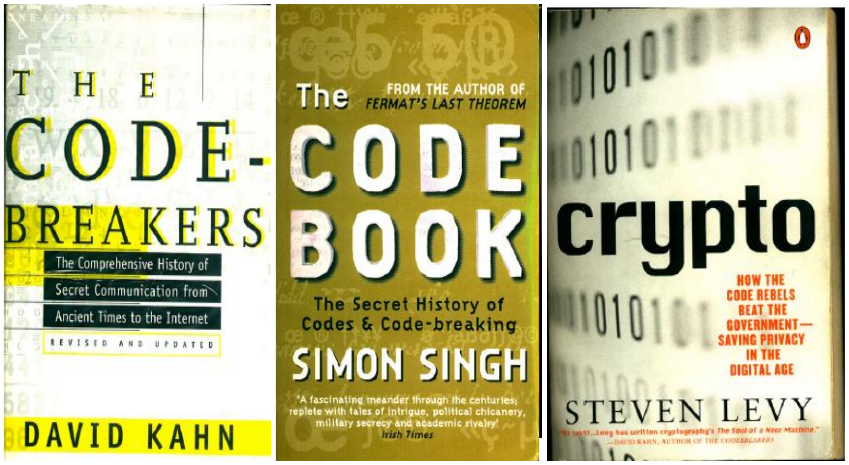
IlmuKomputer.Com
ikatlah ilmu dengan menuliskannya

Kriptografi Ikut Mewarnai Peradapan Dunia

Yendri Ikhlas Fernando
yendrifernando@gmail.com
http://yendrifernando.wordpress.com

Isi

Sebelum tahun 1970, kriptografi merupakan sebuah Dark Art karena masyarakat menganggap ilmu-ilmu yang berkaitan dengan kriptografi adalah ilmu yang mistis dan tidak diajarkan secara umum. Masyarakat menganggapnya sebagai sesuatu yang ajaib yang hanya diketahui caranya bagi orang-orang tertentu. Sampai pada akhirnya, fenomena ini terpecahkan oleh seorang jenius yang bernama David Khan dari India dengan bukunya "The Code Breakers" yang mengupas dunia 'kode'. Selain itu ada lagi buku yang serupa yaitu "Code Book" karya Simon Singh, "Crypto" karya Steven Levy.



Dunia kriptografi terus berkembang sampai pada akhirnya berubah menjadi tren dunia sendiri. Berasarkan data IEEE Spectrum, penyadapan di dunia internasional sudah biasa terjadi semenjak tahun 2003.

Sadap, Filter, Simpan

Sumber: IEEE Spectrum April 2003

Evolusi Pengamanan Data

Secara umum, teori pengamanan data terbagi menjadi 2 kategori besar, yaitu :

1. Steganography = membuat data seolah-olah tidak ada, padahal data itu ada hanya saja disamarkan.

Contoh :

- Sejarah mencatat ketika terjadi peperngan antara Yunani (Greek) vs Persia. Pesan yang disampaikan melalui meja yang dilapisi lilin untuk meyamarkan pesan tersebut.
- Sejarah juga pernah mencatat bahwa pesan disampaikan melalui kepala-kepala budak saat itu yang dibotak dan ditulis sejumlah pesan.
- Kalau saat ini, Steganography bisa kita temukan pada Digital Watermarking yaitu menandai kepemilikan gamabr digital salah satunya dengan menggunakan LSB (Lower Significant Bit) dari pixel sebagai bagian dari pesan. Bisa juga diterapkan di audio (mp3), video , dan format digital lainnya untuk menjadi bagian dari Digital Rights Management (DRM)

2. Cryptography. Ada yang menggunakan metode Tranposition dan ada juga Substitusion .

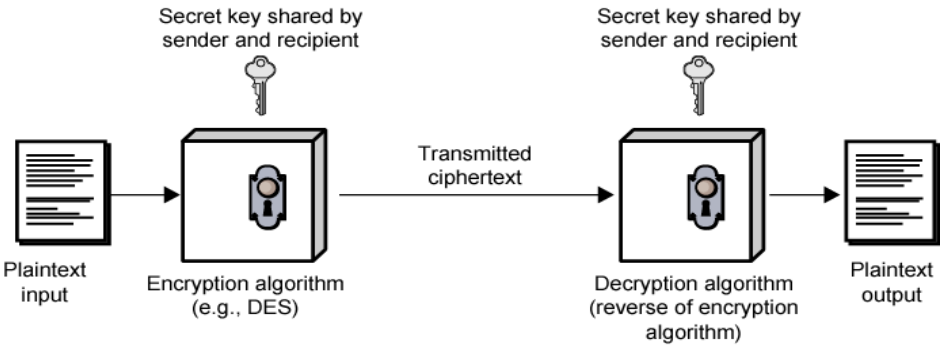
Crptography sebenarnya merupakan suatu ilmu atau seni dalam mengamankan pesan. Pelakunya disebut Cryptographer. Sedangkan Cryptanalysis merupakan ilmu atau seni untuk membuka Cryptography tadi dan orang yang melakukannya disebut Cryptanalyst.

Cryptography juga disebut studi tentang enkripsi dan dekripsi data berdasarkan konsep matematis. Orang yang pintar dalam Cryptografy biasanya memiliki matematika yang kuat pula. Cryptography meningkatkan keamanan data dengan cara menyamarkan dalam bentuk yang tidak dapat dibaca.

Istilah-istilah dalam Cryptografi :

- Plaintext : Data asli
- Ciphertext : Pesan yang dienkripsi
- Enkripsi : Proses dari Plaintext ke Ciphertext
- Dekripsi : Proses dari Ciphertext ke Plaintext
- Key : bilangan atau aturan yang dirahasiakan yang berfungsi untuk proses enkripsi dan dekripsi.

Skemanya seperti ini.



Contoh :

- Lagi-lagi sejarah mencatat seorang Queen Mary yang dihukum pancung karena teknik Cryptography nya kurnag ampuh dalam mengirim pesan penentangan kepada Ratu Elizabeth kepada kelompoknya sehingga diketahui oleh agen-agen kerajaan.

Algoritma Cryptography/Kriptografi Klasik

Ciri-ciri :

- Berbasis karakter
- Masih menggunakan pena, belum ada komputer
- Tergolong kunci yang Simetri

Algoritmanya terbagi menjadi 2, yaitu :

- Cipher Substitusi. Algoritma ini terbagi 4 lagi, yaitu :
  Monoalfabet = setiap karakter ciphertext menggantikan 1 macam karakter plaintext.
  Polyalfabet = setiap karakter ciphertext menggantikan lebih dari 1 macam karakter plaintext.
  Monograf = 1 enkripsi dilakukan terhadap 1 karakter plaintext.
  Polygraf = 1 enkripsi dilakukan terhadap lebih dari 1 karakter plaintext.

* Tiap huruf alfabet digeser 3 huruf ke kanan
  p_i : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
  c_i : **D E F G H I J K L M N O P Q R S T U V W X Y Z A B C**

* Contoh:
  Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX
  Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

Teori seperti diatas pernah dicatat sejarah, yaitu seorang Caesar Cipher yang kodenya terpecahkan oleh Muslim Al Kindi yang mencari huruf yang paling sering muncul pada ciphertext lalu diluruskan dengan huruf yang paling sering muncul di plaintext.

Sejarah lain seperti Enigma Motor, sebuah mesin enkripsi milik Jerman pada Perang Dunia 2 yang digunakan untuk mengirim pesan kepada seluruh pasukan yang tidak dimengerti oleh lawan. Cara membacanya juga menggunakan mesin yang sama kembali, namun pada akhirnya dapat dilumpuhkan oleh Sekutu dengan bantuan Alan Turing kala itu.

- Cipher Transposisi. Algoritma ini mengubah posisi rangkaian huruf di dalam plaintext.
  Contoh :
  Misalkan plainteks adalah
  POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

  Enkripsi:
  POLITEK
  NIKELEK
  TRONIKA
  NEGERIS
  URABAYA

Cipherteks: (baca secara vertikal)
PNTNUOIRERLKOGAIENEBTLIRAEEKIYKKASA
PNTN UOIR ERLK OGAI ENEB TLIR AEEK IYKK ASA

Algoritma Kriptograpi Modern

Ciri-ciri :

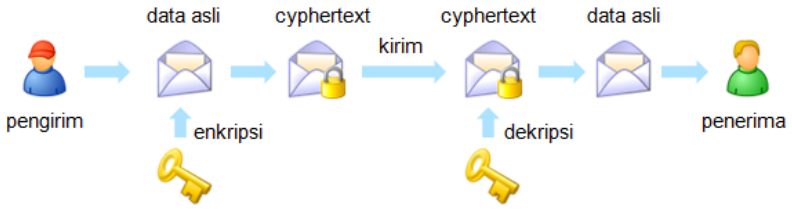
- Berbasi bit
- Key, Ciphertext, Plaintext diproses dalam bit
- Masih menggunakan Algoritma Subsitusi dan Transposisi
- Didorong karena penggunaan pesan digital lewat komputer yang merepresentasikan data dalam biner

Algoritma Kriptografi Berdasarkan Jenis Key(kunci) :

- Algoritma Simetris = kunci yang sama untuk enkripsi & dekripsi

Problem

- Bagaimana mendistribusikan kunci secara rahasia ?
- Untuk n orang pemakai, diperlukan n(n-1)/2 kunci → tidak praktis untuk pemakai dalam jumlah banyak



Kelebihan :

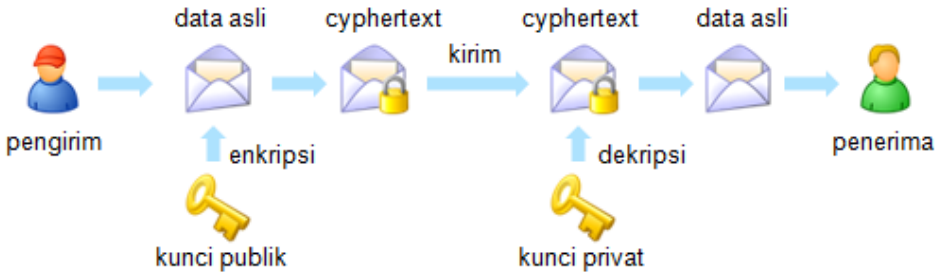
- Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
- Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time*

Kelemahan

- Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
- Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"*

- Algoritma Asimetri = Kunci enkripsi tidak sama dengan kunci dekripsi. Kedua kunci dibuat oleh penerima data

enkripsi → kunci publik
dekripsi → kunci privat



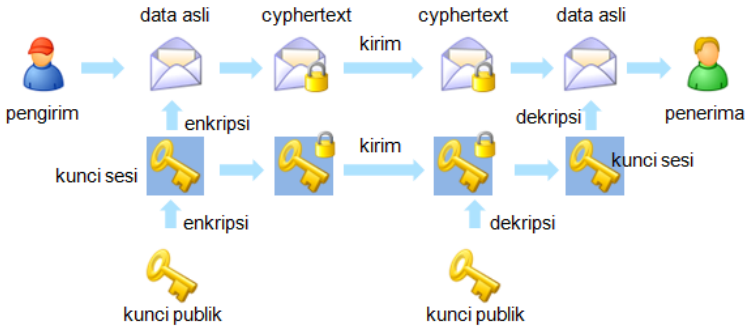
Kelebihan :

- Masalah keamanan pada distribusi kunci dapat lebih baik
- Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan :

- Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
- Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.
  Contoh : RSA, DH, ECC, DSA

Algoritma Hibrid (Penggabungan Simetri dan Asimetri)



Algoritma Kriptografi Berdsarkan Besar Data yang diolah :

- Algoritma Block Cipher
  Contoh :
  Tergolong Simetri = DES, IDEA, AES
- Algoritma Stream Cipher
  Contoh : OTP, A5, RC4

Algoritma Fungsi Hash :

- Contoh :
  MD5, SHA1

Penutup

Demikian dulu penjelasan singkat tentang kriptografi. Ternyata sepanjang sejarah dunia, kriptografi memegang peran penting didalamnya.

Referensi

Slide Nazarudin Syafaat H, MT

Biografi Penulis

Yendri Ikhlas Fernando. Lahir di Riau, tanggal 27 Rabiul Awal 1413 H, 20 September 1992 M. Saat sekarang ini menempuh pendidikan S1 Jurusan Teknik Informatika, Universitas Islam Negeri Sultan Syarif Kasim Riau. Motivator "Islamic-Techo Motivator" di Counselling Training Center (CTC) Indonesia. Aktif sebagai kader dakwah di Lembaga Dakwah Kampus (LDK) Al Karamah UIN Suska Riau.