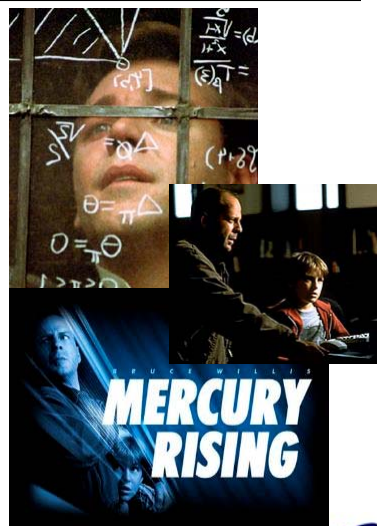


SELUK BELUK KRIPTOGRAFI

Budi Rahardjo

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

- Greek vs Persia
 - Message hidden in waxed table
- Histalaeus
 - Message in shaved head



2000-2002

Copyright, Budi Rahardjo



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



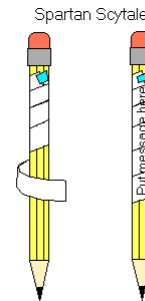
2000-2002

Copyright, Budi Rahardjo

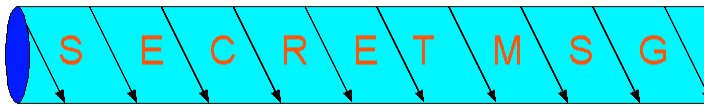


Transposition & Substitution

- Contoh transposition
 - Rail fence
 - Spartan Scytale (5 BC)
- Contoh substitution
 - Caesar cipher (geser 4 huruf)
 - Enigma



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



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



2000-2002

Copyright, Budi Rahardjo



Komponen dari kriptografi

- Plain text
 - Sumber berita/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)



2000-2002

Copyright, Budi Rahardjo





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)



2000-2002

Copyright, Budi Rahardjo



PENGUNAAN ENKRIPSI

- Mengamankan data dengan mengacak data sehingga sulit untuk dibaca
- Memastikan identitas seseorang dengan digital signature

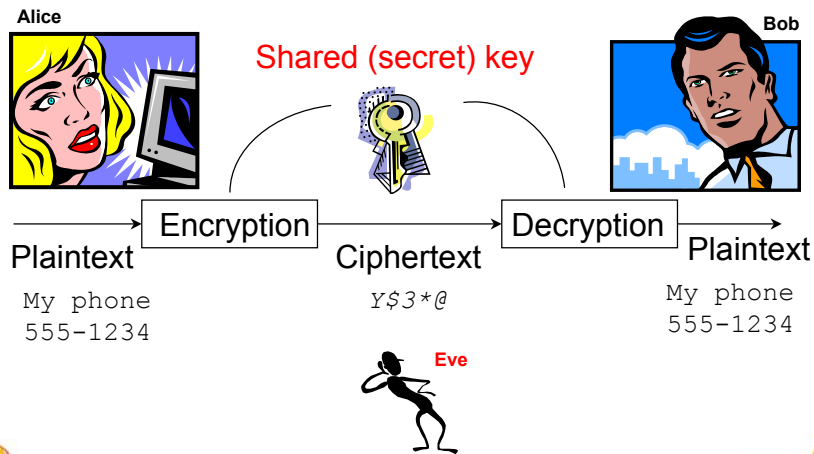


2000-2002

Copyright, Budi Rahardjo



Kripto Kunci Privat



2000-2002

Copyright, Budi Rahardjo



Kripto Kunci Privat

- Menggunakan satu kunci
- Masalah dalam distribusi kunci
 - Pengiriman kunci membutuhkan saluran khusus
 - Jumlah kunci meledak secara eksponensial
- Keuntungan: operasi yang cepat
- Contoh: DES, IDEA



2000-2002

Copyright, Budi Rahardjo



Kripto Kunci Publik

Public key repository
Certificate Authority (CA)



Public key

Private key



Plaintext → Encryption → Ciphertext → Decryption → Plaintext

My phone
555-1234

L) 8*@Hg

My phone
555-1234



2000-2002

Copyright, Budi Rahardjo



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)



2000-2002

Copyright, Budi Rahardjo





Kripto Kunci Publik

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



2000-2002

Copyright, Budi Rahardjo



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



2000-2002

Copyright, Budi Rahardjo



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
```



2000-2002

Copyright, Budi Rahardjo



Penggunaan Hash: Pengirim

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

Keduanya disatukan dan dikirimkan

From: Budi
Subject: Kiriman

Kiriman
datang
Senin
pagi

From: Budi
Subject: Kiriman

Kiriman
datang
Senin
pagi

hash

af005c0810eeca2d5

Enkripsi (jika perlu)

ohx76@#

ohx76@#



2000-2002

Copyright, Budi Rahardjo



Pada Penerima

From: Budi
Subject: Kiriman

Kiriman
datang
Senin
pagi

ohx76@#

hash

Jika keduanya **tidak sama**,
patut dicurigai.
Integritas tidak terjamin.

Jika keduanya **sama**, integritas
terjamin.
Jika enkripsi menggunakan
public key cryptosystem,
pengirim tidak dapat menyangkal.

af005c0810eeca2d5

sama?

dekripsi

af005c0810eeca2d5



2000-2002

Copyright, Budi Rahardjo



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



2000-2002

Copyright, Budi Rahardjo





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

