# Pertemuan 5

Sesi 1 dan 2

# Dasar-dasar keamanan Sistem Informasi

Ayu Firdhayanti (IIB Darmajaya)

Keamanan Sistem Informasi

# DASAR-DASAR KEAMANAN SISTEM

IIB DARMAJAYA

# Pengamanan Informasi



David Khan dalam bukunya “*The Code-breakers*”

membagi masalah pengamanan informasi menjadi dua kelompok; *security* dan *intelligence*.

1. Security dikaitkan dengan pengamanan data,
2. Intelligence dikaitkan dengan pencarian (pencurian, penyadapan) data.

Pengamanan data dapat dilakukan dengan dua cara,

Yaitu ***steganography*** dan ***cryptography*****.**

# Steganografi




## Steganografi

Berasal dari bahasa Yunani yaitu Steganós yang berarti menyembunyikan dan Graptos yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan.

Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

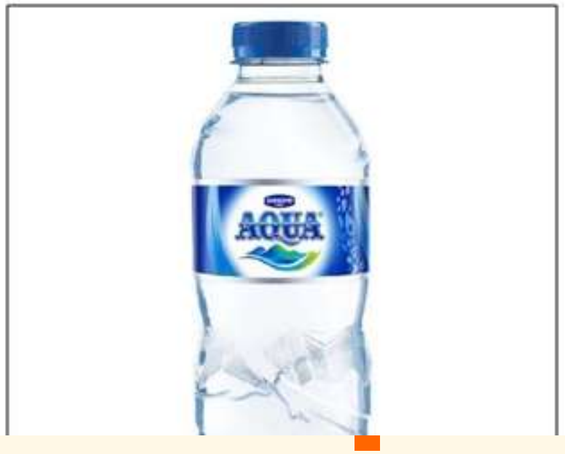
# Steganografi Gambar



**Citra Asli**


+

**Citra Yang Disisipkan**




=

**Citra Hasil Penyisipan**

# Steganografi Teks



## Contoh Steganografi

### Teks

Pesan rahasia dikirimkan dengan mengirim surat pembaca ke sebuah surat kabar. Huruf awal setiap kalimat (atau bisa juga setiap kata) membentuk pesan yang ingin diberikan.

Cara lain adalah dengan membuat puisi dimana huruf awal dari setiap baris membentuk kata-kata pesan sesungguhnya

**Kulihat wajahnya**
**Lidah pun tak dapat berkata**
**Ahh, kenapa harus begini**

**Hatipun tak tenang**
**Rintihan tak kunjung hilang**

**Sejujurnya ku tak sanggup**
**Ninggalkanmu**

Steganografi pada saat ini banyak diterapkan dengan menggunakan *file-file* digital dan menggunakan *file-file* multimedia sebagai kedok untuk menyembunyikan pesan rahasia, baik itu berupa gambar, suara, atau video yang biasa disebut *digital watermarking*.

Steganografi

Berikut adalah beberapa istilah yang sering digunakan dalam teknik steganografi:

- Carrier file : *file* yang berisi pesan rahasia tersebut
- Steganalysis : proses untuk mendeteksi keberadaan pesan rahasia dalam suatu *file*
- Stego-medium : media yang digunakan untuk membawa pesan rahasia
- Redundant bits : sebagian informasi yang terdapat di dalam *file* yang jika dihilangkan tidak akan menimbulakn kerusakan yang signifiakan (setidaknya bagi indera manusia)
- Payload : informasi yang akan disembunyikan

# Kriptografi

# Kriptografi



Kriptografi

"*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Cryptography adalah sebuah kumpulan teknik yang digunakan untuk mengubah informasi/pesan (*plaintext*) kedalam sebuah teks rahasia (ciphertext) yang kemudian bisa diubah kembali ke format semula.

Pelaku atau praktisi kriptografi disebut ***cryptographers***. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut **cipher**, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.

# Kriptografi



*Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. Pelaku/praktisinya disebut *Cryptanalyst, sedangkan Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*.

# Kriptografi

Pengamanan dengan menggunakan *cryptography* membuat pesan nampak. Hanya bentuknya yang sulit dikenali karena seperti diacak-acak.

Pada *cryptography* pengamanan dilakukan dengan dua cara, yaitu transposisi dan substitusi.

a. Pada penggunaan transposisi, posisi dari huruf yang diubah-ubah,
b. Pada penggunaan substitusi, huruf (atau kata) digantikan dengan huruf atau simbol lain.

# Dasar-dasar Enkripsi

# Dasar-dasar Enkripsi



Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) sehingga tidak dapat dibaca oleh orang yang tidak berhak adalah **enkripsi** (*encryption*) atau disebut "e*ncipher*".

Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** (*decryption*) atau disebut "*decipher*".

Data disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (*private key cryptography*) atau dengan kunci yang berbeda (*public key cryptography*).

# Dasar-dasar Enkripsi



Secara matematis, proses atau fungsi enkripsi (*E*) dapat dituliskan sebagai: *E(M) = C*

Proses atau fungsi dekripsi (*D*) dapat dituliskan sebagai: *D(C) = M*

dimana: *M* adalah *plaintext* (*message*) dan *C* adalah *ciphertext*.

# Kriptografi Simetris



Kriptografi kunci simetri berarti menggunakan kunci yang sama untuk proses enkripsi maupun dekripsi. Pada prosesnya, pengirim pesan dan penerima pesan harus saling berbagi kunci rahasia tersebut

# kriptografi asimetris



**Kriptografi kunci publik** (disebut juga **kriptografi asimetris**) adalah sistem kriptografi yang menggunakan sepasang kunci, yaitu (1) kunci publik yang bisa disebarkan dan (2) kunci pribadi yang hanya diketahui oleh pemilik. Pembuatan kunci tersebut bergantung pada algoritme kriptografi yang menggunakan sifat matematis untuk menghasilkan fungsi satu arah. Keamanannya secara efektif hanya berasal dari kunci pribadi yang disimpan dengan baik; kunci publik dapat disebarkan tanpa mengurangi keamanannya

# Kriptografi ***Hybrid***



Kriptografi hibrida merupakan algoritma yng memanfaatkan dua tingkatan kunci yaitu kunci rahasia simetris dengan satu kunci (session key) dan enkripsi asimetris dengan sepasang kunci (public/private key) kriptografi hibrida diharapkan akan memberi keamanan yang lebih baik terhadap pengiriman informasi dengan rasio ...

# Infrastruktur Kunci Publik



Pengamanan komunikasi data untuk keperluan publik (antar institusi, individu-institusi, individu-individu, dsb)

– Kebutuhan komunikasi yang aman

– Heterogenitas pemakai

– Jaringan komunikasi yang kompleks

Komponen infrastruktur kunci publik:

– Tandatangan digital (digital signature): untuk menjamin keaslian dokumen digital yang dikirim

– Otoritas Sertifikat (certificate authority): lembaga yang mengeluarkan sertifikat digital sebagai bukti kewenangan untuk melakukan transaksi elektronis tertentu

# Infrastruktur Kunci Publik (lanjutan)

## Mengapa diperlukan ?



– Kasus KlikBCA beberapa tahun yang lalu

• Ada orang yang meniru persis situs netbanking Bank BCA, dengan URL yang mirip

---

• Situs tersebut menerima informasi login dari nasabah BCA (userID dan password)

• Apa yang terjadi jika informasi login nasabah disalahgunakan ?

– Semakin banyaknya transaksi elektronik yang memerlukan legalitas secara elektronik juga

• Dokumen kontrak

• Perjanjian jual beli

# Algoritma kriptografi klasik:



- Chiper Substitusi (Substitution Chipers)

- Chiper Transposisi (Transposition Chipers)

# Chiper Substitusi



• Ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga caesar chiper), untuk menyandikan pesan yang ia kirim kepada para gubernurnya.

• Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet).

• Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad.

Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu k = 3).

## Tabel substitusi:

• p: 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: 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

1. Pesan

AWASI ASTERIX DAN TEMANNYA OBELIX

disamarkan (enskripsi) menjadi

DZDVL DVWHULA GDQ WHPDQQBA REHOLA

• Penerima pesan men-dekripsi chiperteks dengan menggunakan tabel substitusi, sehingga

chiperteks “DZDVL DVWHULA GDQ WHPDQQBA REHOLA “

dapat dikembalikan menjadi plainteks semula:

• AWASI ASTERIX DAN TEMANNYA OBELIX

# Chiper Transposisi (Transposition Chipers)



- Pada chiper transposisi, plainteks tetap sama, tetapi urutannya diubah. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks.

- Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

# Chiper Transposisi



- Pada chiper transposisi, plainteks tetap sama,

tetapi urutannya diubah. Dengan kata lain,

algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks.

- Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

# Contoh

Misalkan plainteks adalah

DEPARTEMEN TEKNIK KOMPUTER BSI

• Untuk meng-enkripsi pesan, plainteks ditulis secara horizontal dengan lebar kolom tetap, misal selebar 6 karakter (kunci k = 6):

DEPART

EMENTE

KNIKKO

MPUTER

BSI

• maka chiperteksnya dibaca secara vertikal menjadi

DEKMBEMNPSPEIUIANKTRTOETEOR

## Data Encryption Standard (DES)

dikenal sebagai Data Encryption Algorithm (DEA)

oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini.

Aplikasi yang menggunakan DES antara lain:

- enkripsi dari password di sistem UNIX,
- berbagai aplikasi di bidang perbankan

Enigma Rotor Machine

Enigma rotor machine merupakan sebuah alat enkripsi dan dekripsi mekanik yang digunakan dalam perang dunia ke dua oleh Jerman.

## Aplikasi dari Enkripsi

• Contoh penggunaan enkripsi adalah program Pretty Good Privacy (PGP), dan secure shell (SSH).

- Program PGP digunakan untuk mengenkripsi dan menambahkan digital signature dalam e-mail yang dikirim.
- Program SSH digunakan untuk mengenkripsi sesion telnet ke sebuah host.

## Kelemahan Enkripsi

1. Penanganan yang salah atau kesalahan manusia, Kurangnya manajemen data enkripsi
2. Kekurangan dalam cipher itu sendiri
3. Serangan brute force

# Thank You!

Any Questions?