



Block Chiper - Lanjutan

IDEA, Blowfish , RC5 dan CAST 128

Muhammad Adri, S.Pd, MT

AMIK – STMIK Jayanusa Padang
2008

Algoritma TDEA

- Triple DEA (TDEA) diperkenalkan oleh Tuchman pada tahun 1979.
- Standar pertama yang digunakan untuk aplikasi finansial pada tahun 1985
- Tahun 1999, TDEA menjadi salah satu bagian standar enkripsi data.

Algoritma TDEA ...

- Menggunakan 3 key dan 3 eksekusi algoritma DES (Enkripsi - Dekripsi - Enkripsi)

$$C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$$

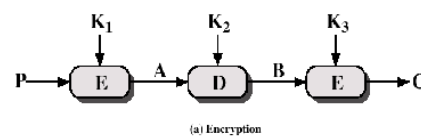
- C = ciphertext
- P = Plaintext
- EK[X] = encryption of X using key K
- DK[Y] = decryption of Y using key K

- Panjang kunci efektif 168 bit
- Untuk dekripsi berlaku persamaan :

$$P = D_{K_1}[E_{K_2}[D_{K_3}[C]]]$$

TDEA Process

- A. Proses enkripsi



- B. Proses dekripsi

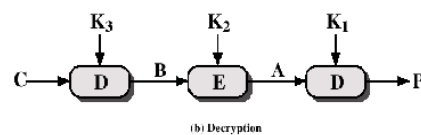


Figure 2.6 Triple DEA

Algoritma AES

- AES (advanced encryption standard), merupakan pengganti TDEA, yang dikemukakan oleh NIST (National Institute of Standard and Technologies) pada tahun 1997.
- AES mempunyai sekuritas yang sama atau lebih baik dari TDEA, tetapi dengan peningkatan efisiensi yang signifikan.
- AES merupakan Block Cipher simetris, dengan panjang blok 128 bit dan panjang kunci 128, 192 dan 256 bit

Algoritma EAS..

- Kriteria penilaian terhadap algoritma EAS :
 - 1. Sekuritas/ keamanan
 - 2. efisiensi komputasi
 - 3. kebutuhan memori
 - 4. kecocokan hardware dan software
 - 5. fleksibilitasnya.

Algoritma IDEA

- IDEA (The International Data Encryption Algorithm) merupakan sebuah Block Cipher Simetrik yang dikembangkan oleh Xuejia Lai dan James Massey dari SFIT (*Swiss Federal Institute of Technology*) pada tahun 1991.
- IDEA menggunakan sebuah key 128 bit
- IDEA mempunyai perbedaan dengan DES dalam dua hal, yaitu fungsi *Round* dan fungsi *Sub Key Generation*

Perbedaan IDEA dan DES

- Fungsi Round
 - DES menggunakan model permutasi (S-Boxes), persilangan antara setengah bagian kanan dengan setengah bagian kiri pada setiap round, sedangkan IDEA menggunakan tiga operasi matematika yaitu : XOR, penjumlahan binary integer 16 bit dan perkalian binary integer 16 bit.
 - Digunakannya tiga kombinasi operasi matematika pada IDEA untuk memperoleh transformasi kompleks, sehingga sulit untuk dianalisa dan di cryptanalisis.

Perbedaan IDEA dan DES...

- fungsi *Sub Key Generation*
 - Pada DES, untuk subkey-nya dihasilkan melalui suatu pergeseran putar (*circular shift*), sedangkan IDEA menghasilkan subkey dengan metoda yang kompleks untuk menghasilkan sebanyak 6 key untuk setiap 8 putaran IDEA

Algoritma Blowfish

- Blowfish, dikembangkan pertama kali pada tahun 1993 oleh Bruce Schneier, seorang konsultan independen dan seorang Cryptographer.
- Blowfish dengan cepat berkembang dan menjadi algoritma alternatif yang paling populer pengganti DES
- Blowfish dirancang untuk mudah diimplementasikan dan kecepatan eksekusi yang tinggi.

Blowfish - Pengantar

- Dengan algoritma yang *compact*, mampu berjalan pada memori 5 Kb.
- Panjang kunci yang digunakan pada Blowfish dapat bervariasi hingga mencapai 448 bit.
- Dalam prakteknya, panjang kunci yang umum digunakan 128 bit.
- Blowfish menggunakan 16 Round.

Blowfish – Fungsi Algoritma

- Blowfish menggunakan model DES dengan S-Boxes dan fungsi XOR, namun juga menggunakan penjumlahan Binary.
- S-Boxes yang digunakan pada Blowfish tidak sama dengan DES, Blowfish menggunakan S-Boxes dinamis yang dihasilkan sebagai fungsi dari Key.
- Dalam Blowfish, subkey dan S-Boxes dihasilkan oleh aplikasi perulangan dari algoritma Blowfish terhadap Key.
- Dengan total 521 eksekusi dari Algoritma enkripsi Blowfish yang dibutuhkan untuk menghasilkan Sub key dan S-boxes.

Blowfish - Kelemahan

- Blowfish tidak sesuai untuk aplikasi-aplikasi yang secret-key nya sering berubah.

Algoritma RC5

- RC5 dikembangkan pada tahun 1994 oleh Ron Rivest, salah seorang penemu algoritma kunci public RSA.
- RC5 didefinisikan di dalam RFC2040, dengan karakteristik sebagai berikut :
 - Sesuai untuk berbagai jenis hardware dan software ; RC5 hanya menggunakan operasi komputasi primitive yang umumnya ditemukan pada mikroprosesor
 - Cepat ; RC5 menggunakan algoritma yang simple dan berorientasi word. Operasi dasar bekerja pada word penuh dalam satu waktu operasi

Algoritma RC5...

- Karakteristik RC5 – Lanjutan :
 - Dapat beradaptasi dengan prosesor dengan panjang word yang berbeda.
 - Jumlah Round yang bervariasi ; tergantung pada kebutuhan terhadap kecepatan dan sekuritasnya
 - Panjang Key yang bervariasi ; tergantung pada kebutuhan terhadap kecepatan dan sekuritasnya
 - Simple ; RC5 mempunyai struktur yang mudah diimplementasikan .
 - Kebutuhan memory yang rendah ; RC5 cocok diimplementasikan pada smartcard atau perangkat lain yang berjalan dengan memori terbatas

Algoritma RC5...

- Karakteristik RC5 – lanjutan
 - Keamanan tinggi ; RC5 mampu menyediakan keamanan yang tinggi, tergantung pada parameter yang akan digunakan
 - Rotasi Data-dependent ; rotasi dan pergeseran yang dilakukan oleh RC5 tergantung pada data.

Algoritma CAST-128

- CAST adalah suatu prosedur perancangan untuk algoritma enkripsi simetris.
- Dikembangkan pada tahun 1997 oleh Carlisle Adams dan Stafford Tavares dari Entrust Technologies
- Salah satu algoritma spesifik yang dikembangkan dalam CAST adalah CAST -128, yang didefinisikan dalam RFC 2144.
- Dibuat dengan panjang kunci mulai dari 40 bit sampai 128 bit dengan kenaikan 8 bit (40, 48, 56,.....,128).

Algoritma CAST-128...

- CAST menggunakan S-Boxes tetap, tetapi lebih besar dibandingkan dengan DES.
- S-Boxesnya dirancang sangat linier dan tahan terhadap cryptanalysis.

Perbandingan antar Algoritma

Algoritma	Key Size	Round	Operasi Matematika	Aplikasi
DES	56 bit	16	XOR, S-Boxes tetap	SET, Kerberos
TDEA	112 atau 168 bit	48	XOR, S-Boxes tetap	Financial, PGP, S/MIME
IDEA	128 bit	8	XOR, jumlah, kali	PGP
Blowfish	Variasi hingga 448 bit	16	XOR, S-Boxes variabel, jumlah	
RC5	Variasi hingga 2048 bit	Hingga 255	Jumlah, kurang, XOR, rotasi	
CAST-128	40 - 128bit	16	Jumlah, kurang, XOR, rotasi, S-Boxes tetap	PGP