponsor pemerintah Jepang (Monbusho). Saat ini sedang menyelesaikan program S2 di Universitas Osaka. Fidens Felix VHS adalah member dari IEEE dan Computer Society.

Memiliki minat pada hal-hal yang berkaitan dengan masalah-masalah politik, khususnya politik internasional, ekonomi dan finansial. Bermotokan vision and action, dan senang mengisi waktu luang dengan kegiatan-kegiatan yang bertemakan self-improvement.

Informasi lebih lanjut tentang penulis ini bisa didapat melalui:

URL: <http://www.fidens.info>

Email: ikc@fidens.info