Sekuritas Jaringan

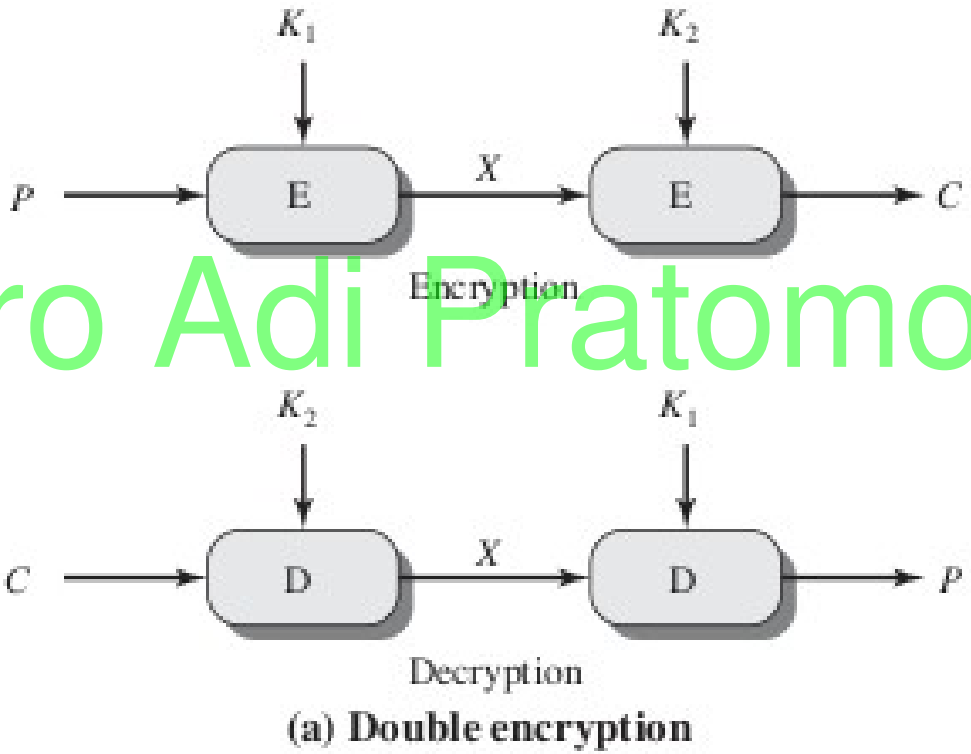
Pertemuan 4

Baskoro Adi P.

Double DES & Triple Des

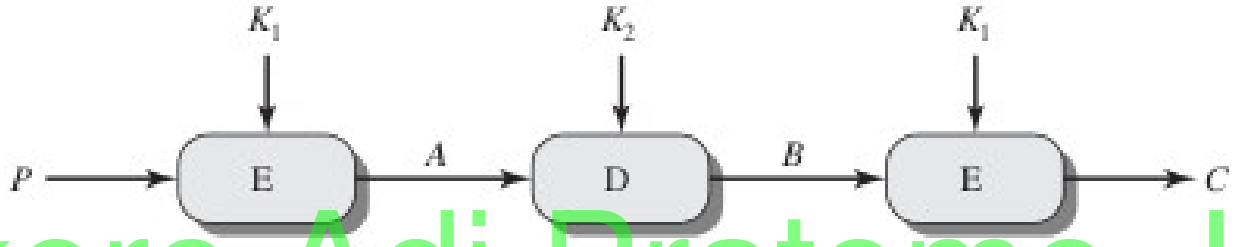
Baskoro Adi Pratomo, Lab KBJ

Double DES



(a) **Double encryption**

Triple DES



(b) Triple encryption

Pseudorandom Number Generator

Baskoro Adi Pratomo, Lab KBJ

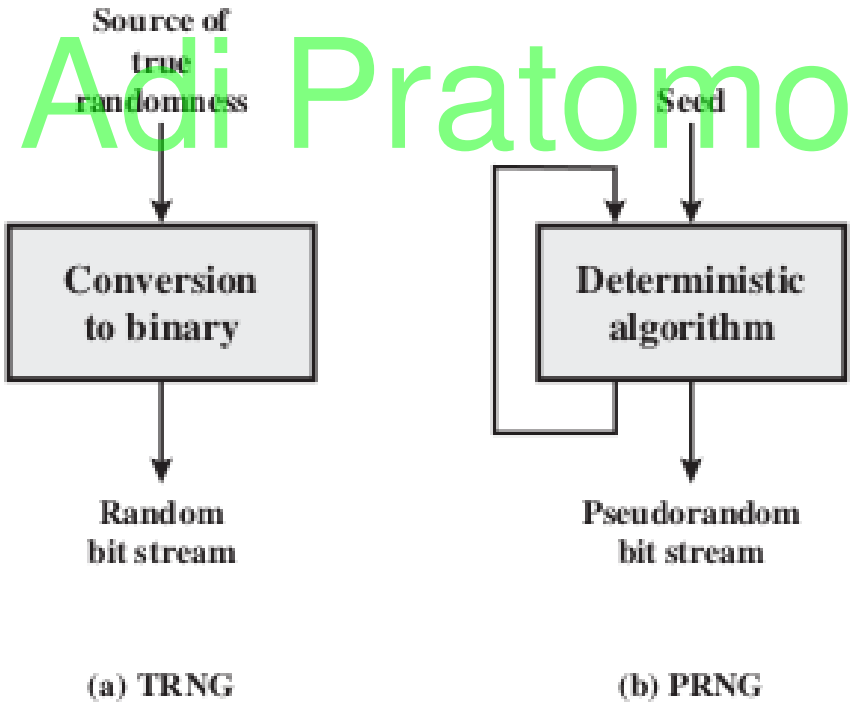
One Time Pad

- Penggunaan kunci dengan isi yang acak dan sepanjang pesan, serta digunakan untuk sekali enkripsi

```
      H       E       L       L       O  message
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) message + key (mod 26)
      E       Q       N       V       Z  → ciphertext
```

Generate Random Number

- True Random Number Generator (TRNG)
- Pseudorandom Number Generator (PRNG)



PRNG Requirements

- Randomness
  - Uniformity
  - Scalability
  - Consistency
- Unpredictability
  - Forward unpredictability
  - Backward unpredictability
- Seed Requirement

PRNG Algorithm

- Purpose Built Algorithm
  - Linear Congruential Generator
  - Blum Blum Shub Generator
- Algorithm based on existing cryptographic algorithm
  - Symmetric Cipher
  - Asymmetric Cipher
  - Hash Function & MAC

Linear Congruential Generators

- $X_{n+1} = (aX_n + c) \bmod m$
- Dimana :
  - m : modulus : m > 0
  - a : multiplier : 0 < a < m
  - c : increment : 0 <= c < m
  - X_0 : Seed / nilai awal : 0 <= X_0 < m

Linear Congruential Generators (2)

- Jika :
  - A = C = 1
  - A = 7, C = 0, M = 32, X_0 = 1
  - A = 5, C = 0, M = 32, X_0 = 1
  - A = 7^5, C = 0, M = 2^{31}, X_0 = 1
- Bagaimana random number yang dihasilkan?

Blum Blum Shub

- Cari dua bilangan p dan q, dimana :
  - p mod 4 = q mod 4 = 3
- n = p x q
- Pilih random number s, dimana :
  - n dan s adalah relatively prime
    - GCD (n, s) = 1
- Generator :

$$X_0 = s^2 \bmod n$$

$$\textbf{for}\ i = 1\ \textbf{to}\ \infty$$

$$X_i = (X_{i-1})^2 \bmod n$$

$$B_i = X_i \bmod 2$$

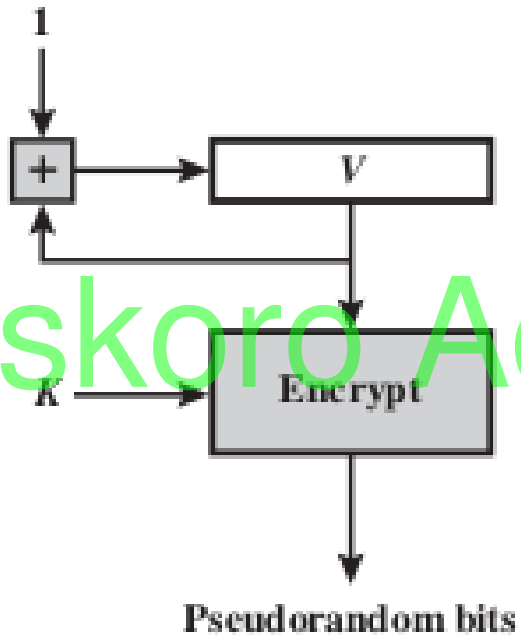
Blum Blum Shub (2)

- Contoh :
  - Jika p = 383, q = 503, s = 101355, hitung B_1

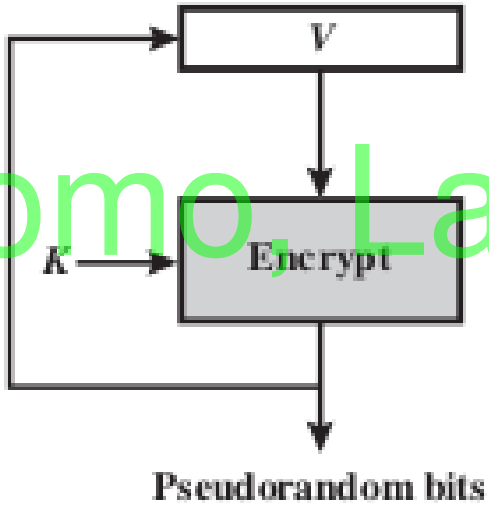
Table 7.1 Example Operation of BBS Generator

i	X_i	B_i
0	20749	
1	143135	1
2	177671	1
3	97048	0
4	89992	0
5	174051	1
6	80649	1
7	45663	1
8	69442	0
9	186894	0
10	177046	0
11	137922	0
12	123175	1
13	8630	0
14	114386	0
15	14863	1
16	133015	1
17	106065	1
18	45870	0
19	137171	1
20	48060	0

PRNG Using Block Cipher



(a) CTR mode



(b) OFB mode

ANSI X9.17 PRNG

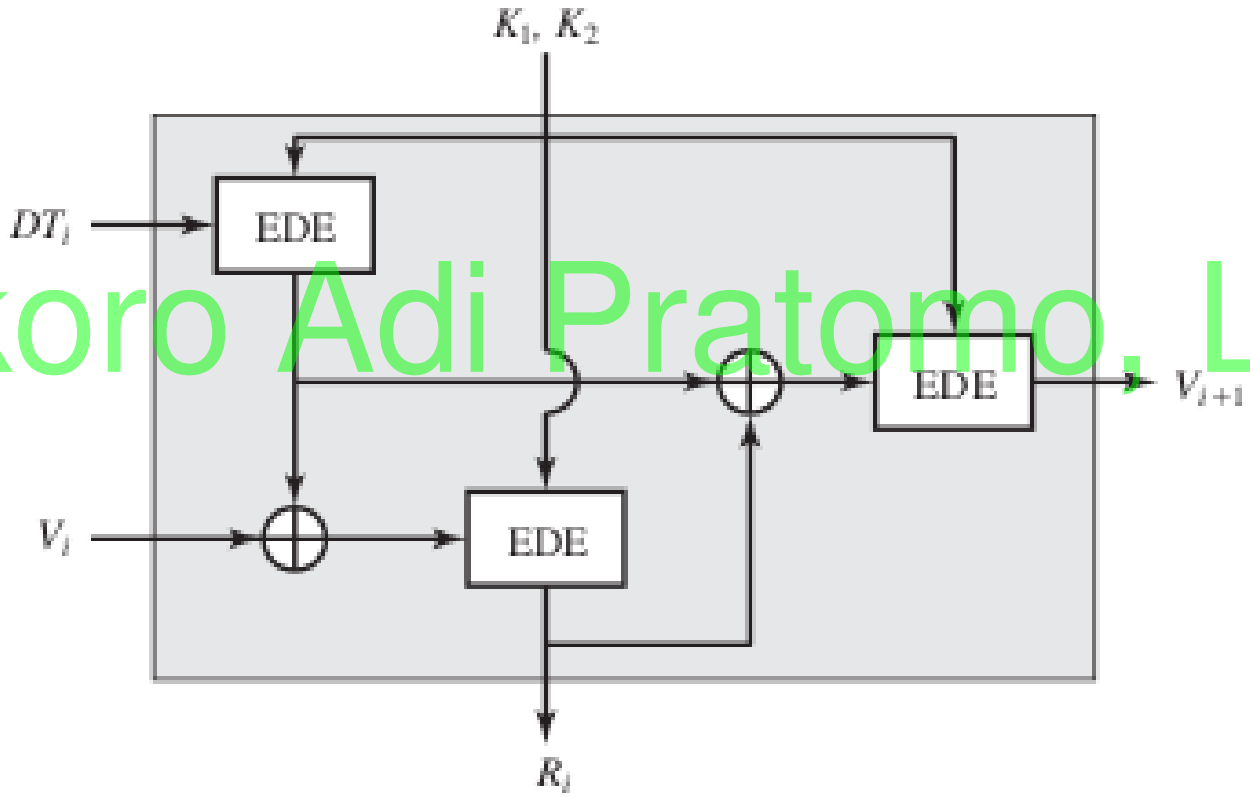


Figure 7.4 ANSI X9.17 Pseudorandom Number Generator

Stream Cipher

Baskoro Adi Pratomo, Lab KBJ

Stream Cipher

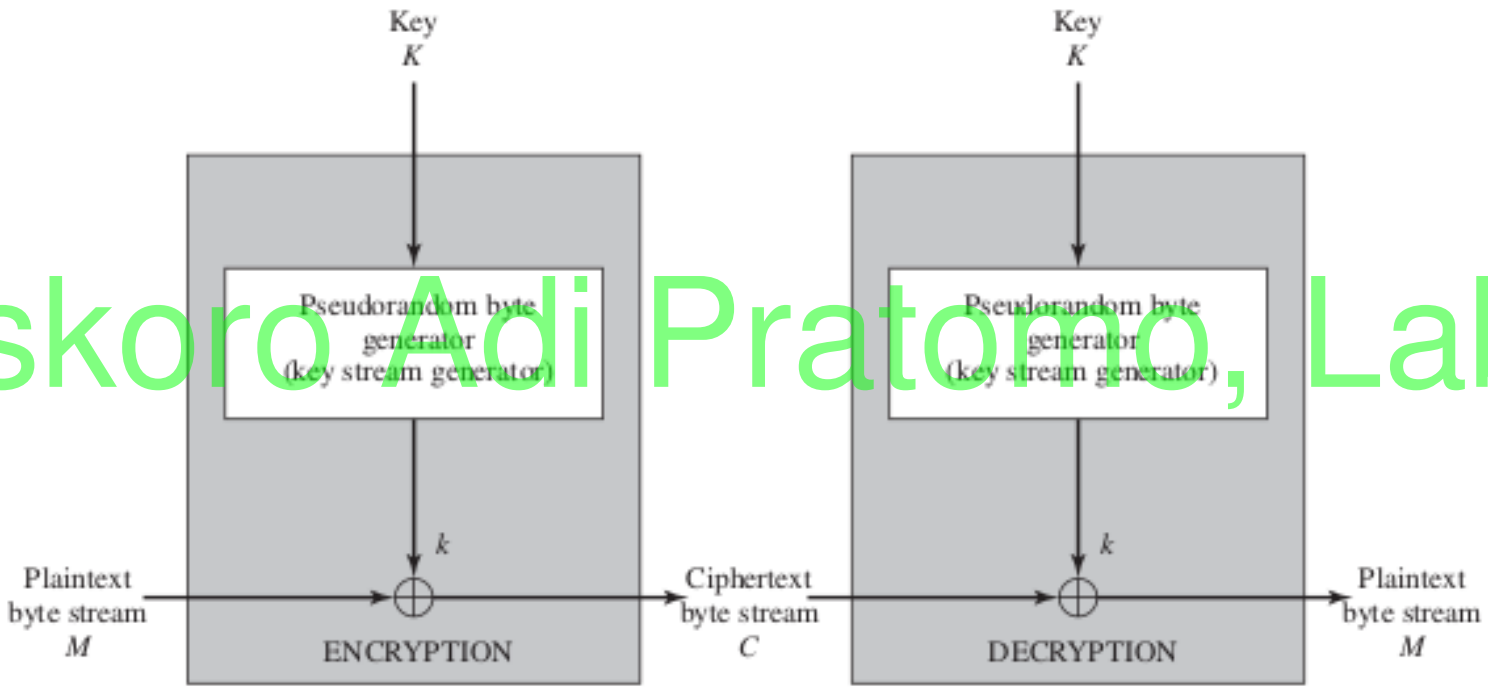


Figure 7.5 Stream Cipher Diagram

Perbandingan Kecepatan

Table 7.4 Speed Comparisons of Symmetric Ciphers on a Pentium II

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	Variable	0.9
RC4	Variable	45

RC4

- Dibuat pada 1987
- Key size : 1-256 bytes
- Operasi : per-byte
- Digunakan di :
  - Secure Socket Layer
  - WEP
  - WPA

RC4 Algorithm

- Siapkan 256 byte state vector S
  - S[0]=0,S[1]=1,S[2]=2,...,S[255]=255
- Inisialisasi :
  - ```
    for i = 0 to 255 do
        S[i] = i;
        T[i] = K[i mod keylen];
    ```
- Permutasi Awal untuk S :
  - ```
    j = 0;
    for i = 0 to 255 do
        j = (j + S[i] + T[i]) mod 256;
        Swap (S[i], S[j]);
    ```

RC4 Algorithm (2)

- Keystream Generation
  - ```
    i, j = 0;
    while (true)
        i = (i + 1) mod 256;
        j = (j + S[i]) mod 256;
        Swap (S[i], S[j]);
        t = (S[i] + S[j]) mod 256;
        k = S[t];
    ```
- Enkripsi :
  - k XOR data
    ```

TUGAS PROGRAMMING
&
DISKUSI