



# Keamanan Komputer

## Prinsip Enkripsi Konevnsional

Muhammad Adri, S.Pd, MT

AMIK - STMIK Jayanusa Padang  
2008

## Prinsip Enkripsi Konvensinal

- Skema enkripsi konevensional, memiliki 5 kompoen dasar, yaitu :
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Keamanan sangat tergantung pada kerahasiaan kunci yang digunakan, bukan pada kerahasiaan algoritma yang dipakai.

## Enkripsi Konvensional - Secure

- Terdapat dua kebutuhan untuk mengamankan enkripsi konvensional, yaitu :
  - Dibutuhkan suatu algoritma yang kokoh.
  - Pengirim dan Penerima harus memiliki kopi kunci rahasia yang digunakan secara aman dan menjaga keamanan kunci tersebut

## Klasifikasi Kriptografi

- Secara umum kriptografi diklasifikasikan atas 3 dimensi yang independen :
  - Jenis operasi yang digunakan untuk mengubah plainteks menjadi ciperteks
    - Substitusi
    - Transposisi
  - Jumlah kunci yang digunakan
    - Single key, secret key, symmetrical key encryption
    - Two key, public key encryption
  - Metoda yang digunakan untuk memproses plainteks
    - Pemrosesan secara *Block Cipher* atau *Stream Cipher*

## Cryptanalysis

- *Cryptanalysis*, adalah suatu aktifitas/ proses untuk membuka ciperteks menjadi plainteks.
- Strategi yang digunakan oleh cryptanalisis tergantung pada skema dan informasi yang dimilikinya
  - Skema enkripsi adalah *computationally secure*.

## Time Key Analysis

Ukuran Key (bits)	Jumlah key alternatif	Waktu yang dibutuhkan untuk dekripsi pada $10^6/\mu\text{s}$
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	$5.4 \times 10^{18}$ years
168	$2^{168} = 3.7 \times 10^{50}$	$5.9 \times 10^{30}$ years

## Block Chiper

- *Block Chiper* : Metoda yang digunakan untuk mengubah suatu plainteks menjadi chiperteks, dengan metoda block data.
- Beberapa algoritma block chiper yang populer dalam enkripsi konvensional :
  - Feistel Chiper , Data Encryption Standard (DES), Triple DES (TDEA), IDEA, Blowfish, RC-5 dan CAST-128

## Feistel

- 2 Word Bit Plaintext
- Dibagi menjadi dua bagian 1 word bit Half Left (Lo) dan 1 word bit Half Right (Ro)

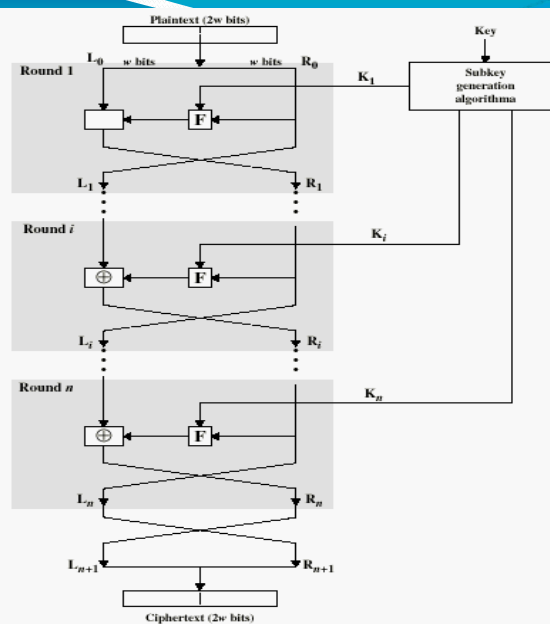


Figure 2.2 Classical Feistel Network

## Feistel Chiper - Struktur

- **Ukuran Blok (*Block size*):** semakin besar ukuran blok, berarti semakin kuat sekuriktinya.
- **Ukuran Kunci (*Key Size*):** Semakin besar ukuran kunci, bermakna semakin kuat sekuritasnya
- **Jumlah perulangan fungsi Feistel (*Number of rounds*):** semakin banyak jumlah perulangan (*multiple rounds*) bedampak terhadap meningkatnya sekuriti
- **Algoritma Pembangkit Subkey (*Subkey generation algorithm*) :** semakin kompleks algoritma yang digunakan, maka semakin tinggi tingkat kesulitan menganalisisnya (cryptanalisis)
- **Fast software encryption/decryption:** Kecepatan eksekusi algoritma