

# PENGANTAR KRIPTOGRAFI

Introduction to Cryptography



www.indocisc.com



Pengamanan

## Security & Intelligence

- Signal Security
  - Steganography
  - Traffic security (call sign changes, dummy msg, radio silence)
  - Cryptography
- Electronic Security
  - Emission security (shifting radar freq.)
  - Counter - Countermeasures (looking through jammed radar)
- Signal Intelligence
  - Interception & Direction-Finding
  - Traffic Analysis
  - Cryptanalysis
- Electronic Intelligence
  - Electronic reconnaissance (eavesdropping on radar emission)
  - Countermeasures (jamming, false radar echose)

Source: David Kahn, *The Code Breakers*

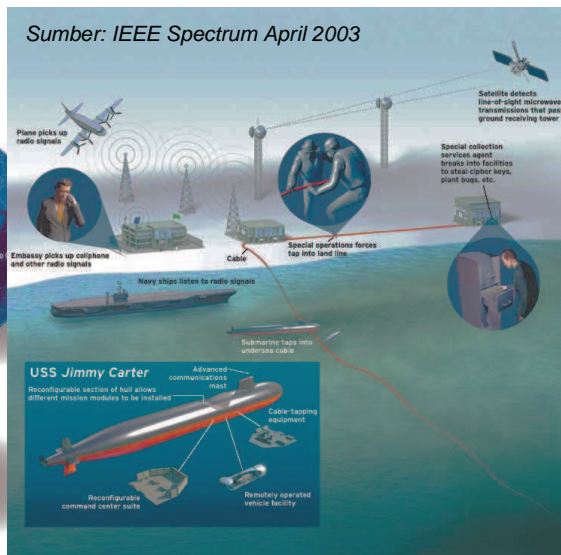
## Keamanan Negara

- Kemampuan mengamankan data dan menangkap data merupakan kepentingan negara
  - Privacy vs keamanan negara?
  - Spy vs spy?

## Penyadapan Internasional



Sumber: IEEE Spectrum April 2003



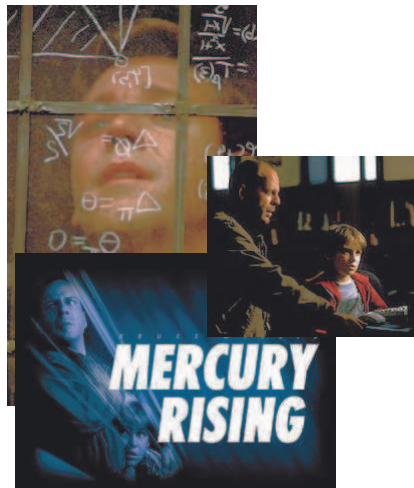
## Sadap, Filter, Simpan

Sumber: IEEE Spectrum April 2003



## Evolusi dari pengamanan data

- **Steganography**
  - Membuat seolah-olah pesan tidak ada
  - Film: "Mercury rising", "Beautiful mind"
- **Cryptography**
  - Transposition (letters arranged)
  - Substitution (letters substituted with other letters)



## Steganography

- Yunani (Greek) vs Persia
  - Pesan disembunyikan di meja yang dilapisi lilin
- Histalaeus
  - Pesan ditato di kepala budak yang telah digunduli
- Digital watermarking
  - Menandai kepemilikan gambar digital

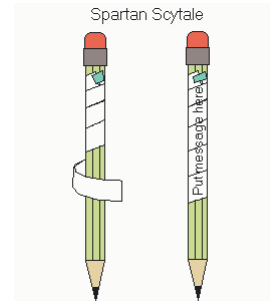
## Enkripsi penentu hidup mati

- Queen Mary dipancung
  - Menggunakan cipher messages untuk mengirimkan berita kepada kelompok anti Queen Elizabeth
  - Lawannya: Walsingham yang menggunakan Thomas Phelippes, seorang pakar pemecah kode

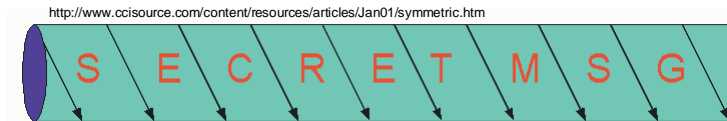


## Kriptografi: Transposition

- Contoh transposition
  - Rail fence
  - Spartan Scytale (5 BC)



<http://www.unmuseum.org/excoded.htm>



<http://www.ccisource.com/content/resources/articles/Jan01/symmetric.htm>

FEB 2004

PENGANTAR KRIPTOGRAFI - INDOCISC

9

## Kriptografi: Substitution

- Contoh substitution
    - Caesar cipher (geser 3 huruf)
- |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |
- Enigma (rotor)
    - Digunakan Jerman pada perang dunia ke 2

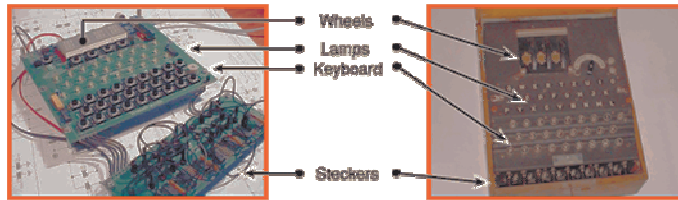


FEB 2004

PENGANTAR KRIPTOGRAFI - INDOCISC

10

## Enigma-E



<http://www.xat.nl/enigma-e/desc/index.htm>



## Komponen dari kriptografi

- Plain text
  - Sumber berita/pesan/teks asli
- Cipher text
  - Teks yang sudah diproses (diacak, digantikan)
- Algoritma & kunci
  - Misal: substitusi (algoritma) & number of shift (kunci)
  - Pemisahan alg & kunci ditemukan oleh Auguste Kerckhoffs von Niewenhof (1883)

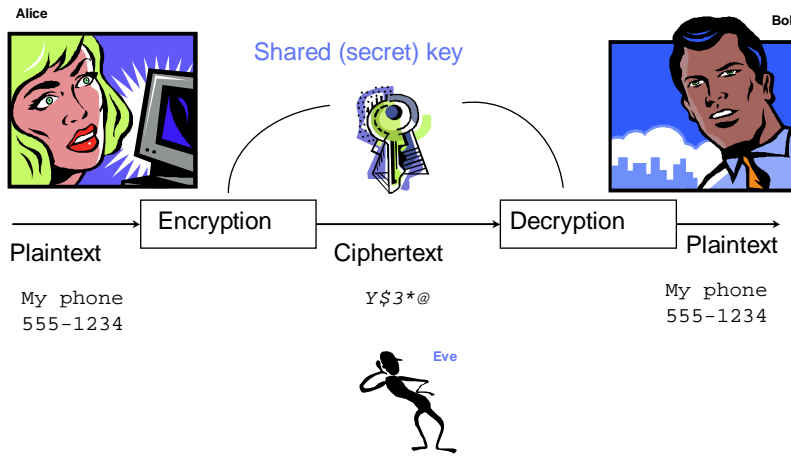
## CRYPTOGRAPHY

- *Private key cryptosystem*  
(Sistem kriptografi kunci privat)
  - Simetrik (kunci untuk mengunci dan membuka sama/satu)
- *Public key cryptosystem*  
(Sistem kriptografi kunci publik)
  - Asimetrik (kunci untuk mengunci dan membuka berbeda)

## PENGGUNAAN ENKRIPSI

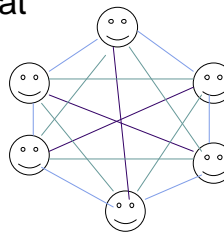
- Mengamankan data dengan mengacak data sehingga sulit untuk dibaca  
Confidentiality
- Meyakinkan tidak ada perubahan data  
Integrity
- Memastikan identitas seseorang dengan digital signature  
Authentication

# Kripto Kunci Privat

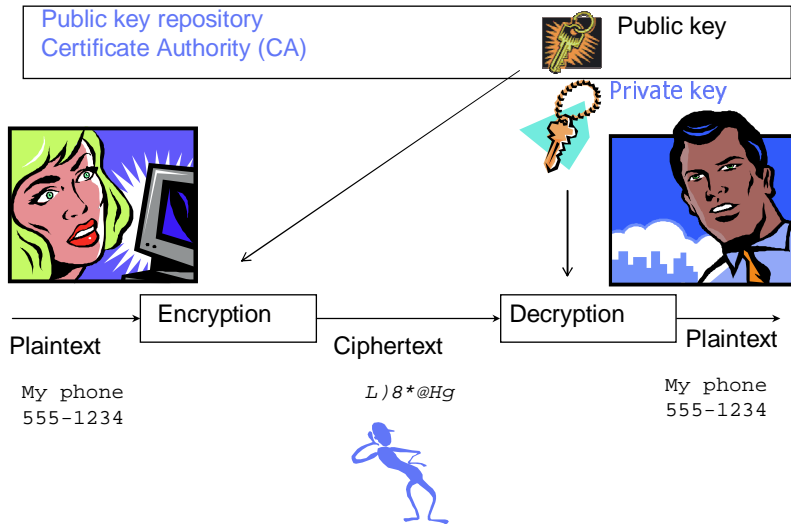


# Kripto Kunci Privat

- Menggunakan satu kunci
- Masalah dalam distribusi kunci
  - Pengiriman kunci membutuhkan saluran khusus
  - Jumlah kunci meledak secara eksponensial:  
 $n(n-1)/2$ : (lihat ilustrasi / gambar di bawah)
- Keuntungan: operasi yang cepat
- Contoh: DES, IDEA



# Kripto Kunci Publik



FEB 2004

PENGANTAR KRIPTOGRAFI - INDOCISC

17

# Kripto Kunci Publik



- Menggunakan kunci yang berbeda untuk enkripsi dan dekripsi
- Jumlah kunci yang lebih sedikit dibandingkan enkripsi dengan kunci privat
- Membutuhkan komputasi yang tinggi (membutuhkan waktu yang lebih lama)

FEB 2004

PENGANTAR KRIPTOGRAFI - INDOCISC

18

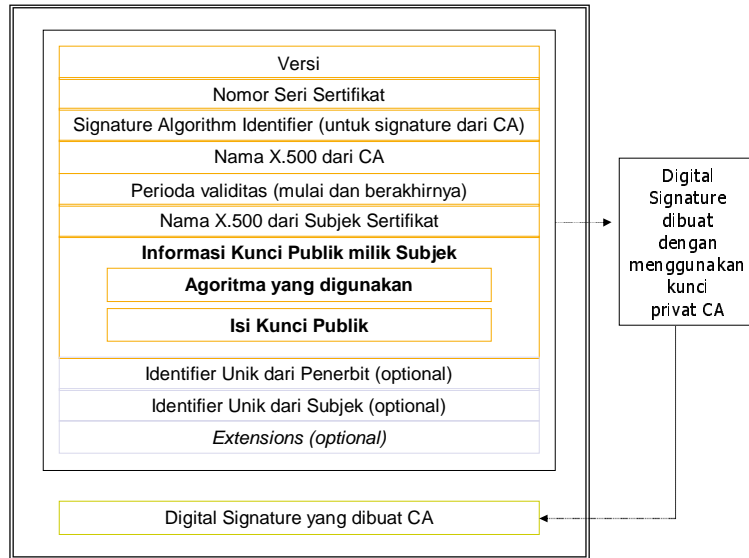
## Kripto Kunci Publik

- Membutuhkan penyimpanan kunci publik (Certificate Authority) yang terpercaya (trusted). Siapa? Verisign?
- Pengelolaan kunci bisa menjadi kompleks (revocation, pihak ketiga, dll.)
- Contoh: RSA, ECC

## Penggunaan Kripto Kunci Publik

- Secure Socket Layer (SSL)
  - HTTPS
  - SSH
  - STUNNEL
- Pretty Good Privacy (PGP) dan GNU Privacy Guard (GPG)

## Sertifikat Digital X.509 versi 3

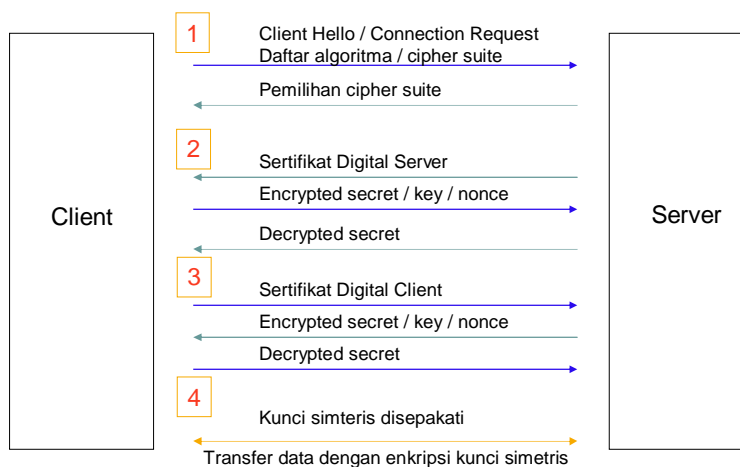


FEB 2004

PENGANTAR KRIPTOGRAFI - INDOCISC

21

## Protokol SSL



FEB 2004

PENGANTAR KRIPTOGRAFI - INDOCISC

22

## Message Digest

- Menghasilkan summary (digest) dari sebuah pesan (file, stream data)
- Menggunakan hash function untuk menghasilkan digest tersebut

## Fungsi Hash (Hash Function)

- Merupakan fungsi satu arah (one way function) yang dapat menghasilkan ciri (signature) dari data (berkas, stream)
- Perubahan satu bit saja akan mengubah keluaran hash secara drastis
- Digunakan untuk menjamin integritas dan digital signature

## Contoh Hash Function

- Contoh: MD5, SHA

```
unix$ md5sum /bin/login
af005c0810eeca2d50f2904d87d9ba1c /bin/login
```

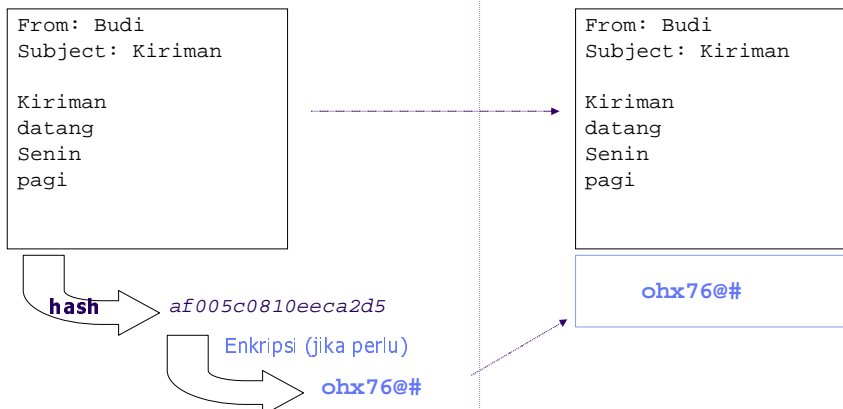
- Program md5sum untuk windows merupakan bagian dari *Cygwin distribution* yang dapat diperoleh dari

<http://sunsite.bilkent.edu.tr/pub/cygwin/cygwin-b20/full.exe>

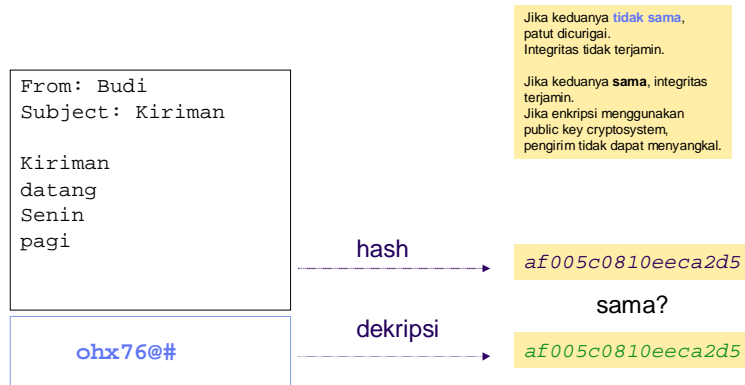
## Penggunaan Hash: Pengirim

Isi email tidak dirahasiakan.  
Diinginkan terjaganya integritas dan non-repudiation

Keduanya disatukan dan dikirimkan



## Pada Penerima



## Contoh Penggunaan Hash

- Hasil hash dienkripsi untuk menjamin keamanannya (integritas)
- Ukuran hasil hash yang lebih kecil dibandingkan ukuran pesan asalnya membutuhkan waktu enkripsi yang lebih singkat (dibandingkan jika mengenkripsi seluruh pesan)
- Digital Signature
- Pesan juga dapat dienkripsi jika diinginkan kerahasiaan

## Masalah Seputar Kripto

- Memastikan keamanan algoritma enkripsi
  - Algoritma harus dievaluasi oleh pakar
  - Algoritma yang tertutup (tidak dibuka kepada publik) dianggap tidak aman
  - Membuat algoritma yang aman tidak mudah
  - *Code maker vs code breakers* akan terus berlangsung

