

Zen of Crypto (and other issues)

Budi Rahardjo
budi@indocise.com
network & application security

**"Simplicity means
the achievement of
maximum effect
with minimum means."**

— Dr. Koichi Kawana

Semakin kompleks, semakin
banyak potensi kesalahan
(celah keamanan?)

“There are two ways of constructing a software design. One way is to make it so **simple** that there are **obviously no deficiencies**.

And the other way is to make it so **complicated** that there are **no obvious deficiencies**”

(C. A. R. Hoare)

Kompleksnya kriptografi menyebabkan salah penggunaan

Agustus 2007

BR - Zen of Crypto

5

Hash function?

Agustus 2007

BR - Zen of Crypto

6

Hash Function

- Sebuah fungsi satu arah
 - Maksudnya?
- Digunakan untuk menjamin integritas dari data
 - *Message Authentication Code* (MAC)
 - *Checksum*
 - Satu bit berubah maka *checksum* akan berubah

Agustus 2007

BR - Zen of Crypto

7

Contoh Checksum

- Parity bit
 - Jumlah bit “1” harus ganjil (atau genap)

Data (7 bit)	Parity
101 0101	1
101 0001	0

Agustus 2007

BR - Zen of Crypto

8

Hash Function

- Harus punya sifat-sifat khusus, diantaranya:
 - Avalanche effect: 1 bit berubah, checksum berubah secara drastis
 - Probabilitas dua pesan yang berbeda menghasilkan checksum yang sama sangat kecil
 - Contoh: MD5, SHA-1, dll.

Penggunaan Hash Yang Salah

Pesan 5 komputer



hash MD5

065aacf6b29aa3f102ffffd5cad5cd1e

Pesan yang dikirim:

Pesan 5 komputer

065aacf6b29aa3f102ffffd5cad5cd1e

MITM

- Pesan ditangkap, diubah ... termasuk mengubah MD5-nya

```
Pesan 5 komputer
065aacf6b29aa3f102ffffd5cad5cd1e
```



```
Pesan 9 komputer
a00f002c0b092d6d220c6769e4ff4dcf
```

Agustus 2007

BR - Zen of Crypto

11

Pengirim:

```
Pesan 5 komputer
065aacf6b29aa3f102ffffd5cad5cd1e
```



intercept

```
Pesan 5 komputer
065aacf6b29aa3f102ffffd5cad5cd1e
```



```
Pesan 9 komputer
a00f002c0b092d6d220c6769e4ff4dcf
```



Penerima:

```
Pesan 9 komputer
a00f002c0b092d6d220c6769e4ff4dcf
```

Agustus 2007

BR - Zen of Crypto

12

Contoh Lain

- Penggunaan *public key cryptography* yang sesungguhnya adalah *private key cryptography* karena kunci dibuat dan didistribusikan secara terentral oleh satu entitas. *False sense of security?*
- Hashed password disimpan di URL atau cookies sebagai bagian dari otentikasi dalam aplikasi berbasis web

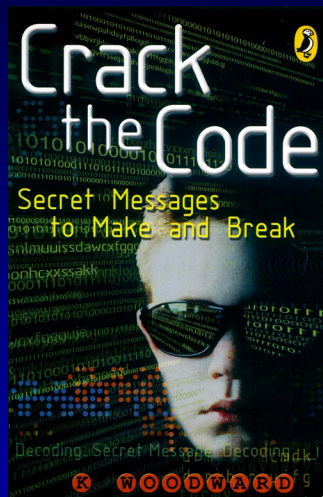
Penggunaan kriptografi
(yang salah)
tidak menjamin keamanan

Meminjam ide dari dunia lain

Agustus 2007

BR - Zen of Crypto

15

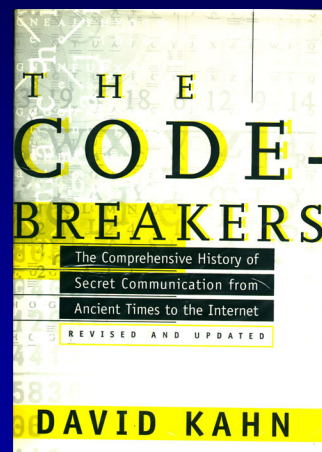


Agustus 2007

BR - Zen of Crypto

16

How to crack a code?



**Brute force:
try all possible combinations**

**Takes a lot of time!
(and resources)**

Analogy (pinjam ide?): Testing Digital Circuits

Agustus 2007

BR - Zen of Crypto

19

AND gate

A	B	out
0	0	0
0	1	0
1	0	0
1	1	1



- AND gate dengan 2 input:

$2^2 = 4$ kombinasi

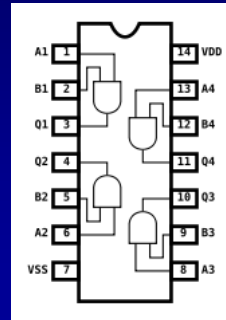
Agustus 2007

BR - Zen of Crypto

20

Kompleksitas Meningkat

- Rangkaian dengan 8 input
 - $2^8 = 256$ kombinasi
- Bagaimana dengan prosesor 64 bit?
 - $2^{64} = \dots$ kombinasi
 - Dibutuhkan waktu yang sangat lama untuk menguji semua kombinasi
- 128 bit? 256 bit?
- Sequential circuits?



Agustus 2007

BR - Zen of Crypto

21

Angka dan Kompleksitas

Besaran Fisik	Besaran Angka
Probabilitas terbunuh karena sambaran petir (setiap harinya)	1 dari 9 milyar (2^{33})
Probabilitas memenangkan hadiah pertama lotre di Amerika	2^{28}
Probabilitas memenangkan hadiah pertama lotre dan terbunuh kena sambaran petir	2^{61}
Umur sebuah planet	2^{30}
Jumlah atom di planet	2^{170}

Agustus 2007

BR - Zen of Crypto

22

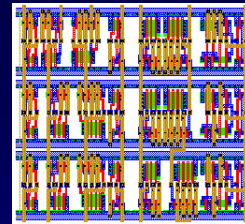
Quantum Computing?

Agustus 2007

BR - Zen of Crypto

23

VLSI Testing



- Pengujian rangkaian dengan kompleksitas yang tinggi
- Tersedia teori & tools untuk melakukan pengujian secara semi otomatis
 - *Brute force vs. guided*
 - (hmmm... seperti *cracking code*?)
 - *Binary Decision Diagram (BDD)*

Agustus 2007

BR - Zen of Crypto

24

Kompleks ke Sederhana?

$$F = abcd + \overline{a}bcd + a\overline{b}cd + abc\overline{d}$$

disederhanakan (melalui matematik
atau K-map) menjadi

$$F = ac$$

Formal Verification

- Pembuktian rangkaian secara matematis
 - Formal logic
 - Formal verification
 - Theorem prover

Terkait?

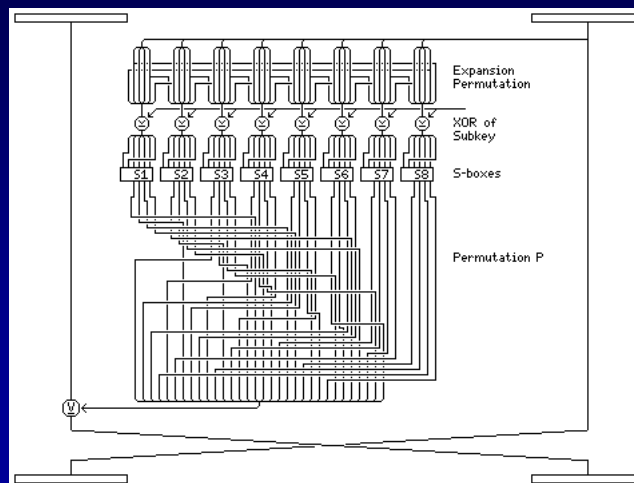
- Rangkaian digital =>
persamaan matematik
- Enkripsi =>
persamaan matematik
- Dapatkah pendekatan di dunia digital circuits digunakan untuk dunia krypto?

Agustus 2007

BR - Zen of Crypto

27

Bagian dari DES



Agustus 2007

BR - Zen of Crypto

28

Algoritma RSA

- Kunci Publik:
 - $n = p \cdot q$, p & q bil. Prima besar dan dirahasiakan
 - e relatif prima terhadap $\Phi(n) = (p-1) \cdot (q-1)$
- Kunci Rahasia:
 - $d = e^{-1} \bmod \Phi(n)$
- Enkripsi:
 - $c = m^e \bmod n$
- Dekripsi:
 - $m = c^d \bmod n$

Sumber: Sarwono Sutikno

Agustus 2007

BR - Zen of Crypto

29

- Bob Colwell “*Engineering, Science, and Quantum Mechanics*,” IEEE Computer, March 2002:

“Generally speaking, most engineers are comfortable with using theories and ideas that neither they nor anyone else completely understand”

Agustus 2007

BR - Zen of Crypto

30

Penutup

- Kriptografi bukanlah jaminan keamanan
- Kompleksitas dari kriptografi dapat membuat salah penggunaannya. Dapatkah kita sederhanakan?
Zen of crypto
- Banyak ide yang bisa dipinjam dari bidang lain