Bahan kuliah IF4020 Kriptografi

Steganografi
(Bagian 1)

Oleh: Dr. Rinaldi Munir

Prodi Informatika

Sekolah Teknik Elektro dan Informatika

Prolog

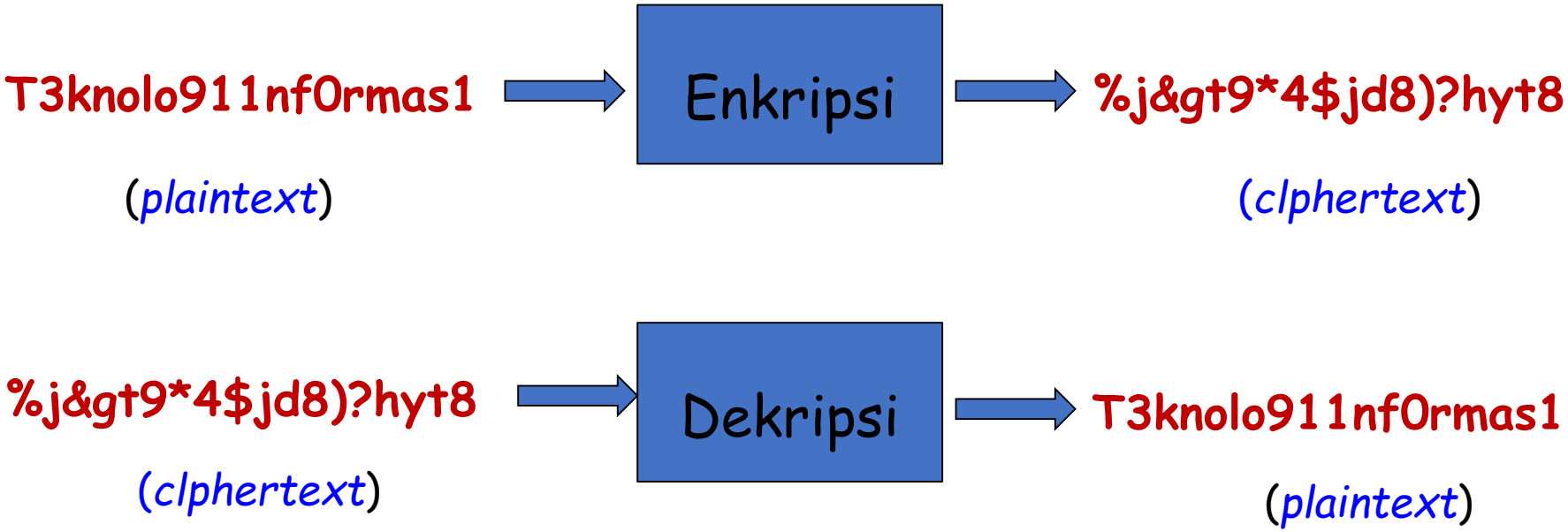
- Misalkan anda mempunyai data rahasia seperti *password*.

  Password: **T3knolo911nf0rmas1**

- Anda ingin menyimpan *password* tersebut dengan aman (tidak bisa diketahui orang lain).

- Bagaimana caranya agar *password* tersebut dapat disimpan dengan aman?

Cara I: Mengenkripsinya



→ **Bidang KRIPTOGRAFI (*cryptography*)**

Cara II: Menyembunyikannya

T3knolo911nf0rmas1

→ **Bidang STEGANOGRAFI (*steganography*)**

Apa Steganografi itu?

- Dari Bahasa Yunani: *steganos* + *graphien*

  "steganos" (*στεγανός*): tersembunyi

  "graphien" (*γραφία*) : tulisan

  steganografi: tulisan tersembunyi (*covered writing*)

- ***Steganography***: ilmu dan seni menyembunyikan pesan rahasia dengan suatu cara sedemikian sehingga tidak seorang pun yang mengetahui keberadaan pesan tersebut.

  Tujuan steganografi: pesan tidak terdeteksi keberadaannya

Perbedaan Kriptografi dan Steganografi

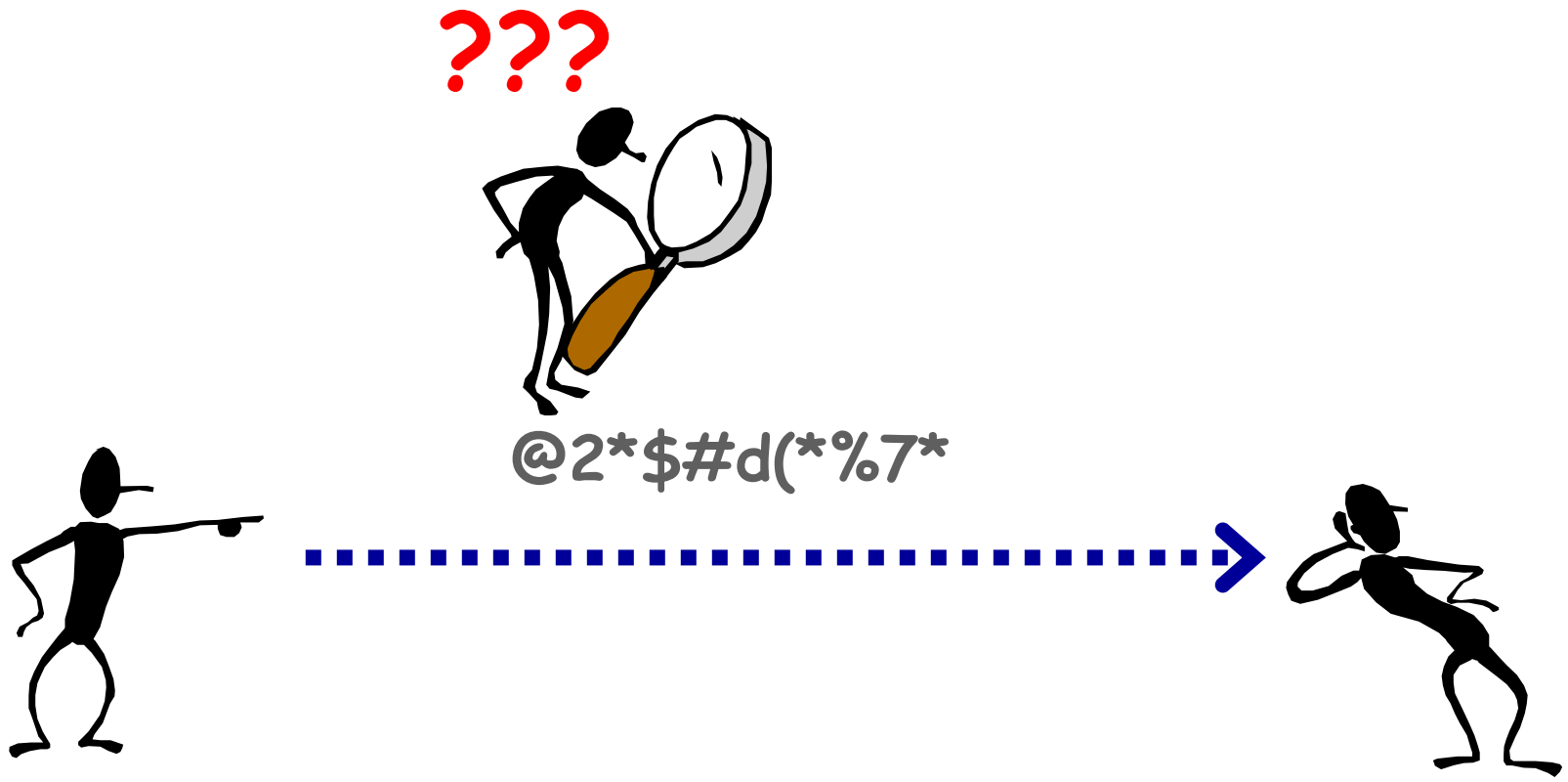
- Kriptografi: menyembunyikan ***isi*** (*content*) pesan

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

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

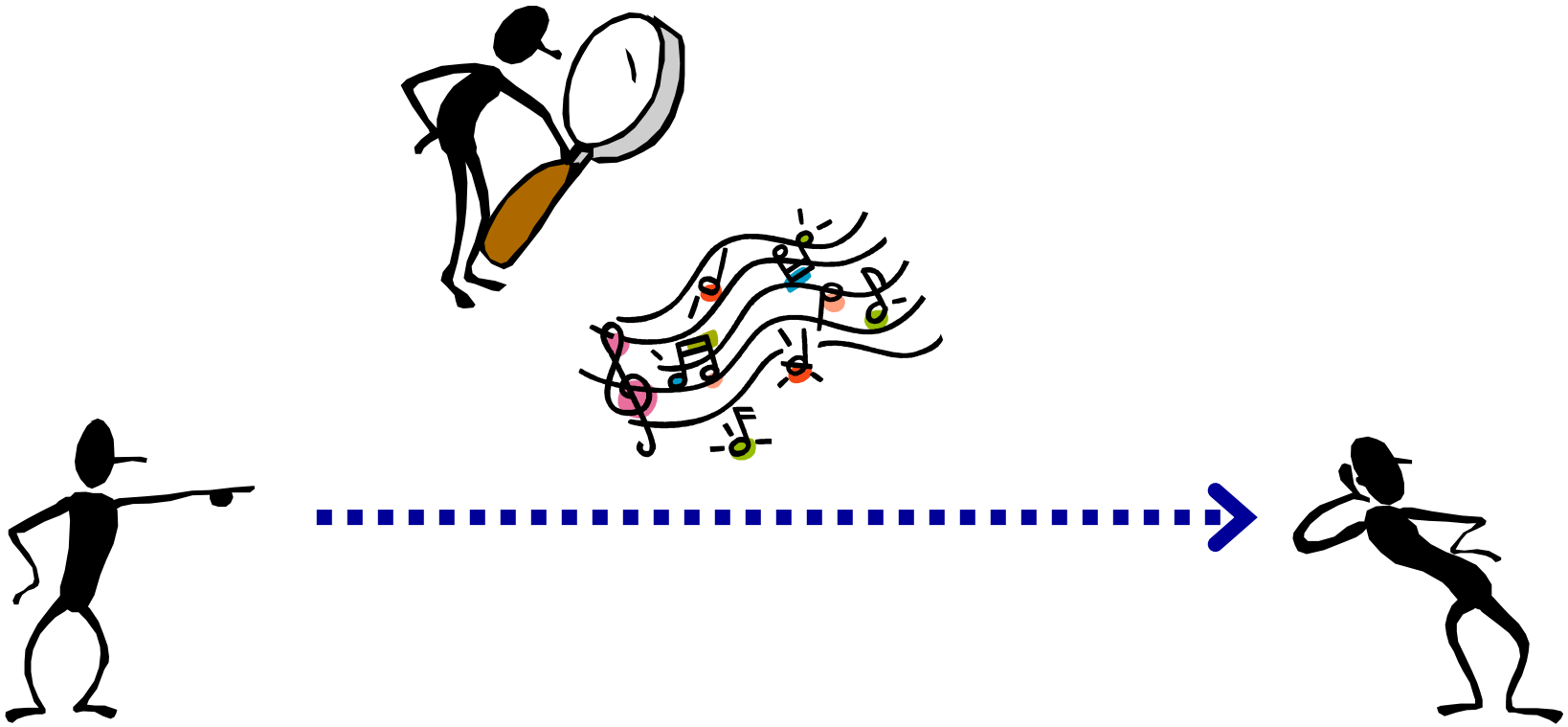
  → Tujuan: untuk menghindari kecurigaan (*conspicuous*) dari pihak ketiga (lawan)

Kriptografi



Pesan yang dienkripsi dengan kriptografi menimbulkan kecurigaan bagi pengamat.
Cipherteks dapat dideteksi keberadaannya.

Steganografi



Stego-data tidak menimbulkan kecurigaan bagi pengamat
Pesan yang tersembunyi di dalamnya tidak dapat dideteksi.

Information Hiding

- *Information hiding*: bidang ilmu yang mempelajari cara menyembunyikan pesan sehingga tidak dapat dipersepsi (baik secara visual maupun audial).

- Yang termasuk ke dalam *information hiding*:
  1. Kriptografi
  2. Steganografi

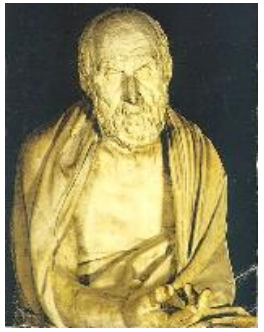
Sejarah Steganografi

- Usia steganografi setua usia kriptografi, dan sejarah keduanya berjalan bersamaan.

- Periode sejarah steganografi dapat dibagi menjadi:
  1. Steganografi kuno (*ancient steganography*)
  2. Steganografi zaman renaisans (*renaissance steganography*).
  3. Steganografi zaman perang dunia
  4. Steganografi modern

Ancient Steganography

Herodatus



- **Steganografi dengan media kepala budak.**

  Ditulis oleh Herodatus (485 – 525 BC), sejarawan Yunani pada tahun 440 BC di dalam buku: *Histories of Herodatus*). Kisah perang antara kerajaan Persia dan rakyat Yunani.

  Herodatus menceritakan cara **Histaiaeus** mengirim pesan kepada **Aristagoras of Miletus** untuk melawan Persia**.** Caranya**:** Dipilih beberapa budak. Kepala budak dibotaki, ditulisi pesan dengan cara tato, rambut budak dibiarkan tumbuh, budak dikirim. Di tempat penerima kepala budak digunduli agar pesan bisa dibaca.

- **Penggunaan *tablet wax***

  Orang-orang Yunani kuno menulis pesan rahasia di atas kayu yang kemudian ditutup dengan lilin (*wax*).

  Di dalam bukunya, Heradatus menceritakan Demaratus mengirim peringatan tentang serangan yang akan datang ke Yunani dengan menulis langsung pada tablet kayu yang kemudian dilapisi lilin dari lebah.

- **Penggunaan tinta tak-tampak (*invisible ink*)**

Pliny the Elder.
AD 23 - 79

Pliny the Elder menjelaskan penggunaan tinta dari getah tanaman *thithymallus*. Jika dituliskan pada kertas maka tulisan dengan tinta tersebut tidak kelihatan, tetapi bila kertas dipanaskan berubah menjadi gelap/coklat

- **Penggunaan kain sutra dan lilin**

- Orang Cina kuno menulis catatan pada potongan-potongan kecil sutra yang kemudian digumpalkan menjadi bola kecil dan dilapisi lilin.

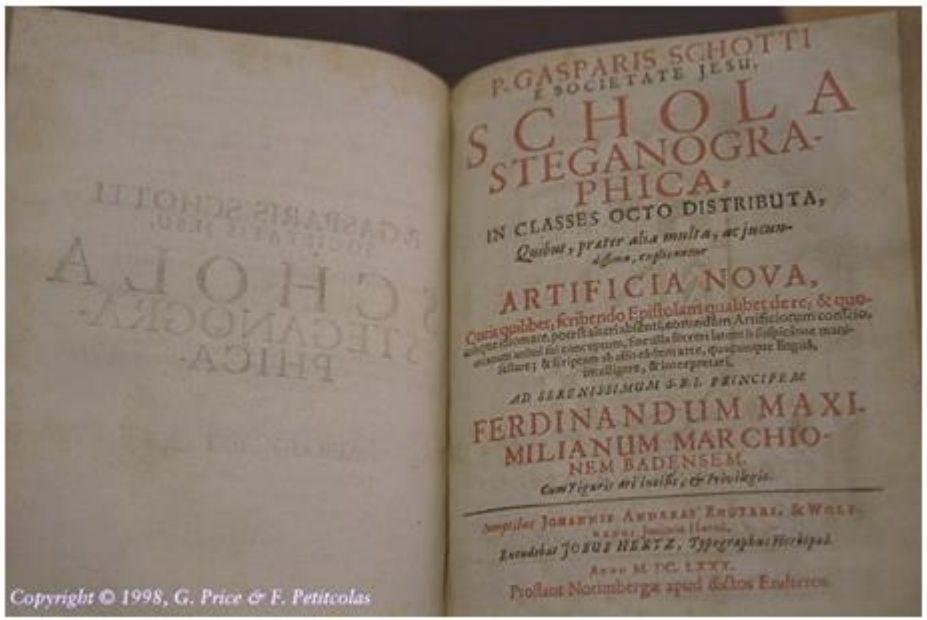
- Selanjutnya bola kecil tersebut ditelan oleh si pembawa pesan.

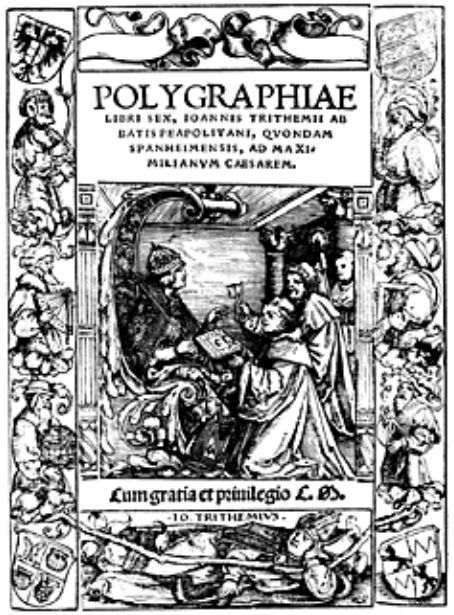
- Pesan dibaca setelah bola kecil dikeluarkan dari perut si pembawa pesan dengan cara BAB.

Renaissance Steganography

Johannes
Trithemius
(1404-1472)

Tahun 1499, Johannes Trithemius menulis buku **Steganographia**, yang menceritakan tentang metode steganografi berbasis karakter





Selanjutnya tahun 1518 dia menulis buku tentang steganografi dan kriptografi, berjudul **Polygraphiae**.

Giovanni Battista Porta
(1535-1615)

Giovanni Battista Porta menggambarkan cara menyembunyikan pesan di dalam telur rebus.

Caranya, pesan ditulis pada kulit telur yang dibuat dari tinta khusus yang dibuat dengan satu ons tawas dan setengah liter cuka.

Prinsipnya penyembunyiannya adalah tinta tersebut akan menembus kulit telur yang berpori, tanpa meninggalkan jejak yang terlihat.

Tulisan dari tinta akan membekas pada permukaan isi telur yang telah mengeras (karena sudah direbus sebelumnya). Pesan dibaca dengan membuang kulit telur

World War Steganography

- Penggunaan tinta tak-tampak (*invisible ink*) dalam spionase.
  - Pada Perang Dunia II, tinta tak-tampak digunakan untuk menulis pesan rahasia
  - Tinta terbuat dari campuran susu, sari buah, cuka, dan urine.
  - Cara membaca: Kertas dipanaskan sehingga tulisan dari tinta tak-tampak tersebut akan menghitam.

Seorang agen FBI sedang menggunakan sinar ultraviolet untuk membaca tulisan yang tersembunyi pada kertas yang dicurigai dari agen spionase.

- **Steganografi dalam Perang Dunia I: *Null Cipher***

  Pesan berikut dikirim oleh Kedubes Jerman pada PD I:

  Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

  Ambil huruf kedua setiap kata, diperoleh pesan berikut: *Pershing sails from NY June 1.*

Contoh *Null Cipher* lainnya:

Big rumble in New Guinea.
The war on celebrity acts should end soon.
Over four die ecstatic elephants replicated.

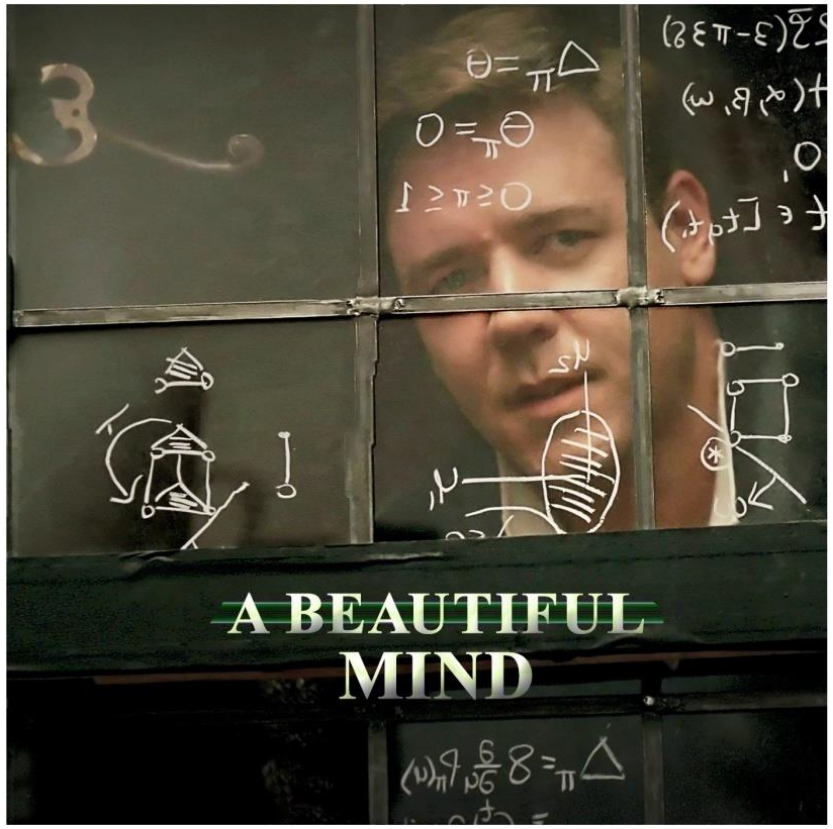
Bring two cases of deer.

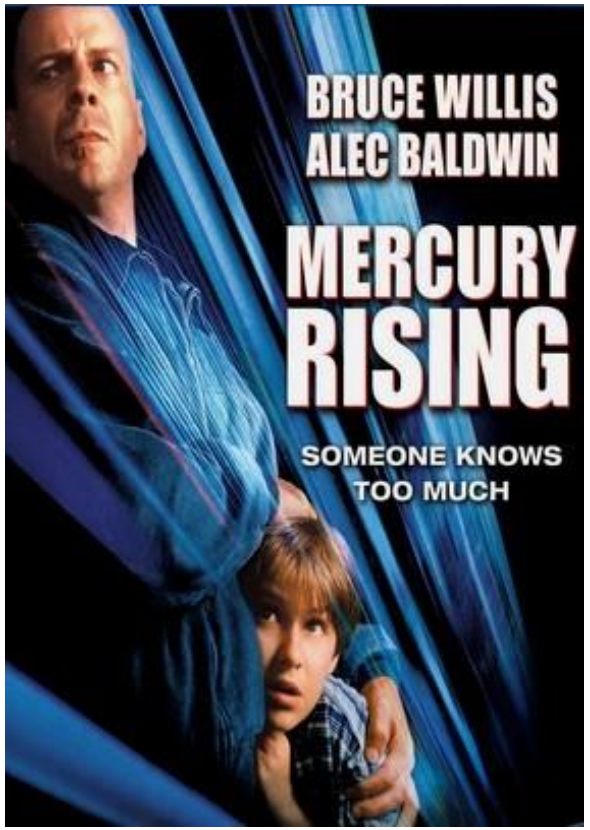
Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

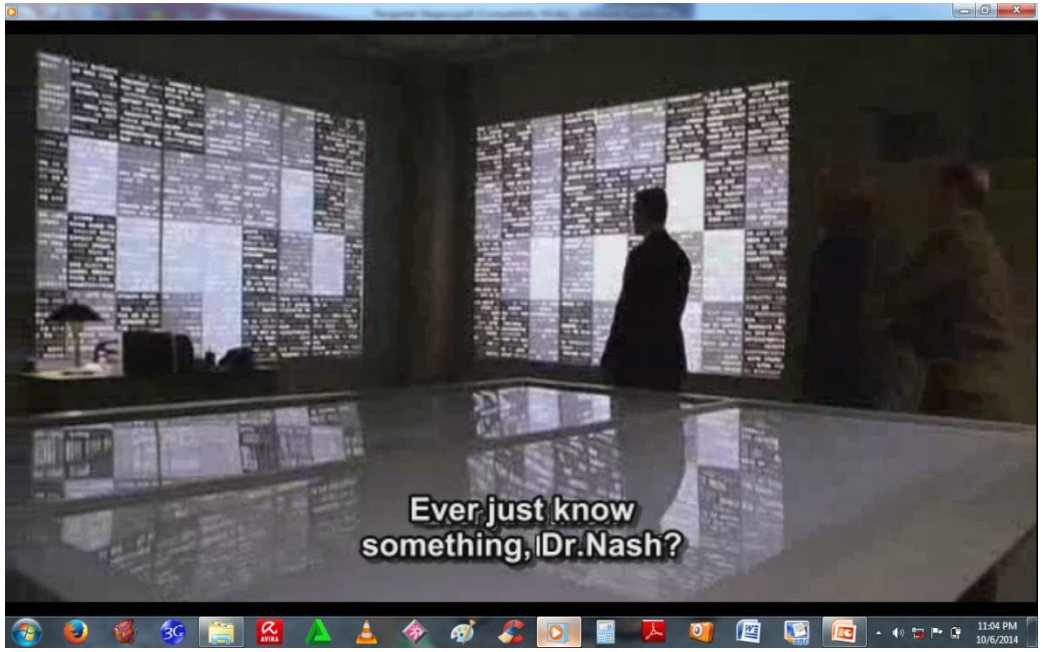
Dengan mengambil huruf ketiga pada setiap kata diperoleh pesan berikut:

Send Lawyers, Guns, and Money.

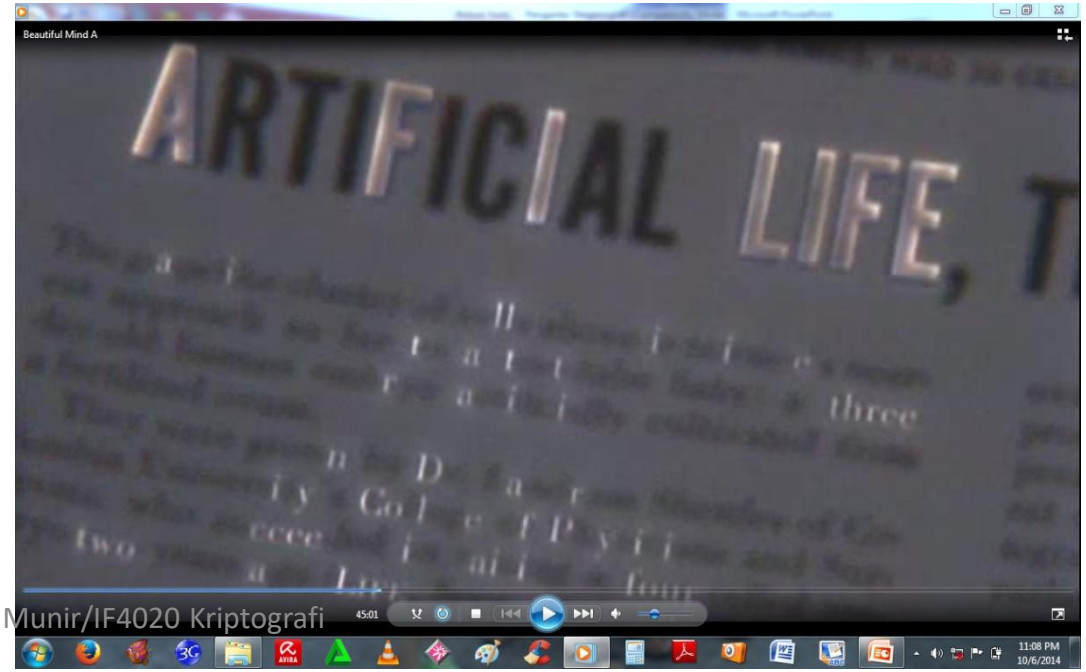
- Steganografi di dalam film *Mercury Rising* dan *Beautiful Mind*







Beberapa adegan film *Beautiful Mind* yang memperlihatkan steganografi

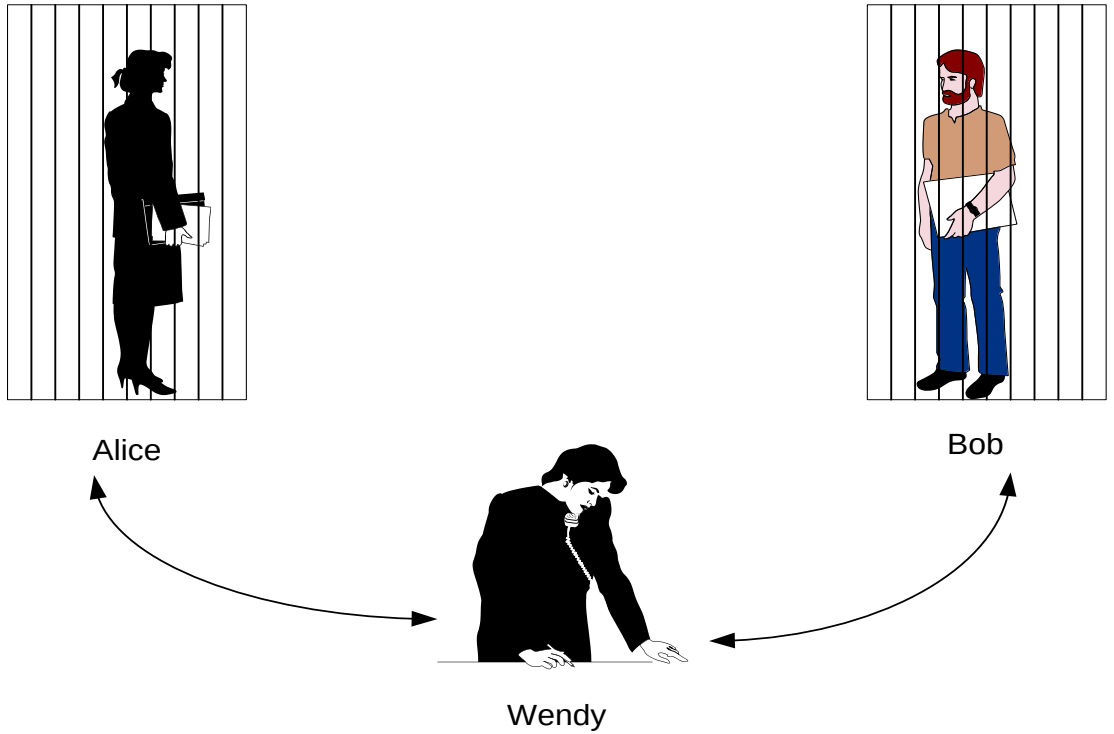


Steganografi dan Terorisme

- 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.

Steganografi Modern - *The Prisoner's Problem*

- Diperkenalkan oleh Simmons – 1983
- Dilakukan dalam konteks *USA – USSR nuclear non-proliferation treaty compliance checking*



Pesan rahasia: "malam ini kita kabur"

- Bagaimana cara Bob mengirim pesan rahasia kepada Alice tanpa diketahui oleh Wendy?

- Alternatif 1: mengenkripsinya

xjT#9uvmY!rc$7yt59hth@#

Wendy pasti curiga!

- Alternatif 2: menyembunyikannya di dalam tulisan lain

masihkah ada lara apabila memoriku ingat nestapa itu. kita ingin tetap abadikan kisah asmara. bersamamu usiaku renta.

Wendy tidak akan curiga!

Information hiding dengan steganografi!

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

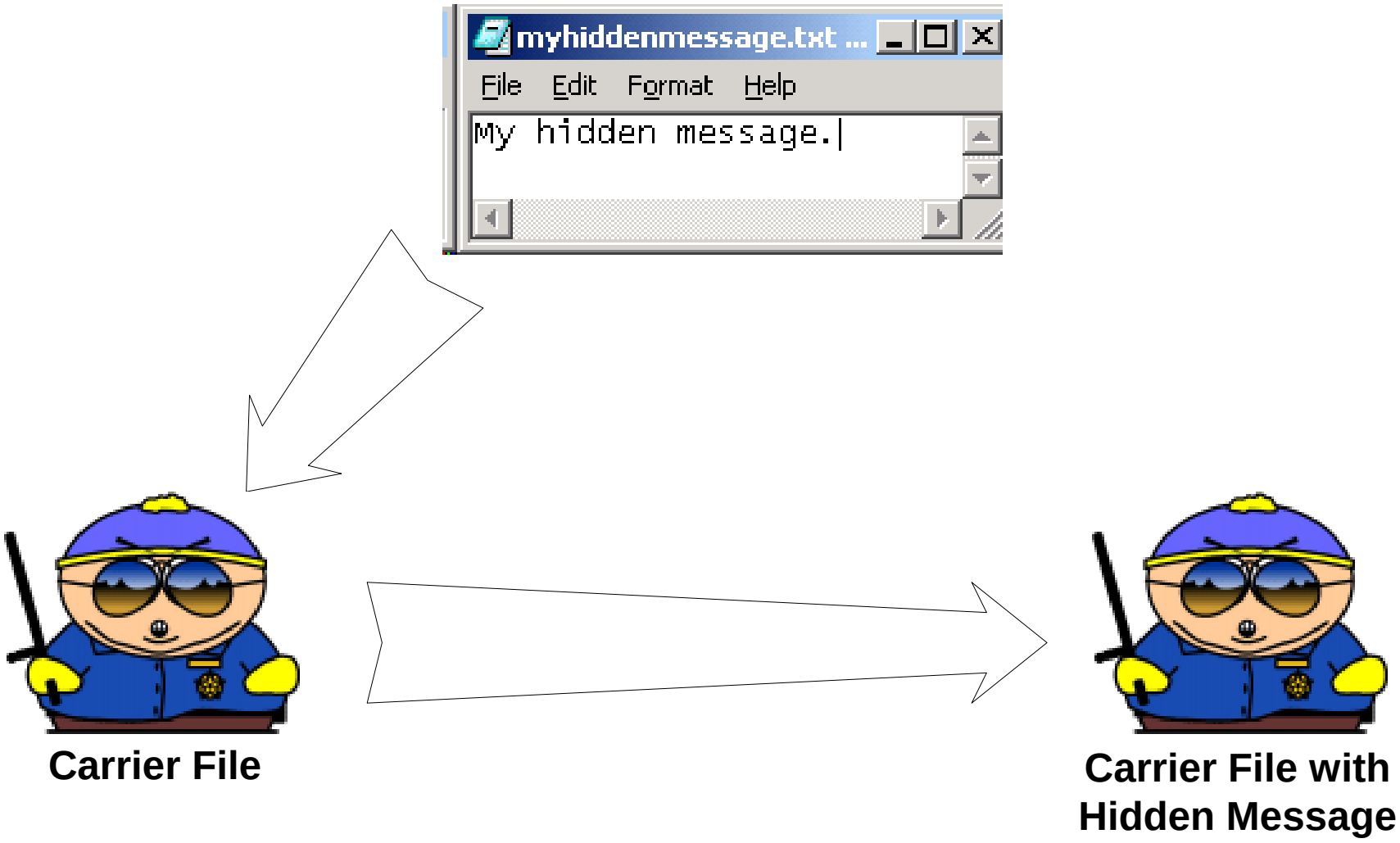
- wav
- mp3

3. Gambar (*image*)

- bmp
- jpeg
- gif
- png

4. Video

-mpeg
- avi
- mp4


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

Terminologi Steganografi Digital

1. *Embedded message* *atau* *secret message*: pesan yang disembunyikan .

   Bisa berupa teks, gambar, audio, video, dll

2. *Cover-object:* media digital yang digunakan untuk menyembunyikan *embedded message*.

   Bisa berupa teks, gambar, audio, video, dll

3. *Stego-object* (*stego-data):* media yang sudah berisi pesan *embedded message*.

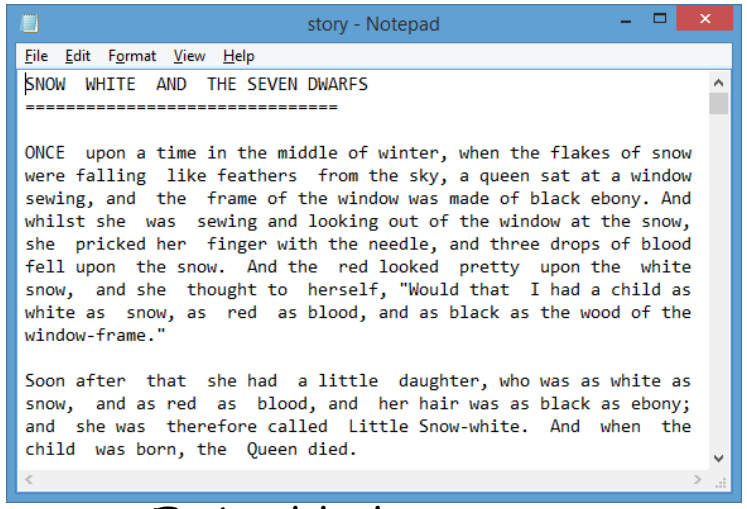
4. *Stego-key*: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stego-object.

Istilah keilmuan serumpun terasa memberikan distorsi persepsi pada maksud sebenarnya. Persepsi yang segera terbentuk dengan istilah tesrebut adalah pertumbuhan dari akar-akar ilmu membentuk suatu rumpun, yang berarti bahwa nuansa historis organisasi/kelompok/unit yang mewadahinya.		
Embedded message	*Cover-image*	*Stego-image*

GIF image

Cover image

Stego-image



Embedded message

Cover image

Stego-image

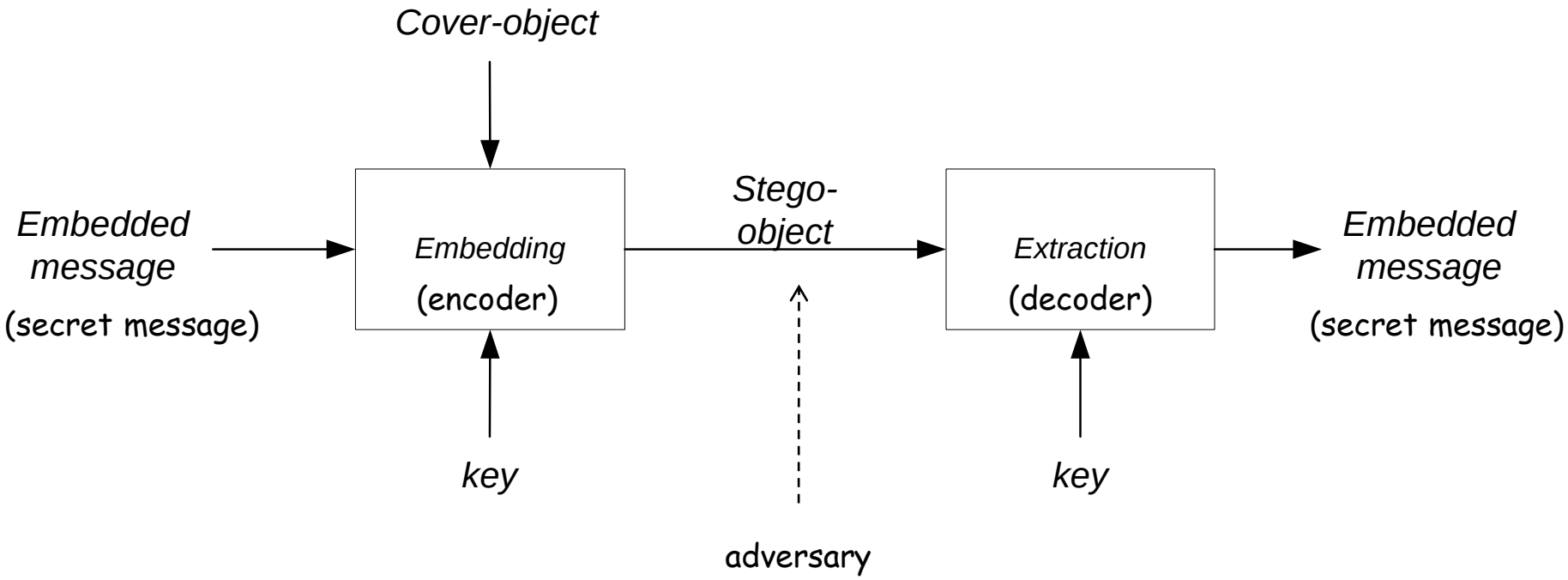
Cover image

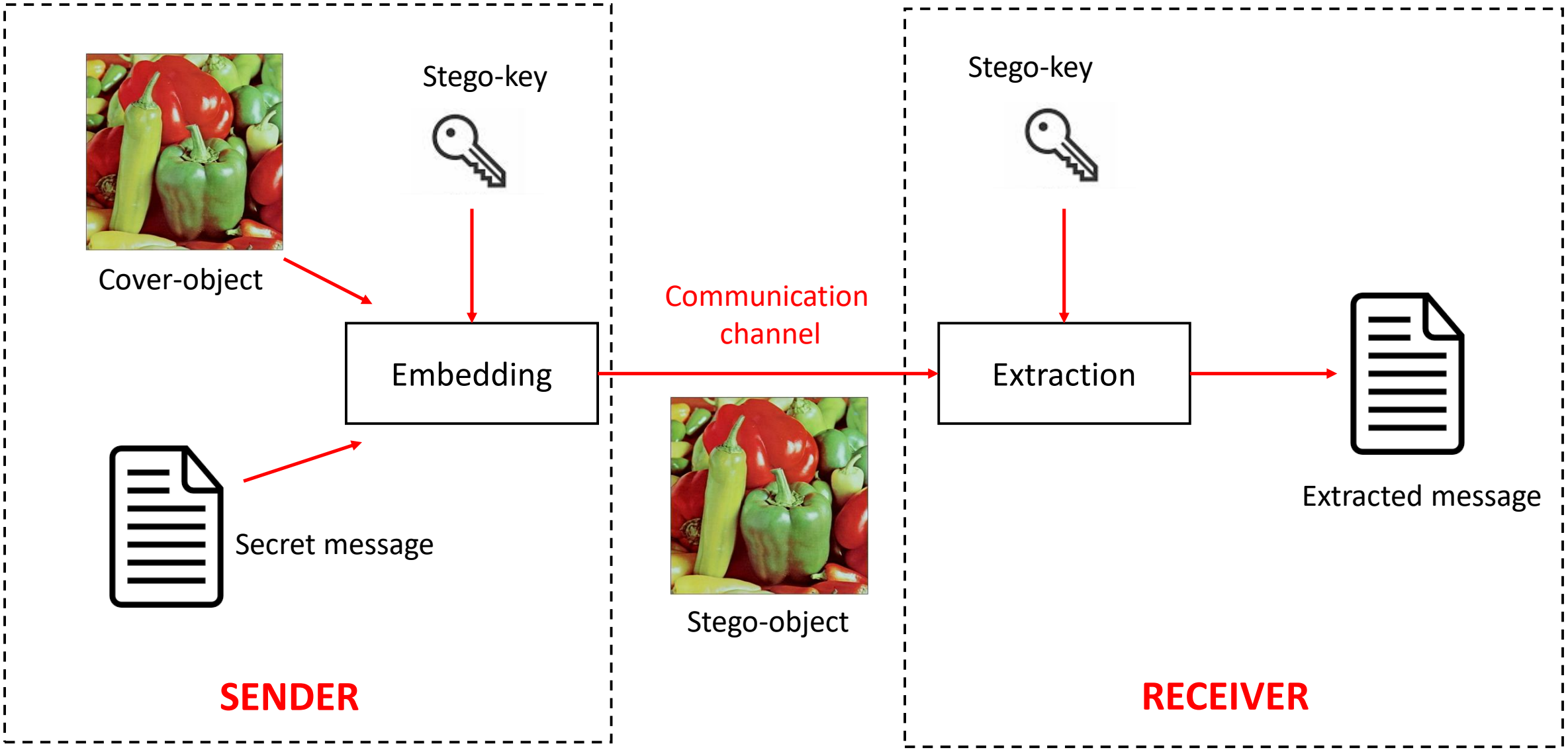
Embedded image

Stego-image

Extracted image

Diagram Proses Steganografi




Stego-key
Cover-object
Embedding
Secret message
SENDER
Communication channel
Stego-object
Stego-key
Extraction
Extracted message
RECEIVER

Kriteria Steganografi yang Bagus

1. *Imperceptible*

   Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audial

2. *Fidelity*.

   Kualitas *cover-object* tidak jauh berubah akibat penyisipan pesan rahasia.

3. *Recovery*.

   Pesan yang disembunyikan harus dapat diekstraksi kembali.

4. *Capacity*

   Ukuran pesan yang disembunyikan sedapat sebesar mungkin

Catatan: *Robustnes* bukan isu penting di dalam steganografi

Kombinasi Kriptografi dan Steganografi

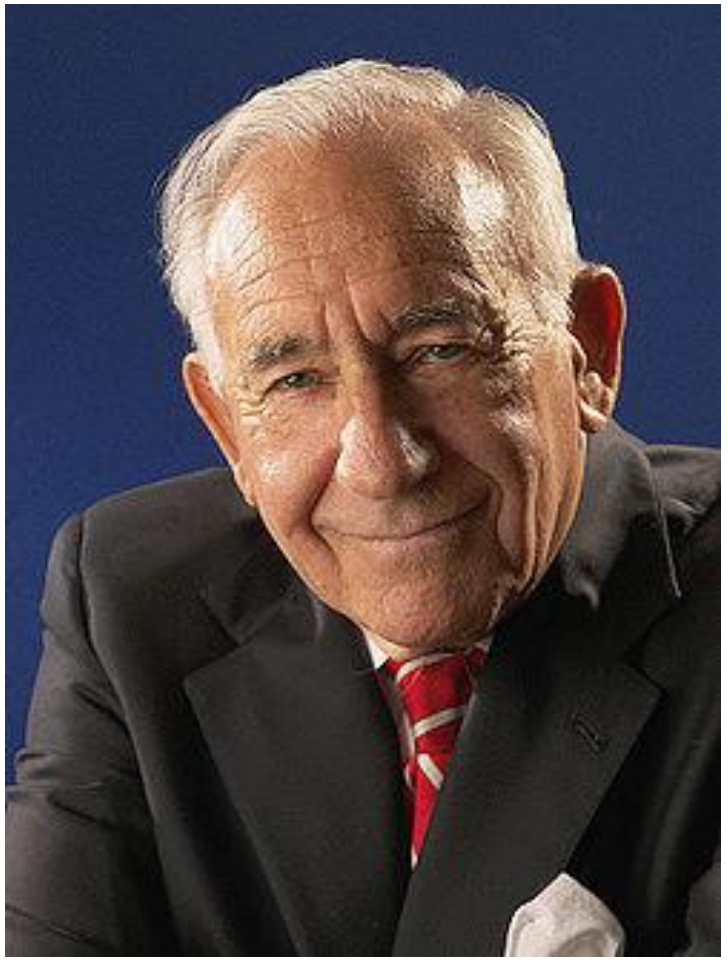
- Steganografi bukan pengganti kriptografi, tetapi keduanya saling melengkapi.

- Keamanan pesan rahasia dapat ditingkatkan dengan menggabungkan kriptografi dan steganografi.

- Mula-mula pesan dienkripsi dengan algoritma kriptografi, selanjutnya pesan terenkripsi disembunyikan di dalam media lain (citra, video, audio, dll) dengan algoritma steganografi.

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*)



Tiga Tipe Steganografi

1. ***Pure steganography***

   Tidak membutuhkan kunci sama sekali. Keamanan steganografi seluruhnya bergantung pada algoritmanya.

   Contoh: *Null Cipher*

   Prinsip Kerkhoff juga seharusnya pada steganografi, bahwa keamanan sistem seharusnya tidak didasarkan pada kerahasiaan algoritma embedding, tetapi pada kuncinya.

   Pure steganography →tidak disukai

2. ***Secret (or symmetric) key Steganography***

   Menggunakan kunci yang sama untuk *embedding* dan *extraction*.

   Contoh: - kunci untuk pembangkitan bilangan acak

   - kunci untuk mengenkripsi pesan dengan algoritma kriptografi simetri (DES, AES, dll)

3. ***Public-key Steganography***

   Menggunakan dua kunci: kunci publik untuk *embedding* dan kunci privat untuk *extraction.*

   Contoh: kunci publik RSA untuk mengenkripsi *embedded message*

   kunci privat RSA untuk mendekripsi *extracted message*

BERSAMBUNG
ke Bagian 2