PROGRAM STUDI TEKNIK INFORMATIKA
Sekolah Teknik Elrektro dan Informatika

INSTITUT TEKNOLOGI BANDUNG

Pengenalan Kriptografi dan Steganografi untuk Keamanan Informasi

RINALDI MUNIR

Lab Ilmu dan Rekayasa Komputasi
Kelompok Keahlian Informatika

Institut Teknologi Bandung

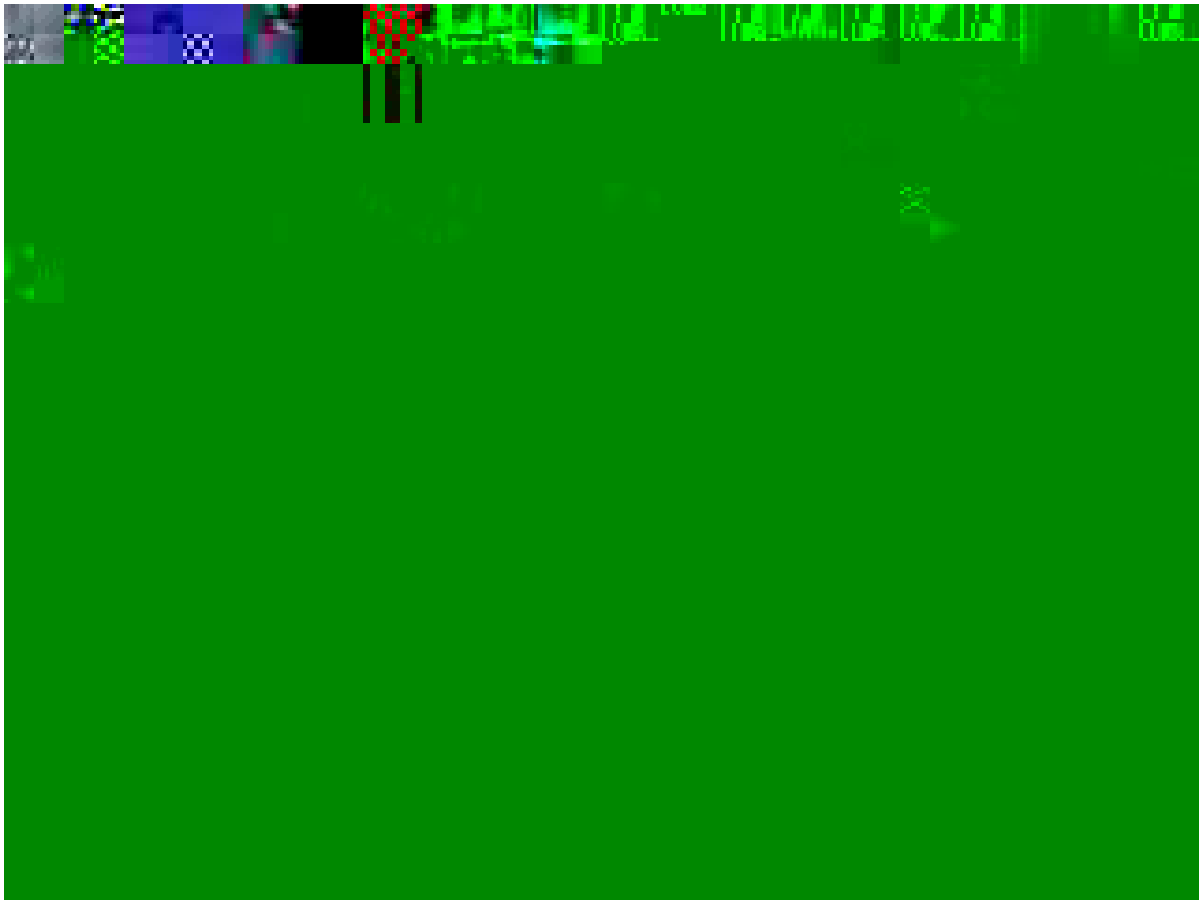
Bisakah anda mengerti informasi berikut ini?

Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/• p}âpx;
épêp/|t}t|äzp}/qp}êpz/étzp{x/zt• xâx
}vêp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
ppsp{pw/p}pz<p}pz/zt• xâx}v/êp}
v/qpüä|t}tâpé/spüx/sp{p|/• péxü=/]
p{äüx|ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pwât| pâ/ztwxsä• p}/|tützp=

(a)

(b)

atau video berikut:



(c)

Jika tidak bisa membacanya, ini informasi aslinya:

Ketika saya berjalan-jalan di pantai, saya menemukan banyak sekali kepiting yang merangkak menuju laut. Mereka adalah anak-anak kepiting yang baru menetas dari dalam pasir. Naluri mereka mengatakan bahwa laut adalah tempat kehidupan mereka.

(a)

(b)


Total Video Converter
http://effectmatrix.com
THE FOLLOWING PREVIEW HAS BEEN APPROVED FOR
ALL AUDIENCES
BY THE MOTION PICTURE ASSOCIATION OF AMERICA
THE FILM ADVERTISED HAS BEEN RATED
PG PARENTAL GUIDANCE SUGGESTED
SOME MATERIAL MAY NOT BE SUITABLE FOR CHILDREN
FOR SCARY MOMENTS, SOME CREATURE VIOLENCE
AND MILD LANGUAGE

(c)

- Informasi yang tidak bisa dimengerti maknanya itu dinamakan *ciphertext.*

- Sebaliknya informasi yang dapat dimengerti maknanya dinamakan *plaintext*.

- *Plaintext* dapat ditransformasikan menjadi *ciphertext*, begitu pula sebaliknya.

- Transformasi *plaintext* menjadi *ciphertext* dilakukan dengan menggunakan **kriptografi** (*cryptography*).

- Kata *cryptography* berasal dari bahasa Yunani: κρυπτο (*hidden* atau *secret*) dan γραφη (*writing*)

  Artinya "*secret writing*"

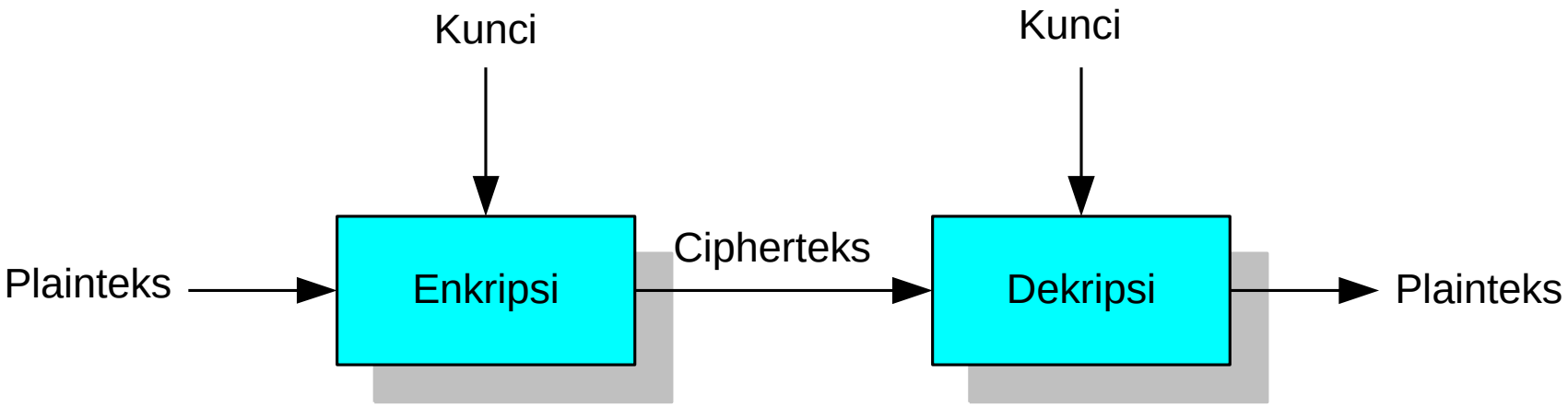
  Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

- Istilah kriptografi dalam Bahasa Indonesia: **Ilmu Persandian**

Kriptografi terdiri dari dua proses:

1. **Enkripsi**: transformasi dari plainteks menjadi cipherteks
2. **Dekripsi**: transformasi dari cipherteks menjadi plainteks

Kedua menggunakan **kunci** rahasia



- Mengapa kriptografi saat ini sangat penting?

  → untuk menjaga kerahasiaan informasi

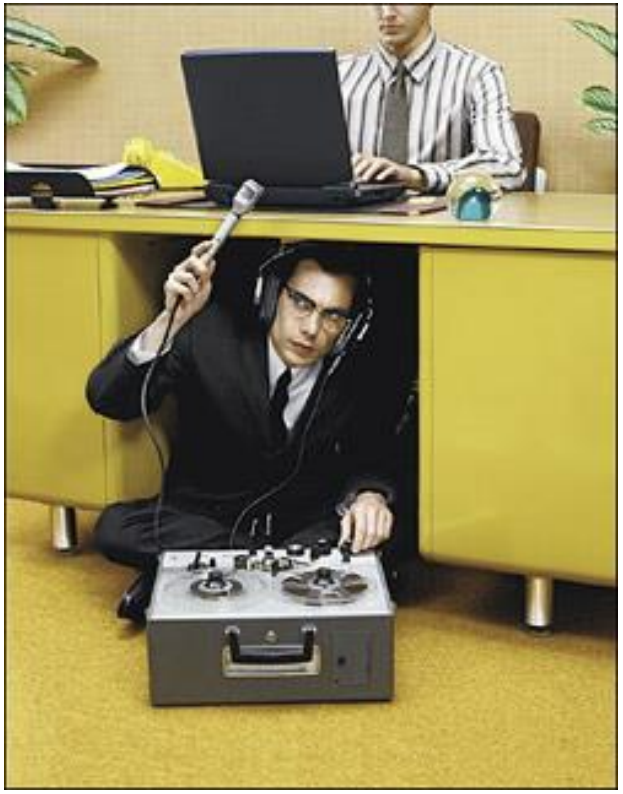
  - data/informasi rahasia negara
  - data/informasi rahasia organisasi
  - data/informasi personal

- Pada era digital saat ini, pertukaran informasi rawan terhadap penyadapan oleh pihak ketiga.

- Kriptografi berguna untuk melakukan pengamanan informasi yang rahasia agar tidak bocor kepada publik.

Penyadapan

1. Wiretapping



15506-41DG
'Office: 9am' Disc
© JupiterImages

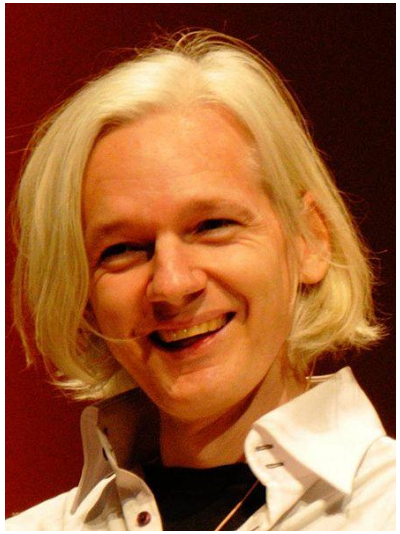
Creatas
www.comstock.com

2. Acoustic Eavesdropping

3. Electromagnetic eavesdropping

Masih ingat dengan kasus2 berikut?

1. **Wikileaks**: mengungkapkan dokumen-dokumen rahasia negara dan perusahaan kepada publik melalui situs web.



Julian Assange, salah satu pendiri situs WikiLeaks.

Kantor dan tempat penyimpanan data WikiLeaks.

Dokumen yang dibocorkan:

1. Data Nasabah Bank Julius Baer
2. Surel Sarah Palin
3. Video Helikopter Apache
4. Perang Afganistan
5. Berkas Guantanamo
5. Dokumen Perang Irak
6. Kawat diplomatik Amerika Serikat

(Sumber: Wikpedia)

2. Kasus penyadapan percakapan ponsel antara Artalyta Suryani (Ayin) dan Kemas Yahya Rahman yang melibatkan Jaksa Urip Tri Gunawan tentang “dugaan” suap Rp 6 Milyar lebih.

Transkrip percakapan:

A: Halo..
K: Halo.
A: Ya, siap.
K: Sudah dengar pernyataan saya (Soal penghentian penyelidikan kasus BLBI)? He…he…he
A: Good, very good.
K: Jadi tugas saya sudah selesai.
A: Siap, tinggal…
K: Sudah jelas itu, gamblang. Tidak ada permasalahan lagi

A: Bagus itu

K: Tapi saya dicaci maki. Sudah baca Rakyat Merdeka (surat kabar Rakyat Merdeka yang terbit di Jakarta)?

A: Aaah Rakyat Merdeka, mah nggak usah dibaca

K: Bukan, katanya saya mau dicopot ha..ha…ha. Jadi gitu ya…

A: Sama ini Bang, saya mau informasikan

K: Yang mana?

A: Masalah si Joker.

K: Ooooo nanti, nanti, nanti.

A: Nggak, itu kan saya perlu jelasin, Bang

K: Nanti, nanti, tenang saja.

A: Selasa saya ke situ ya…

K: Nggak usah, gampang itu, nanti, nanti. Saya sudah bicarakan dan sudah ada pesan dari sana. Kita…

A: Iya sudah

K: Sudah sampai itu

A: Tapi begini Bang…

K: Jadi begini, ini sudah telanjur kita umumkan. Ada alasan lain, nanti dalam perencanaan

Menyingkap Dunia Penyadapan (1)

Pejabat Gerah Gunakan Ponsel

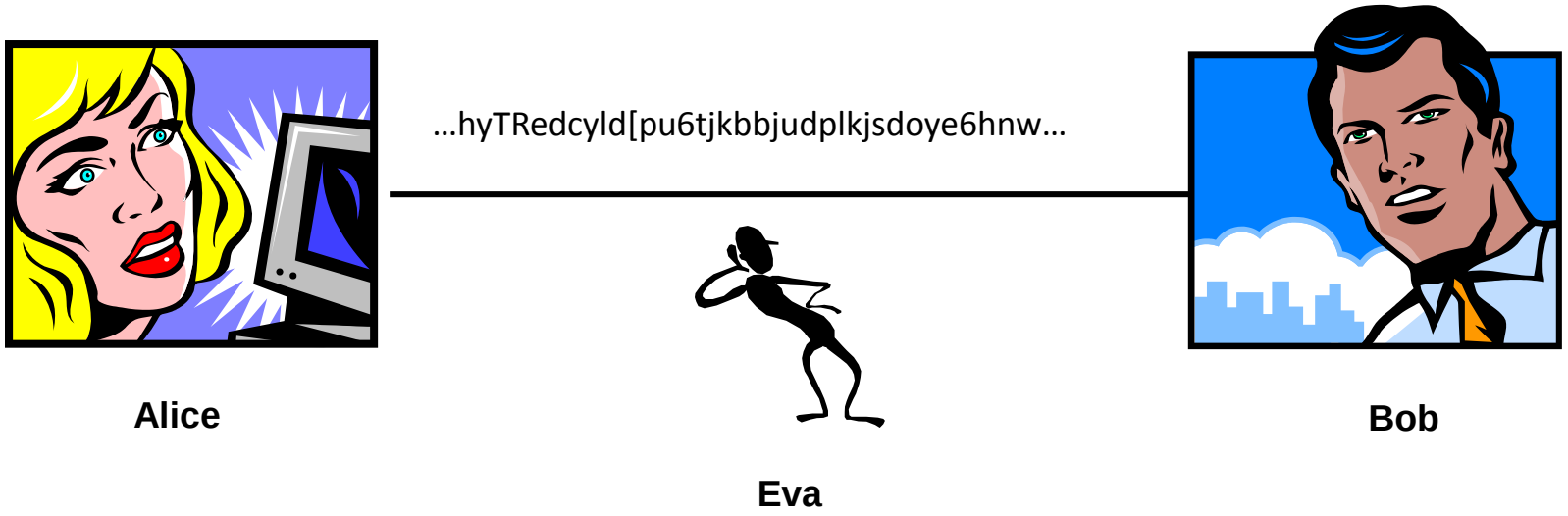
Sjamsir Siregar - inilah.com/Abdul Rauf

INILAH.COM, Jakarta Penyadapan seperti jadi dunia terang benderang di Pengadilan Tipikor. Apa saja yang dikatakan Artalyta Suryani, tersangka kasus penyuapan jaksa, diumbar. Seperti apa sebenarnya penyadapan? Bagaimana aturannya?

Suara Sjamsir Siregar terdengar keras dari balik teleponnya. "Aku sedang sibuk bekerja. Kalau mau bertemu, silahkan. Tapi nantilah dicarikan waktu. Kalau bicara di telepon, jangan! Banyak penyadapan sekarang. Sudah ya, aku mau sholat Jumat dulu," kata Kepala Badan Intelijen Negara (BIN) itu.

Moral of the story:

Kasus-kasus kebocoran informasi dan penyadapan tersebut menunjukkan bahwa KROPTIGRAFI itu sangat penting untuk dipelajari, digunakan, dan dikembangkan.



Dengan ilmu dan teknologi kriptografi, informasi disajikan dalam bentuk *ciphertext* sehingga pihak ketiga tidak dapat memahami artinya.

Data Encryption on Motion

- Sinyal yang ditransmisikan dalam percakapan dengan *handphone.*
- Nomor PIN kartu ATM yang ditransmisikan dari mesin ATM ke komputer bank.
- Nomor PIN kartu kredit pada transaksi *e-commerce* di internet.
- Siaran televisi berbayar (Pay TV)
- Pesan melalui *BlackBerry Messenger* (BBM)

Data Encryption at Rest

1. Dokumen teks

Plainteks (`plain.txt`):

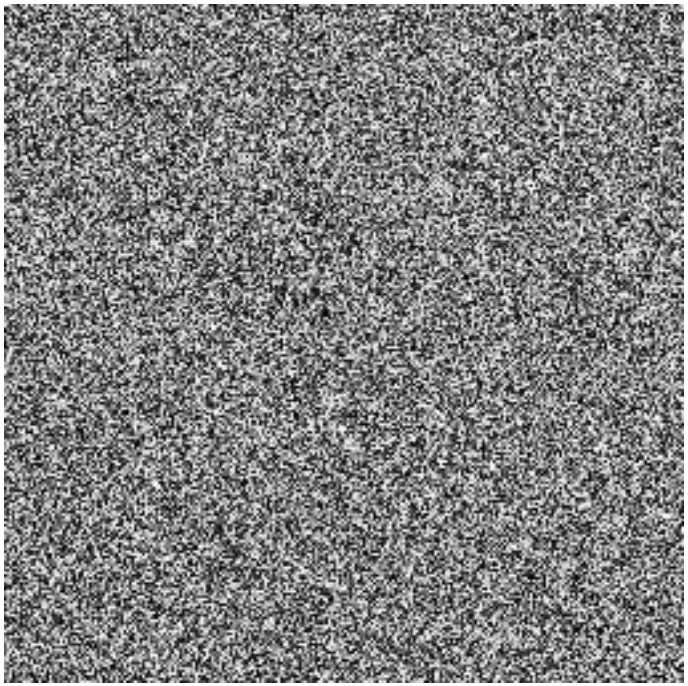
```
Ketika saya berjalan-jalan di pantai,
saya menemukan banyak sekali kepiting
yang merangkak menuju laut. Mereka
adalah anak-anak kepiting yang baru
menetas dari dalam pasir. Naluri
mereka mengatakan bahwa laut adalah
tempat kehidupan mereka.
```

Cipherteks (`cipher.txt`):

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/□p}âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/zt□xâx
}v  êp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
p  psp{pw/p}pz<p}pz/zt□xâx}v/êp}
v/qpüä  |t}tâpé/spüx/sp{p|/□péxü=/]
p{äüx  |ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pw  ât|□pâ/ztwxsä□p}/|tützp=
```

2. Dokumen Gambar

Plain image



Cipher image

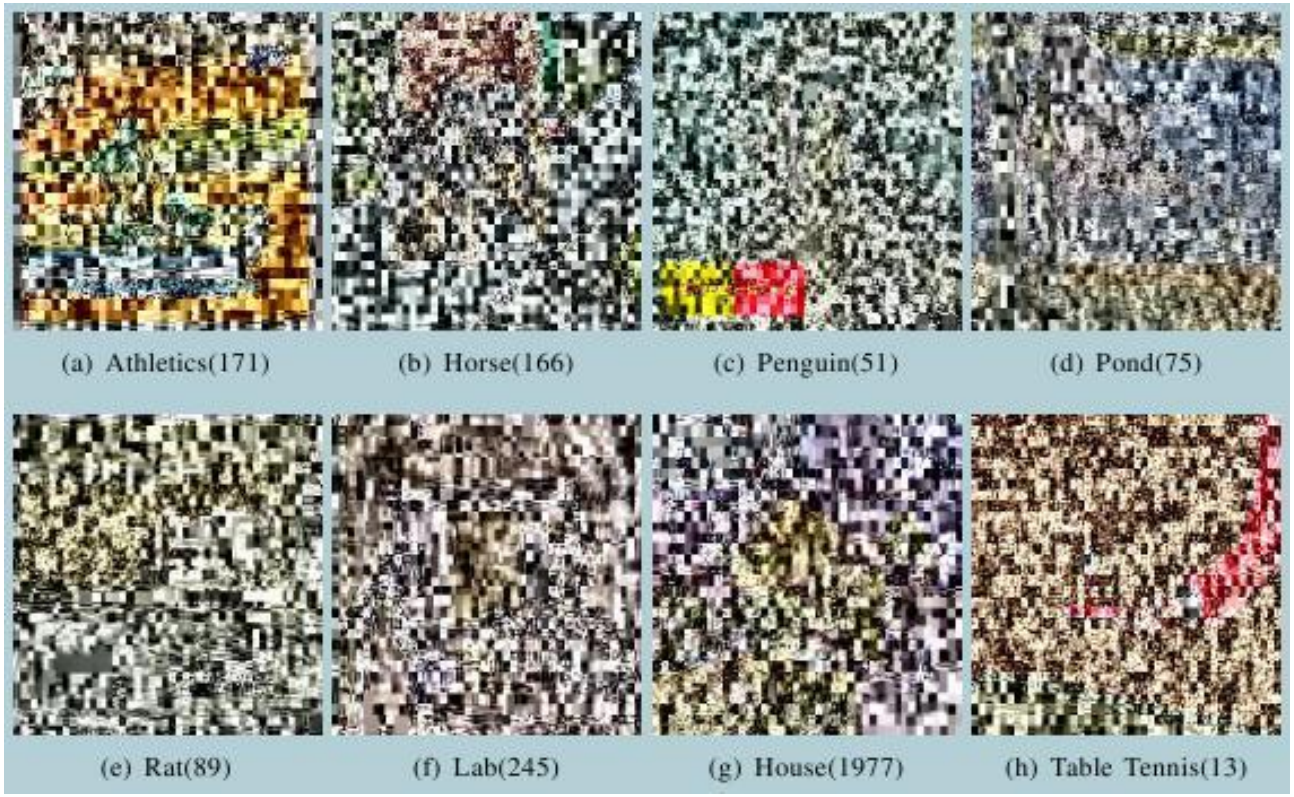
3. Dokumen Basisdata

Cipherteks (`siswa2.dbf`):

NIM	Nama	Tinggi	Berat
000001	tüp}vzpz/|t}äyä/{ää	|äzp}	épêp
000002	|t}tâpé/spüx/sp	péxü=	ztwxsä□
000003	ât|□pâ/ztwxsä□p}/|	}/|tü	spüx/
000004	épêp/|t}t|äzp}/qpêpz	qp}êpz	wxsä
000005	étzp{x/zt□xâx}v êp}	päâ/psp	étzp{
000006	spüx/sp{p|/□péxü=/]	xâx}v	ttüzp/|
000007	Ztâxzp/épêp/qtüypp}<	äzp}	}äyä/{
000008	qpwåp/{päâ/psp{pw	Ztwxs	xâx}v
000009	}t|äzp}/qp}êpz/ép{	qp}êp	äzp}/qp

Keterangan: hanya *field* Nama, Berat, dan Tinggi yang dienkripsi.

4. Video


(a) Athletics(171)
(b) Horse(166)
(c) Penguin(51)
(d) Pond(75)
(e) Rat(89)
(f) Lab(245)
(g) House(1977)
(h) Table Tennis(13)

Elemen Kriptografi

1. **Algoritma kriptografi (*cipher*)**

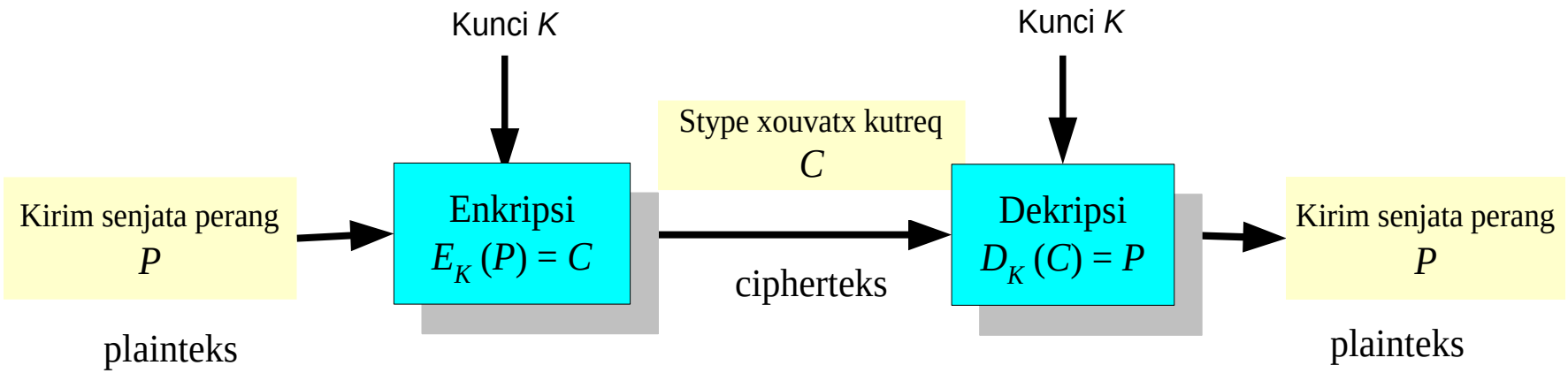
   Aturan untuk *encryption* dan *decryption,* atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

2. **Kunci**

   Parameter yang digunakan untuk transformasi *encryption* dan *decryption.* Kunci bersifat rahasia (*secret*), sedangkan algoritma kriptografi tidak rahasia (*public*)

3. **Pesan**

   Informasi yang di-enkripsi/dekripsi


Kunci K
Kunci K
Stype xouvatx kutreq
C
Kirim senjata perang
P
Enkripsi
$E_K(P) = C$
cipherteks
Dekripsi
$D_K(C) = P$
Kirim senjata perang
P
plainteks
plainteks

Algoritma Kriptografi

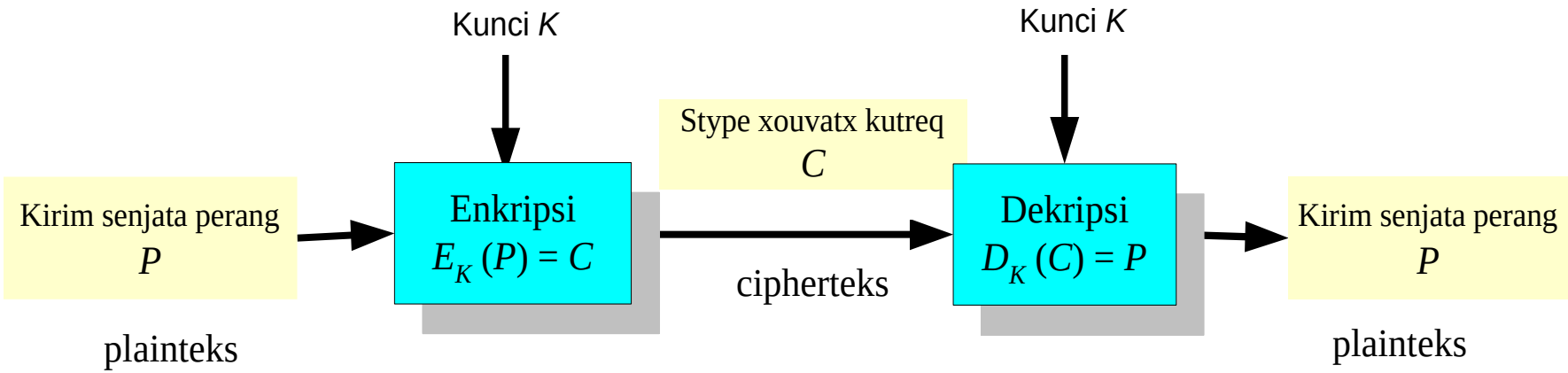
1. Algoritma kriptografi kunci-simetri
   (*symmetric-key cryptography*)

2. Algoritma kriptografi kunci-publik
   (*public-key cryptography*)

3. Fungsi Hash

Kriptografi kunci-simetri

- *Symmetric-key cryptography*
- Kunci enkripsi = kunci dekripsi

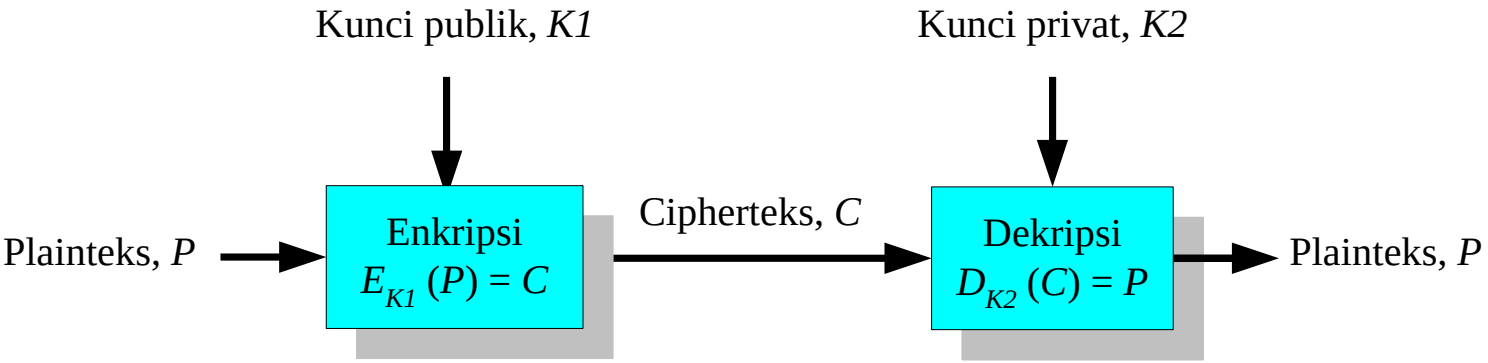


- Contoh algoritma kriptografi kunci-simetri:

-*DES* (*Data Encyption Standard*)
- AES
-Blowfish
- SEED
- IDEA
- GOST
-Serpent
- RC4, RC5, dll

Kriptografi kunci-publik

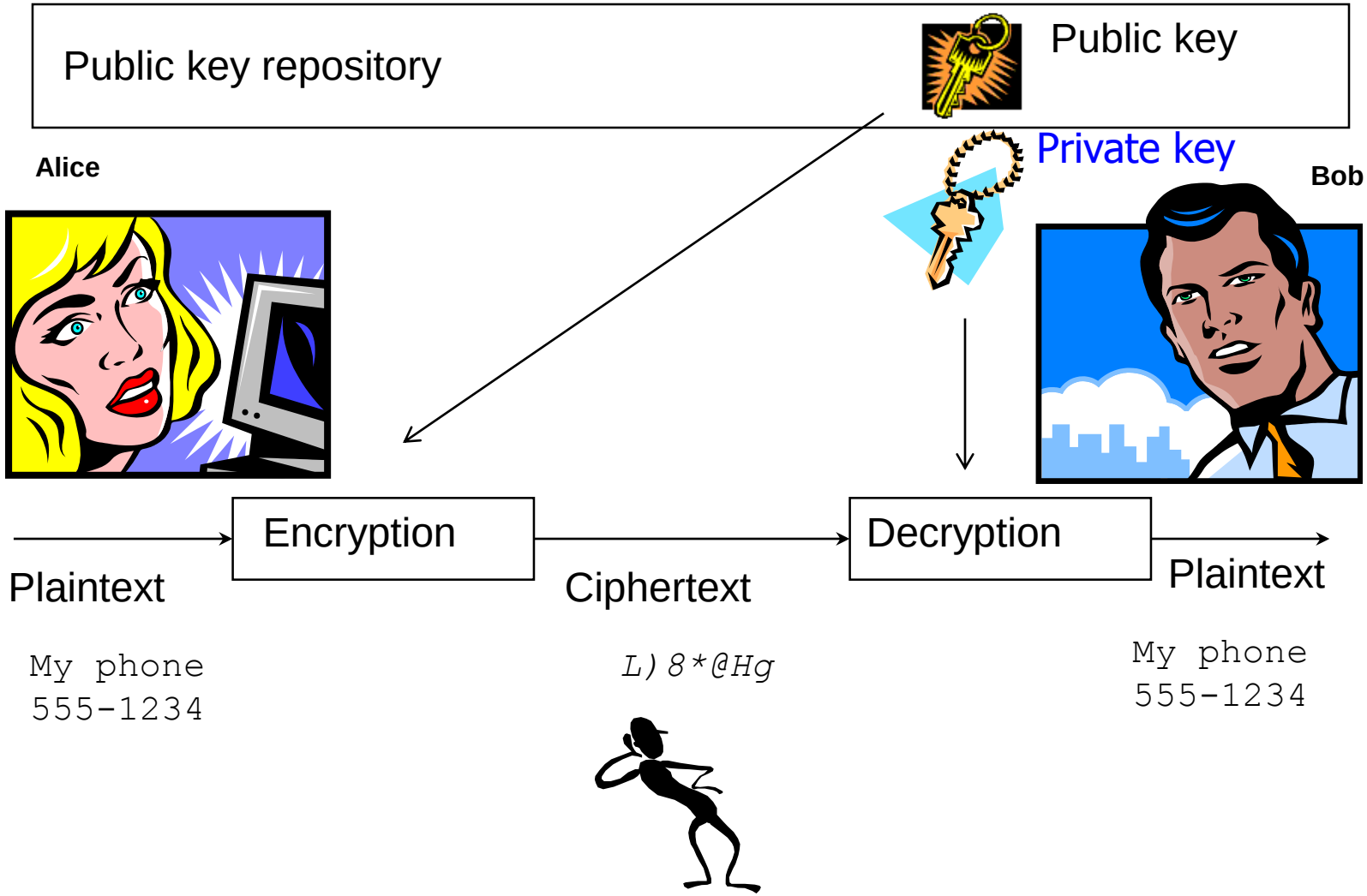
- Kunci enkripsi ≠ kunci dekripsi
- Nama lain: **kriptografi kunci-publik**
- Kunci enkripsi bersifat publik (*public key*) sedangkan kunci dekripsi bersifat rahasia (*secret key* atau *private key*).



- Contoh algoritma kriptografi kunci-simetri:
  - RSA
  - ElGamal
  - Rabin
  - Diffie-Hellman Key Exchange
  - DSA
  - Elliptic Curve Cryptography (ECC)

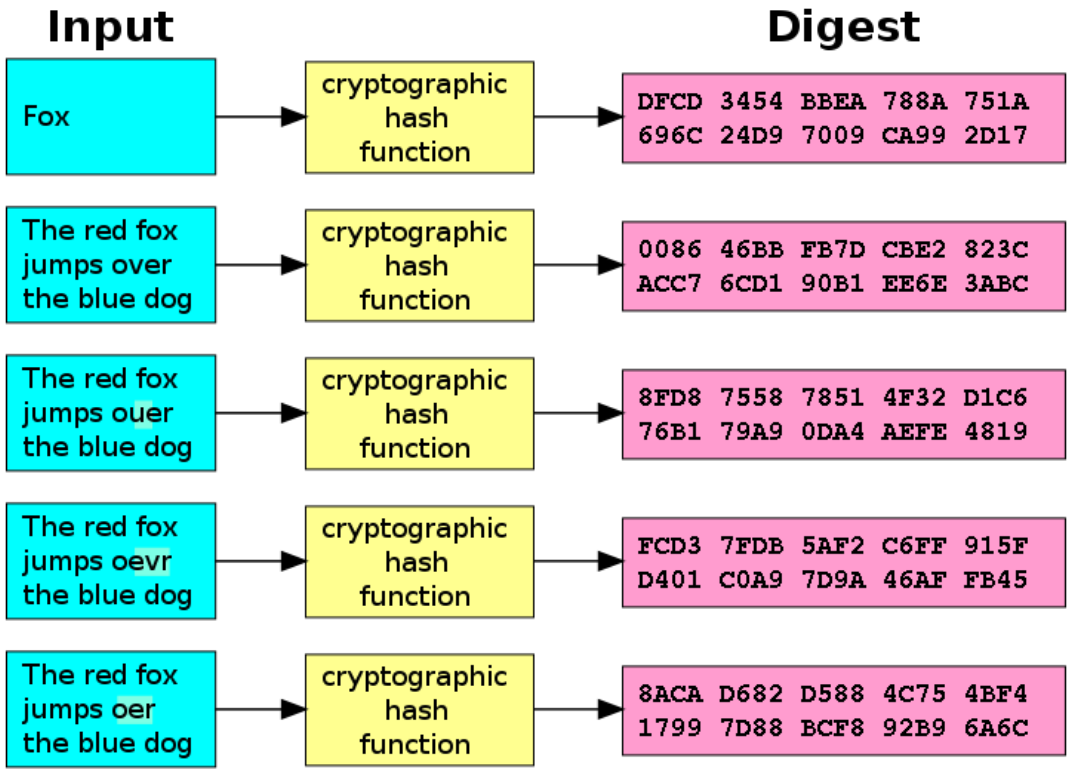
Kriptografi Kunci-publik

(http://budi.insan.co.id/courses/ec7010)



Fungsi *Hash*

- Mengkompresi pesan menjadi ukuran sangat kecil dan *fixed*
- Sensitif terhadap manipulasi sekecil apapun



Contoh:

(i) Pesan (berupa *file*) asli

Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa lebih panas dari hari-hari biasanya. Menurut laporan Dinas Meteorologi Kota Bandung, suhu tertinggi kota Bandung adalah 33 derajat Celcius pada Hari Rabu, 17 Oktober yang lalu. Suhu terseut sudah menyamai suhu kota Jakarta pada hari-hari biasa. Menurut Kepala Dinas Meteorologi, peningkatan suhu tersebut terjadi karena posisi bumi sekarang ini lebih dekat ke matahari daripada hari-hari biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah penduduk yang padat, polusi dari pabrik di sekita Bandung, asap knalpot kendaraan, ikut menambah kenaikan suhu udara kota.

Nilai MD5: **2F82D0C845121B953D57E4C3C5E91E63**

(ii) Misal 33 diubah menjadi 32

Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa lebih panas dari hari-hari biasanya. Menurut laporan Dinas Meteorologi Kota Bandung, suhu tertinggi kota Bandung adalah 32 derajat Celcius pada Hari Rabu, 17 Oktober yang lalu. Suhu terseut sudah menyamai suhu kota Jakarta pada hari-hari biasa. Menurut Kepala Dinas Meteorologi, peningkatan suhu tersebut terjadi karena posisi bumi sekarang ini lebih dekat ke matahari daripada hari-hari biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah penduduk yang padat, polusi dari pabrik di sekita Bandung, asap knalpot kendaraan, ikut menambah kenaikan suhu udara kota.

Nilai MD5: **2D1436293FAEAF405C27A151C0491267**

Sebelum diubah : $MD5_1$ = **2F82D0C845121B953D57E4C3C5E91E63**
Sesudah diubah : $MD5_2$ = **2D1436293FAEAF405C27A151C0491267**
Verifikasi: $MD5_1 \neq MD5_2$ (arsip sudah diubah)

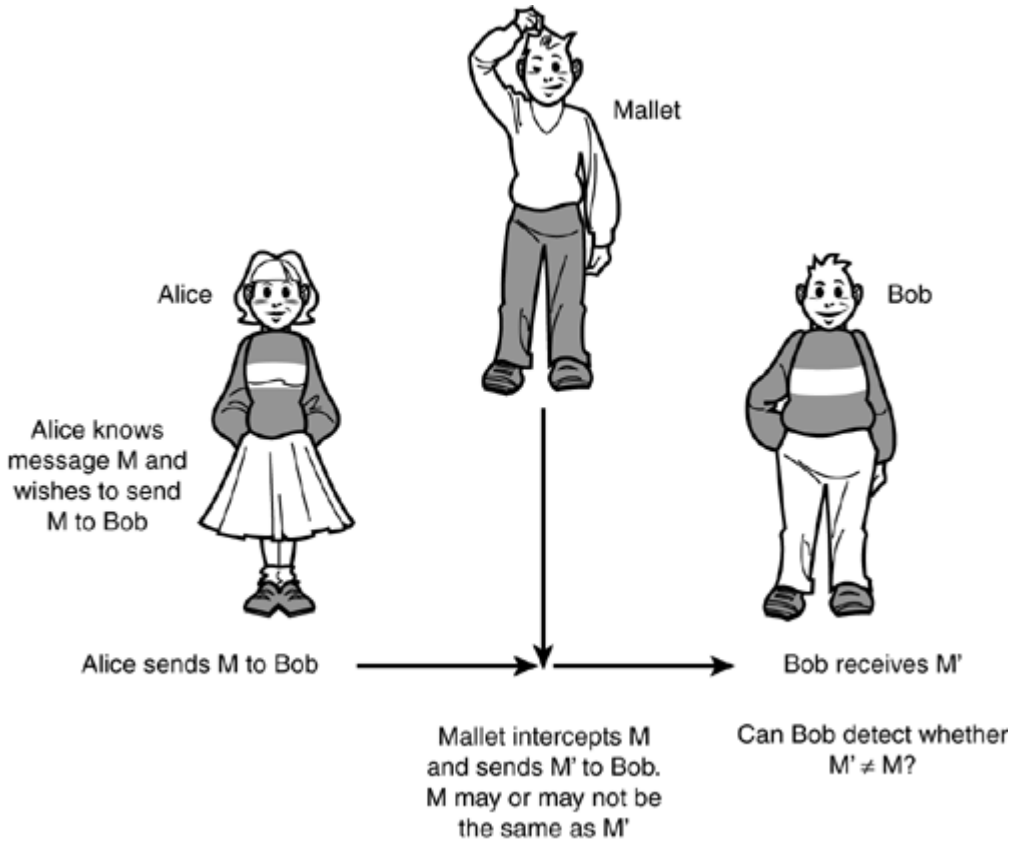
Kegunaan Kriptografi

1. **Kerahasiaan (*confidentiality*)**

   Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.

2. Integritas data (*data integrity*)

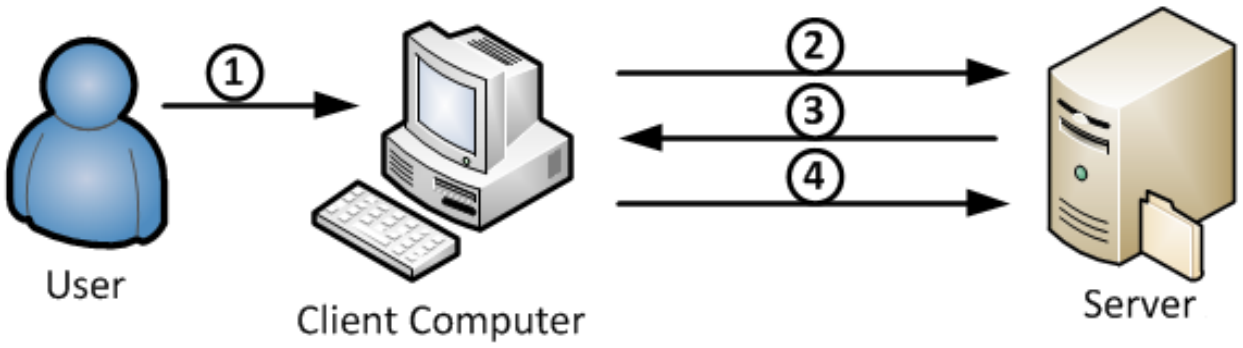
Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.



3. **Otentikasi** (*authentication*)

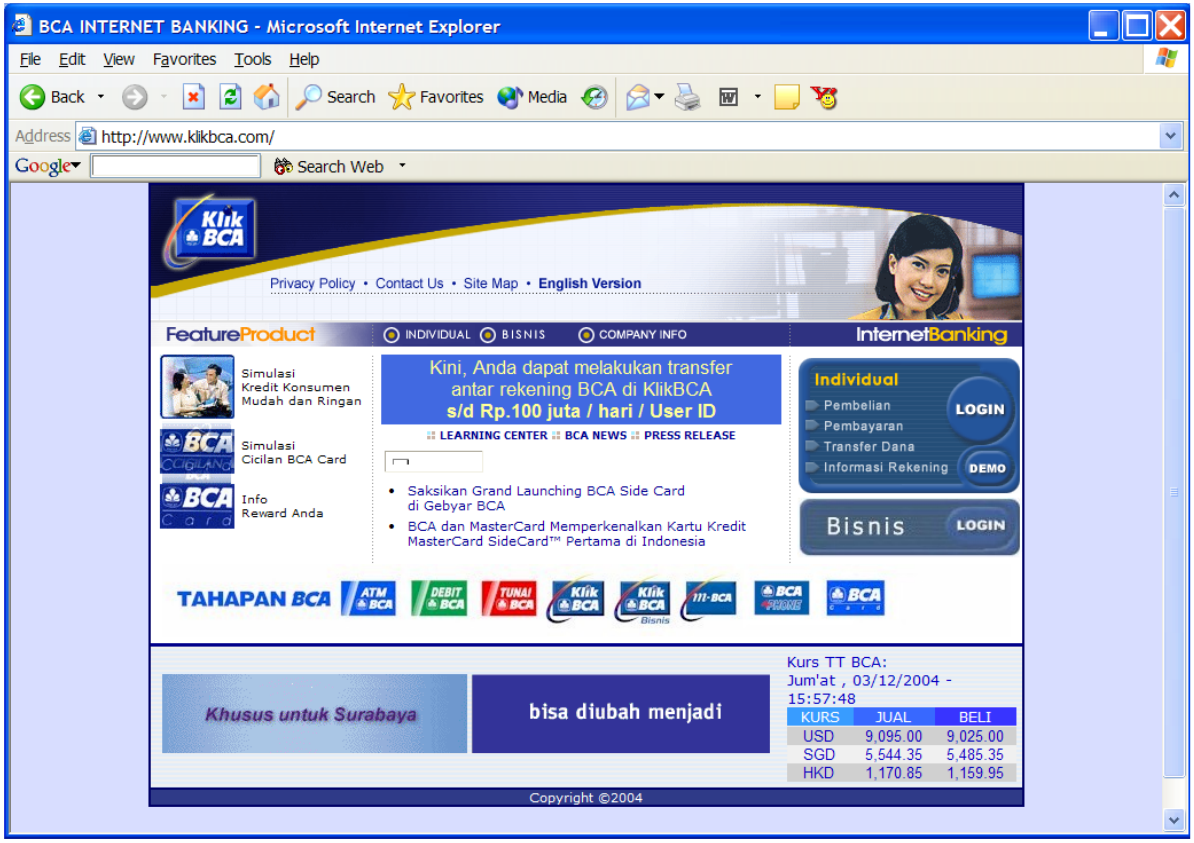
   Layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication)*

   "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?"



- Contoh kasus pemalsuan otentikasi (*phising*)

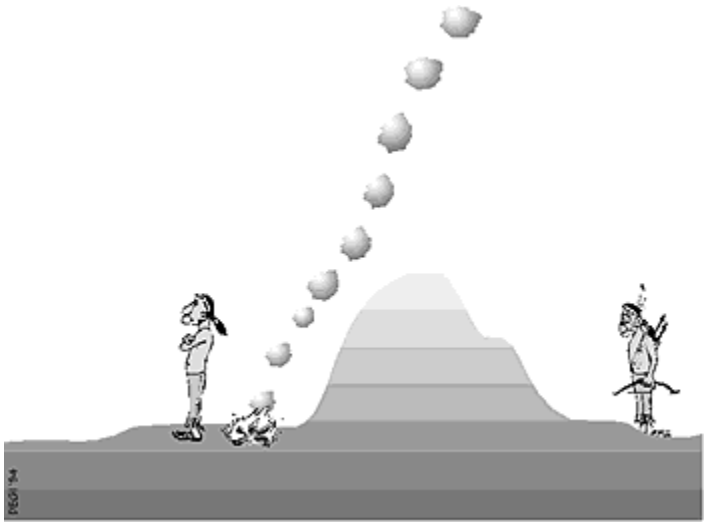
Web Bank BCA: www.klikbca.com



Situs palsu mirip Bank BCA: www.kilkbca.com, www.clickbca.com, www.klickbca.com

4. **Nirpenyangkalan** (*non-repudiation*)

Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.



Saat ini….

Kehidupan kita saat ini dikelilingi oleh kriptografi, mulai:

- ATM tempat mengambil uang,
- Telepon genggam (HP),
- Komputer di lab/kantor,
- Internet,
- Gedung-gedung bisnis,
- sampai ke pangkalan militer

Lembaga Terkait Kriptografi

- Di Indonesia:

  1. Lembaga Sandi Negara (Lemsaneg)

     (*National Crypto Agency*), http://www.lemsaneg.go.id/

  2. Sekolah Tinggi Sandi Negara (STSN)

     http://stsn-nci.ac.id/

- Di Amerika

  1. National Security Agency (NSA)

Steganografi

- Selain melakukan penyandian dengan kriptografi, informasi juga dapat diamankan dari *unauthorized access* dengan menggunakan steganografi.

- ***Steganography***: ilmu dan seni menyembunyikan pesan rahasia ke dalam media lain sehingga keberadaannya tidak terdeteksi.

Ledakkan bom pukul 20.00 WIB

Perbedaan Kriptografi dan Steganografi

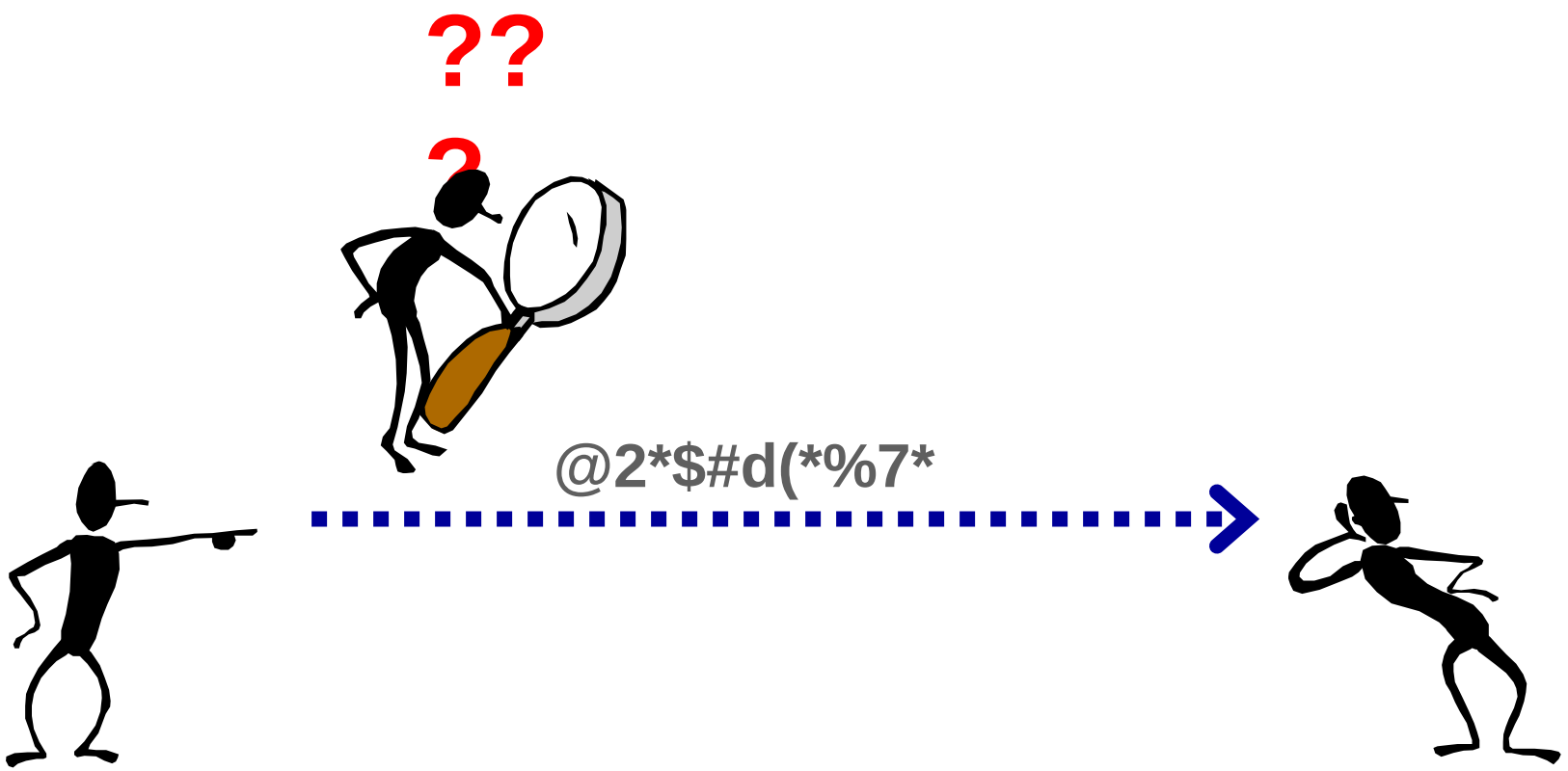
- Kriptografi: menyembunyikan ***isi*** (*content*) pesan

  → Tujuan: agar pesan tidak dapat dibaca oleh pihak ketiga (lawan)

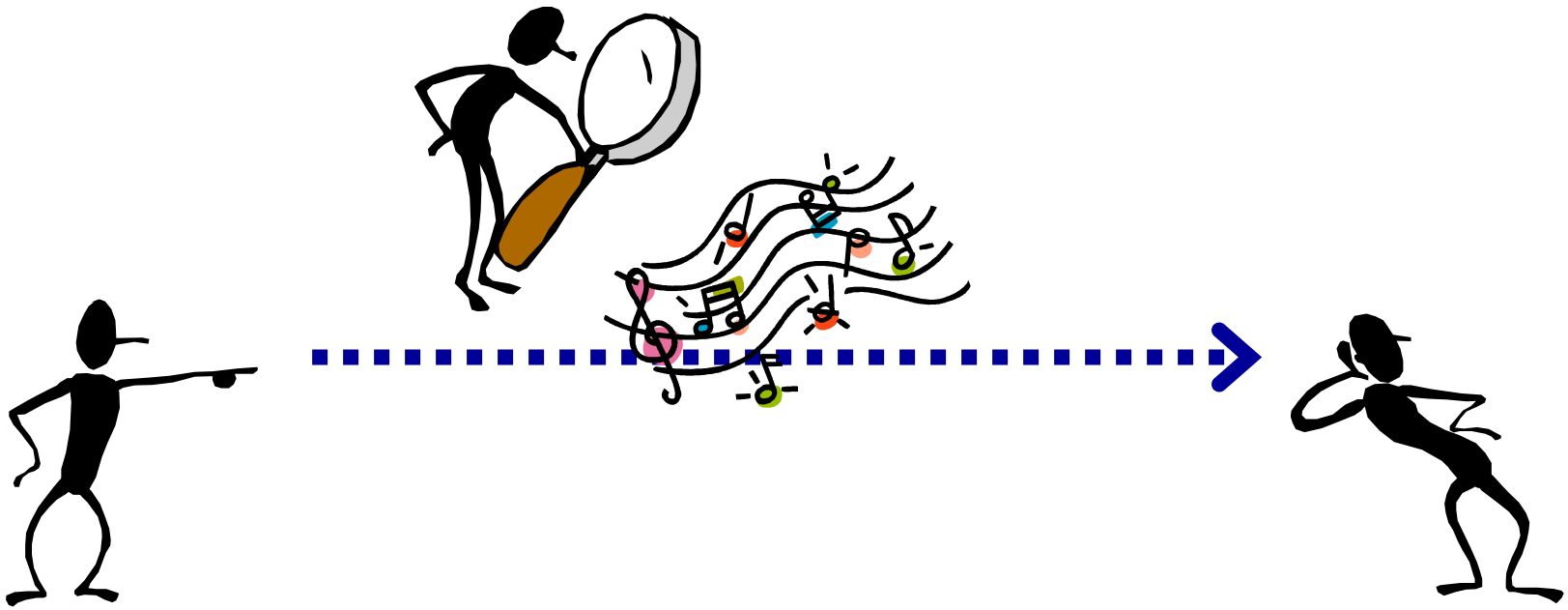
- Steganografi: menyembunyikan ***keberadaan*** (*existence*) pesan

  → Tujuan: untuk menghindari kecurigaan (*conspicuous*) dari pihak ketiga (lawan)

Kriptografi

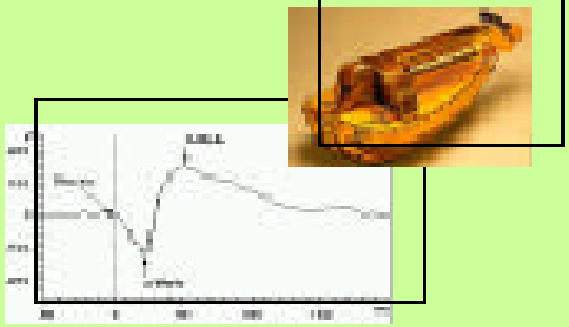


Steganografi



Stego-data are inconspicuous. Steganography will **not be detected**.

George obtains oranges yet eights' are rubbish!



Encrypted messages are conspicuous. They will be detected as ciphertext or silly data.

hlwDlwFpbAtjdf0BA/9KBX2jS17O5SRQsu2PF
caBqUXlQdyt1Fri/Wsg+eXoYsxnJI1Cn2JD7vjl
F2GH8GEr/vGQk8SQVCMyXzfPkgW0tr6RJX
AEIFF9rjnDB3kOmmVc1adrTQnLrqiC/I5r/kJs
ezowgZl82T/QVk59YsuChd+Ce8vql/klCeqmv
w9J2amre3uxpWlOqCEQNzZyHx8HeYPf29k
Xu+uk1gekZZVdELmLD/Wa/xBKFTNUBrl+16
ewoQBxQ8+3cTXSlGPTqdzDSasgQG17Z1sr
/Lhu0qze+m64GYY0OukeiCPvhHJQuXZn2UW

Steganografi Digital

- Steganografi digital: penyembunyian pesan digital di dalam dokumen digital lainnya.
- *Carrier file*: dokumen digital yang digunakan sebagai media untuk menyembunyikan pesan.

1. Teks

"Kita semua bersaudara"

-Txt
- doc
- html

2. Audio

- wav
- mp3

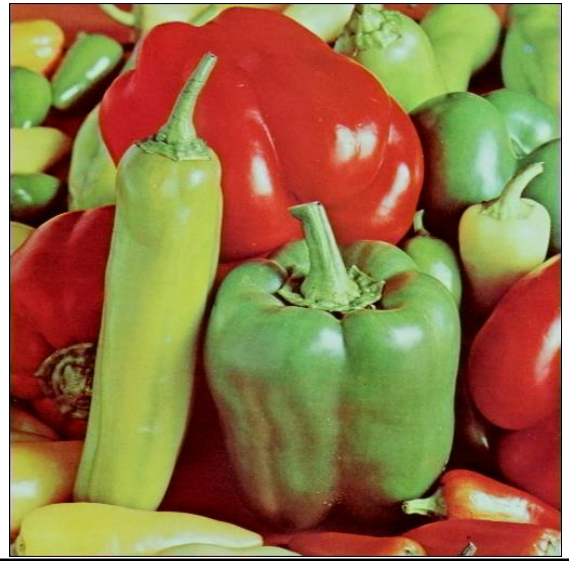
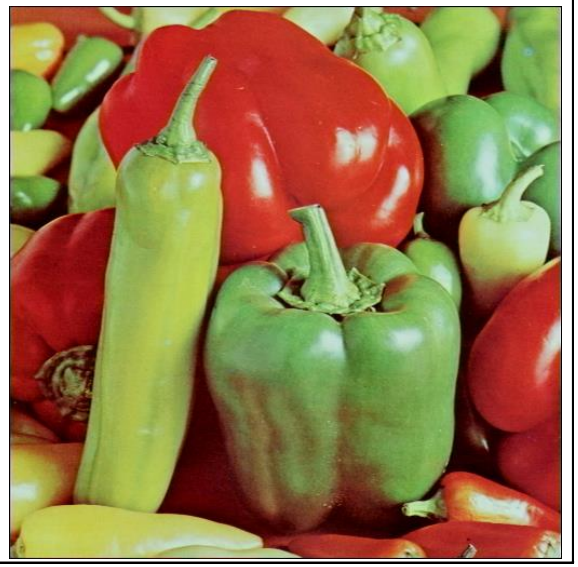
3. Gambar (*image*)

- bmp
- jpeg
- gif

4. Video

-Mpeg
- avi
- dll


myhiddenmessage.txt ...
File Edit Format Help
My hidden message.
Carrier File
Carrier File with
Hidden Message

Pada Hari Rabu tanggal 15 April 2015 dilangsungkan kuliah umum information security di K=Gedung Cyber Security, Kampus ITB Jatinangor. Pesertanya adalah aparat penegak hokum, yaitu Pak Polisi		

Embedded Message *Cover-image* *Stego-image*

Extraction

Cover image

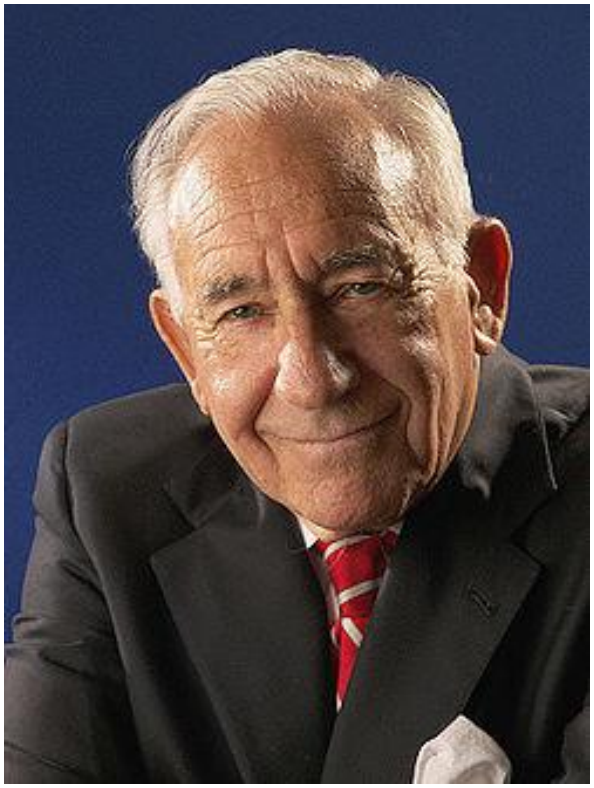
Embedded image

Stego-image

Extracted image

Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection).

(David Kahn, penulis buku *The Codebreakers - The Story of Secret Writing*)



Steganografi dan Terorisme

- Ilmu steganografi mendadak naik daun ketika pasca 11 September 2001 pihak FBI menuding *Al-Qaidah* menggunakan steganografi untuk menyisipkan pesan rahasia melalui video atau gambar yang mereka rilis secara teratur di Internet.