

---

## **ASPEK PENGAMANAN DALAM DUNIA E-COMMERCE**

Budi Rahardjo  
budi@cert.or.id

Dipresentasikan pada pertemuan “Pembentukan Tim Pengarah dan Tim Pelaksana Pengkajian Peningkatan Efisiensi Melalui Optimalisasi Pemanfaatan Asset BUMN Bidang Usaha Logistik”  
3 Agustus 2000, Hotel President, Jakarta

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



---

## **AGENDA**

- ◆ Statistik keamanan
- ◆ E-commerce membutuhkan pengamanan
- ◆ Aspek-aspek pengamanan
- ◆ Beberapa permasalahan
- ◆ Sumber informasi dan bahan bacaan

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## LATAR BELAKANG

- ◆ Ekonomi baru (new economy) didorong oleh teknologi
- ◆ Ekonomi baru belum dimengerti
  - Bubble economy
  - Kesempatan atau ancaman bagi Indonesia?
- ◆ Kepercayaan (trust) adalah fondasi bagi e-commerce
  - Apakah sudah pada level yang dapat diterima?
  - Bisnis tidak dapat menunggu sampai terjadi aman 100%

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## STATISTIK KEAMANAN

- ◆ Susah mencari angka yang pasti dikarenakan negative publicity
- ◆ 1996. FBI National Computer Crime Squad, detected computer crime 15%, only 10% of that number is reported.
- ◆ 1996. American Bar Association: survey of 1000 companies, 48% experienced computer fraud in the last 5 years.
- ◆ 1996. Di Inggris, NCC Information Security Breaches Survey: computer crime increased 200% from 1995 to 1996.
- ◆ 1997. FBI: computer crime case in court increased 950% from 1996 to 1997, convicted in court increased 88%.

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## MASIH TENTANG STATISTIK

### ◆ 1999 CSI/FBI Computer Crime and Security Survey

Disgruntled employees	86%
Independent hackers	74%
US Competitors	53%
Foreign corp.	30%
Foreign gov.	21%

<http://www.gosci.com>

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## STATISTIK INDONESIA

- ◆ Banyak web Indonesia yang sudah pernah “diobok-obok” oleh para vandal
- ◆ Cracker Indonesia tertangkap di Singapura
- ◆ Statistik dari SANS, Indonesia masuk dalam rangking (2%) yang mencoba melakukan attack terhadap web di Amerika Serikat

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## MASALAH UTAMA

- ◆ Awareness masalah keamanan masih rendah
  - Tidak ada budget
  - Implementasi yang tidak didesain untuk aman sehingga lebih mahal untuk memperbaiki

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## ASPEK SECURITY

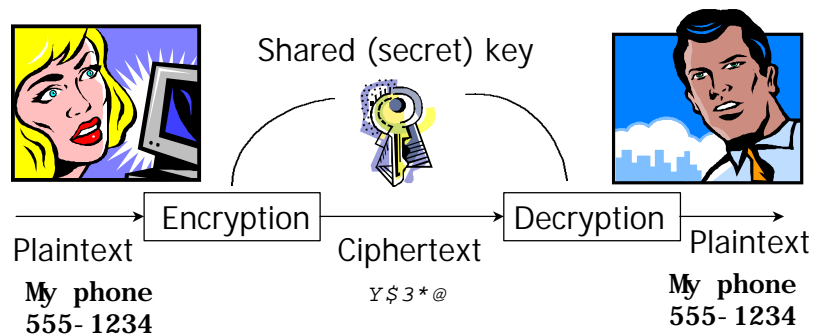
- ◆ Privacy / confidentiality
- ◆ Integrity
- ◆ Authentication
- ◆ Availability
- ◆ Non-repudiation
- ◆ Access control

Beberapa aspek ini dapat dijalankan dengan menggunakan kriptografi (enkripsi & dekripsi)

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## Private Key Cryptosystem



INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



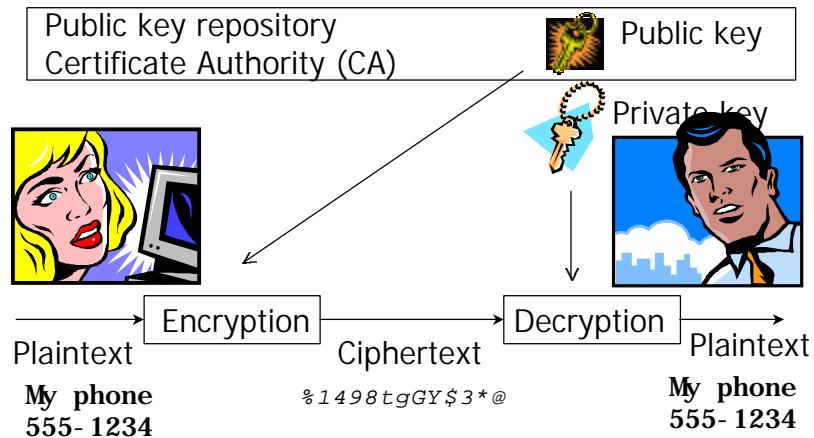
## Private Key Cryptosystem

- ◆ Menggunakan satu kunci rahasia untuk enkripsi dan dekripsi
- ◆ Ada masalah dalam management kunci
  - Distribusi kunci membutuhkan channel yang berbeda dan aman
  - Jumlah kunci meningkat secara eksponensial dengan bertambahnya jumlah pengguna
- ◆ Keuntungan: fast operation
- ◆ Contoh: DES, IDEA

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## Public Key Cryptosystem



INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## Public Key Cryptosystem

- ◆ Menggunakan kunci yang berbeda untuk enkripsi dan dekripsi
- ◆ Jumlah kunci menjadi lebih sedikit
- ◆ Kekurangan: membutuhkan komputasi yang lebih tinggi dan membutuhkan key repository
- ◆ Management kunci juga dapat menjadi kompleks
- ◆ Contoh: RSA, ECC

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## MASALAH LAIN

- ◆ Larangan ekspor dari Amerika untuk teknologi kriptografi yang memiliki level tinggi
- ◆ Ijin penggunaan teknologi kriptografi?
- ◆ Masalah privacy?
- ◆ Cyberlaw? Digital Signature Law/Act?
- ◆ National Critical Infrastructure Protection

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



## IDCERT

- ◆ Indonesia Computer Emergency Response Team
- ◆ Model: CERT, AUSCERT
- ◆ Membutuhkan dukungan
- ◆ <http://www.cert.or.id>
- ◆ Email: [budi@cert.or.id](mailto:budi@cert.or.id)

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

