

Keamanan Teknologi Informasi & Kriptografi

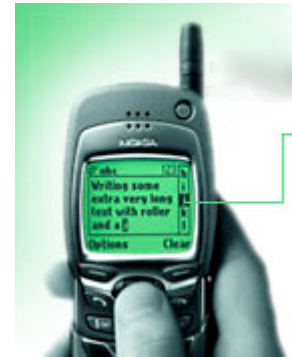
Budi Rahardjo

br@paume.itb.ac.id

Seminar STSN – Balai Sidang Universitas Indonesia
12 Juli 2008

Aplikasi Teknologi Informasi

- Aplikasi teknologi informasi sudah menjadi bagian dari kehidupan kita sehari-hari
 - Telekomunikasi (telepon, seluler, SMS, ...)
 - Internet (email, chat, web, blog, ...)
 - Televisi, radio, ...



Aplikasi Teknologi Informasi

- Perbankan (transfer uang, mesin ATM)
- Electronic money (APMK)
- ID tags



Keamanan Teknologi Informasi

- Keamanan dari data/informasi menjadi penting
 - Kerahasiaan transaksi elektronik
 - Kerahasiaan data pribadi
 - Terjaganya integritas dan akurasi data bank, data perkuliahan, ...

Aspek Keamanan TI

Utama

- Confidentiality
- Integrity
- Availability

Tambahan/Khusus

- Non-repudiation
- Authentication
- Access Control
- Accountability
- ...

Pengamanan TI

- Kecuali **availability**, pengamanan data / informasi dilakukan dengan menggunakan teknologi **kriptografi**

Masalah Kriptografi

- Salah penggunaan kriptografi berbahaya
 - *False sense of security*
- Perlu pemahaman tentang kriptografi
 - Perlu pemahaman ilmu kriptografi

Security / Cryptography Research

Snippet dari penelitian mahasiswa saya

- Theory
 - Digital Chaotic Cryptography [Budi Sulis]
 - (Secure) Implementation of ECC [Marisa W]
 - Strength of Crypto Algorithms
- Applications
 - Reasoning About Security in Mobile Money Protocol [Primus]
 - Distributing Security Tasks in Ad Hoc Network Environment [Samuel Betta]

Digital Chaotic Crypto

- Chaos
 - Perubahan kecil (di sisi input) menimbulkan perbedaan yang sangat besar (di sisi output)
 - Avalanche effects, randomness, pseudo random generator, random discriminator

Digital Chaotic Crypto [2]

- Masalah
 - Dasar sistem chaos adalah sistem yang kontinyu
 - Menjadi masalah jika dibawa ke dunia diskrit (digital)
 - Padahal implementasi sistem banyak di dunia digital
 - Perlu dikembangkan teori baru
 - Apa ukuran “tingkat keamanan”?

Secure ECC Implementation

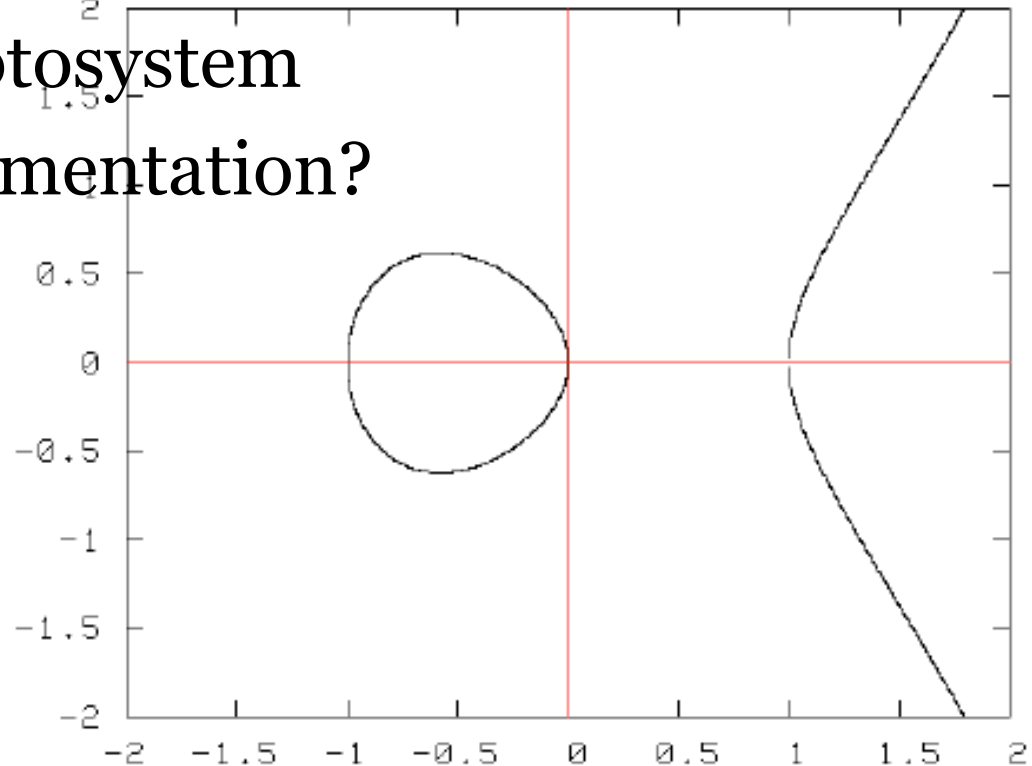
- Elliptic Curve Cryptosystem (ECC)
 - Salah satu algoritma public key cryptosystem
 - Efficient implementation?

ECC key pair generation

Let E be an elliptic curve defined over a finite field \mathbb{F} suppose that P has prime order n . Then the cyclic subgroup generated by P is

$$\langle P \rangle = \{\infty, P, 2P, 3P, \dots, (n-1)P\}$$

The prime p , the equation of the elliptic curve E , are the public domain parameters. A private key is an integer d chosen at random from the interval $[1, n-1]$, and the corresponding public key is the point $Q = dP$.



Secure ECC Implementation [2]

- Masalah
 - Pemilihan kurva ECC ternyata menentukan tingkat keamanan
 - Bagaimana menentukan kurva-kurva tersebut?
 - Apa ukuran “tingkat keamanan”?

Strength of Algorithms

- Apa ukuran “keamanan” sebuah algoritma?
- Apa saja yang menentukan keamanannya?
 - Randomness?
 - Avalance effect?
 - State space? Key space?
 - Computing power?
 - Cryptanalysis?
 - Pemanfaatan?

Mobile Money Protocol

- Melakukan modelling protokol yang digunakan untuk transaksi dengan APMK
- Melakukan verifikasi masalah keamanan protokol yang digunakan

Security of Ad Hoc Network

- Ad hoc network merupakan jaringan yang digunakan ketika terjadi bencana
- Bagaimana masalah keamanannya?
 - Otentikasi dari sumber pesan (instruksi)
 - Integritas pesan
 - Kerahasiaan pesan

Masalah

- Ilmu masih sulit dan kurang menarik
 - Terlalu banyak matematik yang *njlimet*

Cryptosystem

A cryptosystem is a five-tuple (Π, X, K, E, Δ) , where the following conditions are satisfied:

1. X is a finite set of possible ciphertext
2. Π is a finite set of possible plaintext
3. K , the keyspace, is a finite set of possible keys
4. For each $K \in K$, there is an encryption rule $e_K \in E$ and a corresponding decryption rule $d_K \in \Delta$. Each $e_K : \Pi \rightarrow X$ and $d_K : X \rightarrow \Pi$ are functions such that $d_K(e_K(x)) = x$ for every plaintext $x \in \Pi$.

Sumber gambar:

Marisa Widyastuti, "Cryptosystem & ECC", 3 Oktober 2007

Masalah

- Terbatasnya peneliti di bidang ini
- Membutuhkan komunitas untuk berdiskusi, berkolaborasi
 - Secara fisik
 - Secara virtual
 - Mari?

Penutup

- Meningkatnya ketergantungan kita kepada teknologi informasi
- Makin pentingnya pengamanan data / informasi dari aplikasi teknologi informasi
- Kriptografi dibutuhkan untuk pengamanan
- Dibutuhkan banyak orang yang memahami kriptografi. Mari berkolaborasi