

Bahan kuliah IF4020 Kriptografi

# Review Beberapa Block Cipher (Bagian 2: GOST, RC5, dll)



Oleh: Rinaldi Munir

Program Studi Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung  
2023

# GOST

# Tinjauan Umum GOST (Magma)

- *GOST* = *Gosudarstvenny Standard*, artinya standard pemerintah, disebutkan di dalam standard GOST 28147-89 (RFC 5830).
- Merupakan algoritma enkripsi *cipher* blok standard dari negara Uni Soviet dulu (USSR).
- Pada mulanya *cipher* blok ini tidak mempunyai nama, tetapi di dalam standard yang baru, GOST R 34.12-2015 (RFC 7801, RFC 8891), *cipher* blok ini dinamakan *Magma*.
- GOST dikembangkan pada tahun 1970 namun baru dirilis kepada publik pada tahun 1990 setelah Uni Soviet bubar.
- Dibuat oleh Soviet sebagai alternatif terhadap algoritma enkripsi standard Amerika Serikat, *DES*.
- *GOST* secara struktural mirip dengan *DES* (menggunakan jaringan Feistel)

- Ukuran blok pesan = 64 bit
- Panjang kunci = 256 bit
- Jumlah putaran = 32 putaran
- Setiap putaran menggunakan kunci putaran.
- Kunci putaran sebenarnya hanya ada 8 buah,  $K_1$  sampai  $K_8$ , namun karena ada 32 putaran, maka 8 buah kunci putaran ini dijadwalkan penggunaannya.

**Tabel 6.2** Penjadwalan kunci internal GOST

Putaran	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Kunci internal	$K_1$	$K_2$	$K_3$	$K_4$	$K_5$	$K_6$	$K_7$	$K_8$	$K_1$	$K_2$	$K_3$	$K_4$	$K_5$	$K_6$	$K_7$	$K_8$

Putaran	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Kunci internal	$K_1$	$K_2$	$K_3$	$K_4$	$K_5$	$K_6$	$K_7$	$K_8$	$K_8$	$K_7$	$K_6$	$K_5$	$K_4$	$K_3$	$K_2$	$K_1$

- Standard GOST yang baru menspesifikasikan *cipher* blok 128-bit yang diberi nama *Kuznyechik*.

- Pembangkitan kunci putaran sangat sederhana.
- Kunci eksternal yang panjangnya 256 bit dibagi ke dalam delapan bagian yang masing-masing panjangnya 32 bit.
- Delapan bagian ini yang dinamakan  $K_1, K_2, \dots, K_8$ .
- Contoh:  $K = \text{'abcdefghijklmnopqrstuvwxy123456'}$  (32 x 8 bit = 256 bit)

maka  $K_1 = \text{'abcd'}$

$K_5 = \text{'qrst'}$

$K_2 = \text{'efgh'}$

$K_6 = \text{'uvwx'}$

$K_3 = \text{'ijkl'}$

$K_7 = \text{'yz12'}$

$K_4 = \text{'mnop'}$

$K_8 = \text{'3456'}$

- *GOST* menggunakan Jaringan *Feistel*

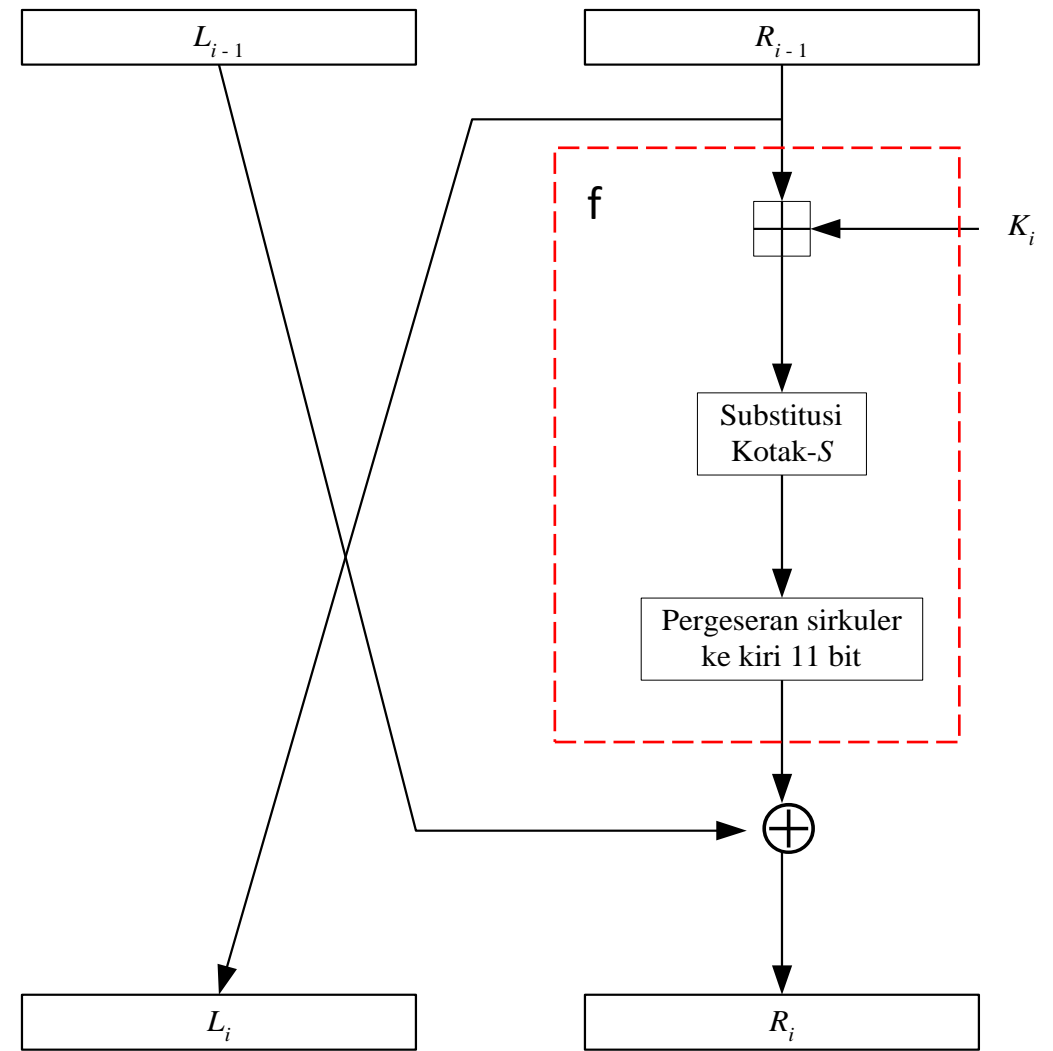
- Satu putaran *GOST*:


$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

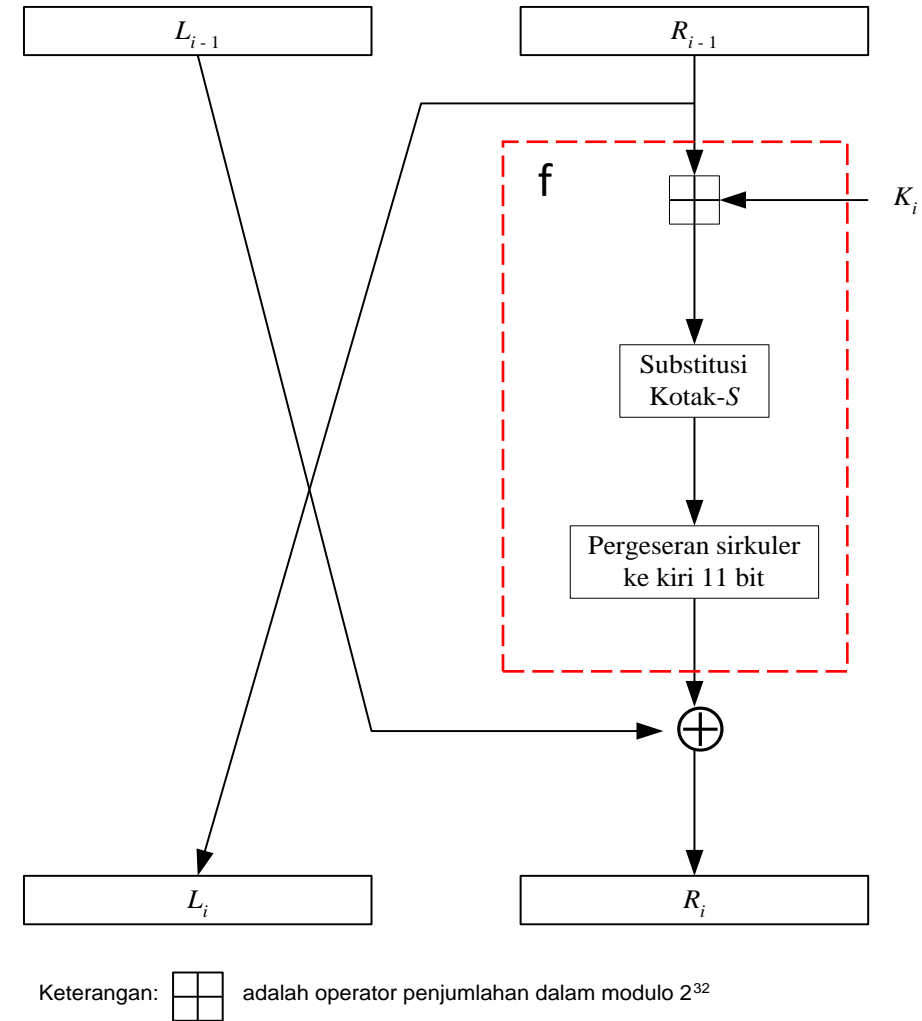
- Fungsi  $f$  terdiri dari

- penjumlahan dalam modulus  $2^{32}$
- substitusi
- pergeseran



Keterangan:  adalah operator penjumlahan dalam modulo  $2^{32}$

- Hasil penjumlahan  $R_{i-1}$  dengan  $K_i$  menghasilkan luaran yang panjangnya 32 bit.
- Luaran ini dibagi menjadi 8 bagian yang masing-masing panjangnya 4 bit.
- Setiap 4 bit masuk ke dalam kotak  $S$  untuk proses substitusi. Empat bit pertama masuk ke dalam kotak  $S$  pertama, 4 bit kedua masuk ke dalam kotak  $S$  kedua, demikian seterusnya.
- Hasil substitusi setiap kotak  $S$  adalah 4 bit. *GOST* memiliki 8 buah kotak  $S$ , setiap kotak berisi 16 buah elemen nilai. Setiap kotak berisi permutasi angka 0 sampai 15.



Kotak-S 1:															
4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

Kotak-S 2:															
14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9

Kotak-S 3:															
5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11

Kotak-S 4:															
7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3

Kotak-S 5															
6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2

Kotak-S 6:															
4	11	10	0	7	2	1	13	3	6	8	5	9	12	14	14

Kotak-S 7:															
13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12

Kotak-S 8:															
1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12



- Misalnya pada kotak  $S$  pertama, masukannya:

0010            (nilai desimal 2)

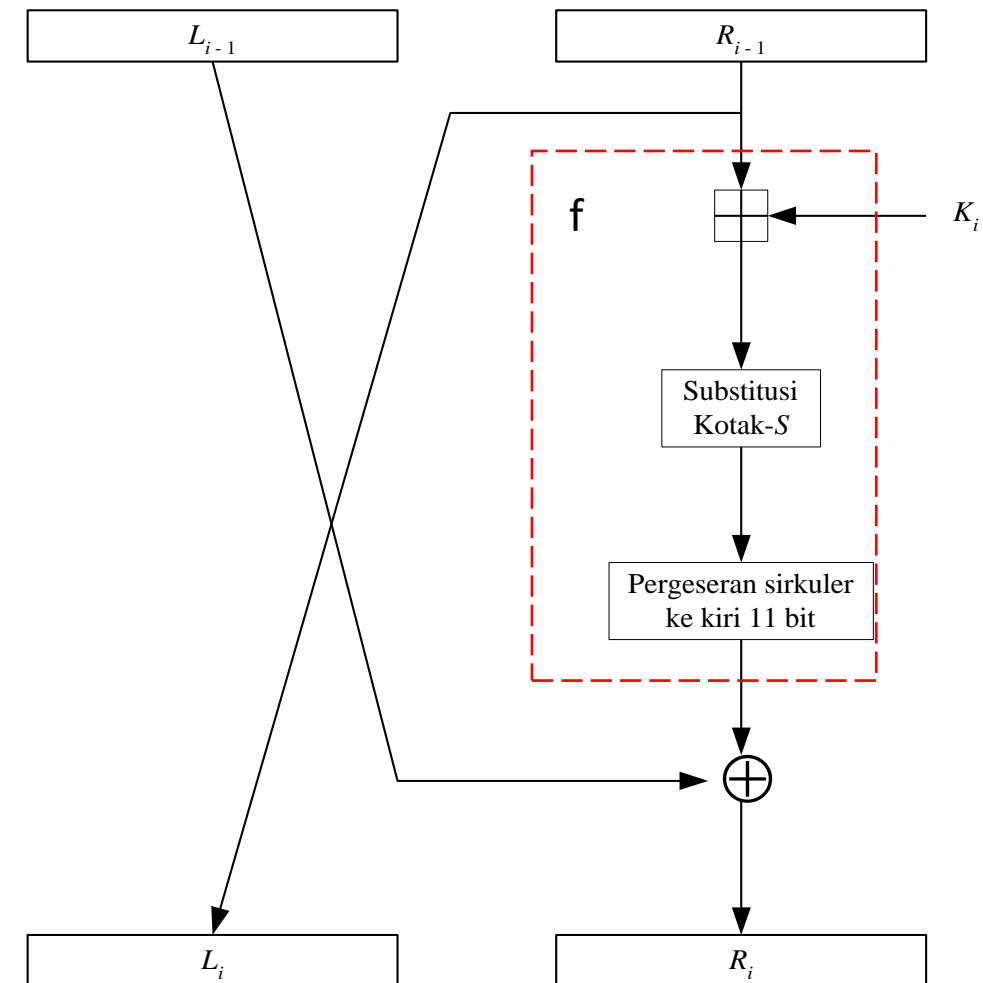
maka luarannya: nilai di dalam elemen ke-2:


9 atau 1001

Kotak- $S$ 1:															
4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

- Hasil substitusi dari semua kotak  $S$  ini digabung menjadi pesan 32-bit.

- Kemudian pesan 32-bit ini digeser ke kiri sejauh 11 bit secara sirkuler.
- Hasilnya kemudian di-*XOR*-kan dengan  $L_{i-1}$  untuk kemudian memberikan bagian cipherteks kanan yang baru,  $R_i$ . Proses ini diulang sebanyak 32 kali.
- Dekripsi merupakan kebalikan dari enkripsi. Dari “bawah” ke “atas” mengikuti jaringan Feistel.



Keterangan:  adalah operator penjumlahan dalam modulo  $2^{32}$

## Perbedaan GOST dengan DES:

1. Kunci *DES* 56 bit, sedangkan kunci GOST lebih panjang yaitu 256 bit. Ini menyebabkan *exhaustive key search* terhadap *GOST* lebih sukar dibandingkan dengan *DES*.
2. Jumlah putaran *DES* 16 kali, sedangkan *GOST* lebih banyak yaitu 32 kali sehingga membuat kriptanalisis menjadi sangat sulit
3. Kotak *S* di dalam *DES* menerima masukan 6 bit dan luaran 4 bit (berukuran  $6 \times 4$ ), sedangkan kotak *S* di dalam *GOST* menerima masukan 4 bit dan luaran 4 bit (berukuran  $4 \times 4$ )
4. Pembangkitan kunci internal *DES* rumit, sedangkan di dalam *GOST* pembangkitan kunci internalnya sederhana
5. *DES* mempunyai permutasi yang tidak teratur, sedangkan *GOST* hanya menggunakan pergeseran 11-bit secara sirkuler

## Cryptanalysis of GOST [\[ edit \]](#)

---

The latest cryptanalysis of GOST shows that it is secure in a theoretical sense. In practice, the data and memory complexity of the best published attacks has reached the level of practical, while the time complexity of even the best attack is still  $2^{192}$  when  $2^{64}$  data is available.

Since 2007, several attacks have been developed against reduced-round GOST implementations and/or [weak keys](#).<sup>[6][7]</sup>

In 2011 several authors discovered more significant flaws in GOST, being able to attack the full 32-round GOST with arbitrary keys for the first time. It has even been called "a deeply flawed cipher" by [Nicolas Courtois](#).<sup>[8]</sup> Initial attacks were able to reduce time complexity from  $2^{256}$  to  $2^{228}$  at the cost of huge memory requirements,<sup>[9]</sup> and soon they were improved up to  $2^{178}$  time complexity (at the cost of  $2^{70}$  memory and  $2^{64}$  data).<sup>[10][11]</sup>

In December 2012, Courtois, Gawinecki, and Song improved attacks on GOST by computing only  $2^{101}$  GOST rounds.<sup>[12]</sup> Isobe had already published a single key attack on the full GOST cipher,<sup>[13]</sup> which Dinur, Dunkelman, and Shamir improved upon, reaching  $2^{224}$  time complexity for  $2^{32}$  data and  $2^{36}$  memory, and  $2^{192}$  time complexity for  $2^{64}$  data.<sup>[14]</sup>

Since the attacks reduce the expected strength from  $2^{256}$  (key length) to around  $2^{178}$ , the cipher can be considered broken. However, for any block cipher with block size of  $n$  bits, the maximum amount of plaintext that can be encrypted before rekeying must take place is  $2^{n/2}$  blocks, due to the [birthday paradox](#),<sup>[15]</sup> and none of the aforementioned attacks require less than  $2^{32}$  data.

Sumber: Wikipedia

# RC5

# RC5

- *RC5* dibuat oleh Ronald Rivest dari Laboratorium *RSA* pada tahun 1994.
- Salah satu finalis AES, yaitu *RC6*, dikembangkan dari *RC5*
- Tidak seperti algoritma *cipher* blok lainnya, *RC5* mempunyai:
  - ukuran blok yang variabel (16, 32, 64)
  - panjang kunci yang variabel (0 sampai 2040 bit)
  - dan jumlah putaran yang variabel (0 sampai 255).

Parameter	Simbol	Nilai yang dibolehkan
Ukuran blok (dalam bit)	$w$	16, 32, 64
Jumlah putaran	$r$	0, 1, ..., 255
Panjang kunci eksternal $K$ (dalam <i>byte</i> , 1 <i>byte</i> = 8 bit)	$b$	0, 1, ..., 255

## Pembentukan Kunci Putaran

- Kunci putaran ada sebanyak  $2r + 2$  buah yang masing-masing disimpan di dalam elemen-elemen larik yang dilabeli sebagai  $S[0], S[1], \dots, S[t - 1]$  dengan  $t = 2r + 2$ .
- Setiap elemen larik panjangnya satu *word* (1 *word* =  $w$  bit)

Parameter	Simbol	Nilai yang dibolehkan
Ukuran blok (dalam bit)	$w$	16, 32, 64
Jumlah putaran	$r$	0, 1, ..., 255
Panjang kunci eksternal $K$ (dalam <i>byte</i> , 1 <i>byte</i> = 8 bit)	$b$	0, 1, ..., 255

- Mula-mula, semua *byte* dari kunci eksternal,  $K[0..b - 1]$ , disalin ke dalam larik  $L$  yang berukuran  $c$  *word*,  $L[0.. c - 1]$  . (ingat:  $b$  dalam *byte*,  $c$  dalam *word*,  $c < b$ )
- lalu *padding* dengan sejumlah 0 jika perlu (*padding* terjadi jika  $b$  bukan kelipatan  $w$ ).
- Kemudian inisialisasi larik  $S$  sebagai berikut:

```

S[0] ← Pw
for i ← 1 to t - 1 do
    S[i] ← S[i - 1] + Qw
endfor

```

Parameter	Simbol	Nilai yang dibolehkan
Ukuran blok (dalam bit)	$w$	16, 32, 64
Jumlah putaran	$r$	0, 1, ..., 255
Panjang kunci eksternal $K$ (dalam <i>byte</i> , 1 <i>byte</i> = 8 bit)	$b$	0, 1, ..., 255



yang dalam hal ini nilai  $P_w$  dan  $Q_w$  (dalam heksadesimal) berbeda-beda bergantung pada  $w$  sebagai berikut [STA98]:

$w$	16	32	64
$P_w$	B7E1	B7E15163	B7E151628AED2A6B
$Q_w$	9E37	9E3779B9	9E3779B97F4A7C15

Konstanta  $P_w$  dan  $Q_w$  didasarkan pada representasi bilangan alam  $e$  dan  $\phi$  dalam biner,

$$P_w = \text{Odd}[(e - 2)2^w]$$

$$Q_w = \text{Odd}[(\phi - 1)2^w]$$

Odd adalah fungsi yang memberikan integer ganjil terkecil yang dekat dengan input yang diberikan

yang dalam hal ini,

$$e = 2.718281828459\dots$$

$$\phi = 1.618033988749\dots = \frac{1 + \sqrt{5}}{2}$$

Akhirnya, campurkan  $L$  dan  $S$  sebagai berikut:

```
i ← 0
j ← 0
X ← 0
Y ← 0
n ← 3 * max(r, c)
for k ← 1 to n do
    S[i] ← (S[i] + X + Y) <<< 3
    X ← S[i]
    i ← (i + 1) mod (t)
    L[j] ← (L[j] + X + Y) <<< ( X + Y)
    Y ← L[j]
    j ← (j + 1) mod (c)
endfor
```

# Enkripsi

- Tinjau *RC5* dengan ukuran blok 64 bit dan jumlah putaran  $r$ .
- Enkripsi menggunakan kunci putaran  $S_0, S_1, \dots, S_{2r+2}$  yang masing-masing panjangnya 32-bit.
- Dua kunci putaran digunakan untuk setiap putaran  $i = 1, 2, \dots, r$  dan dua buah kunci putaran tambahan sebelum putaran pertama jadi seluruhnya ada  $2r + 2$  buah kunci internal).
- Untuk melakukan enkripsi, mula-mula blok plainteks dibagi menjadi 2 bagian,  $A$  dan  $B$ , yang masing-masing panjangnya 32 bit. Kemudian masing-masing bagian dijumlahkan (dalam modulo  $2^{32}$ ) dengan  $S_0$  dan  $S_1$ :

$$A \leftarrow A + S[0]$$

$$B \leftarrow B + S[1]$$

Selanjutnya untuk setiap putaran 1 sampai  $r$  dilakukan operasi *XOR*, pergeseran ke kiri secara sirkuler, dan penjumlahan dalam modulo  $2^{32}$  dengan kunci putaran sebagai berikut:

**for**  $i \leftarrow 1$  **to**  $r$  **do**

$A \leftarrow ((A \oplus B) \lll B) + S[2i]$

$B \leftarrow ((B \oplus A) \lll A) + S[2i+1]$

**endfor**

**for**  $i \leftarrow 1$  **to**  $r$  **do**

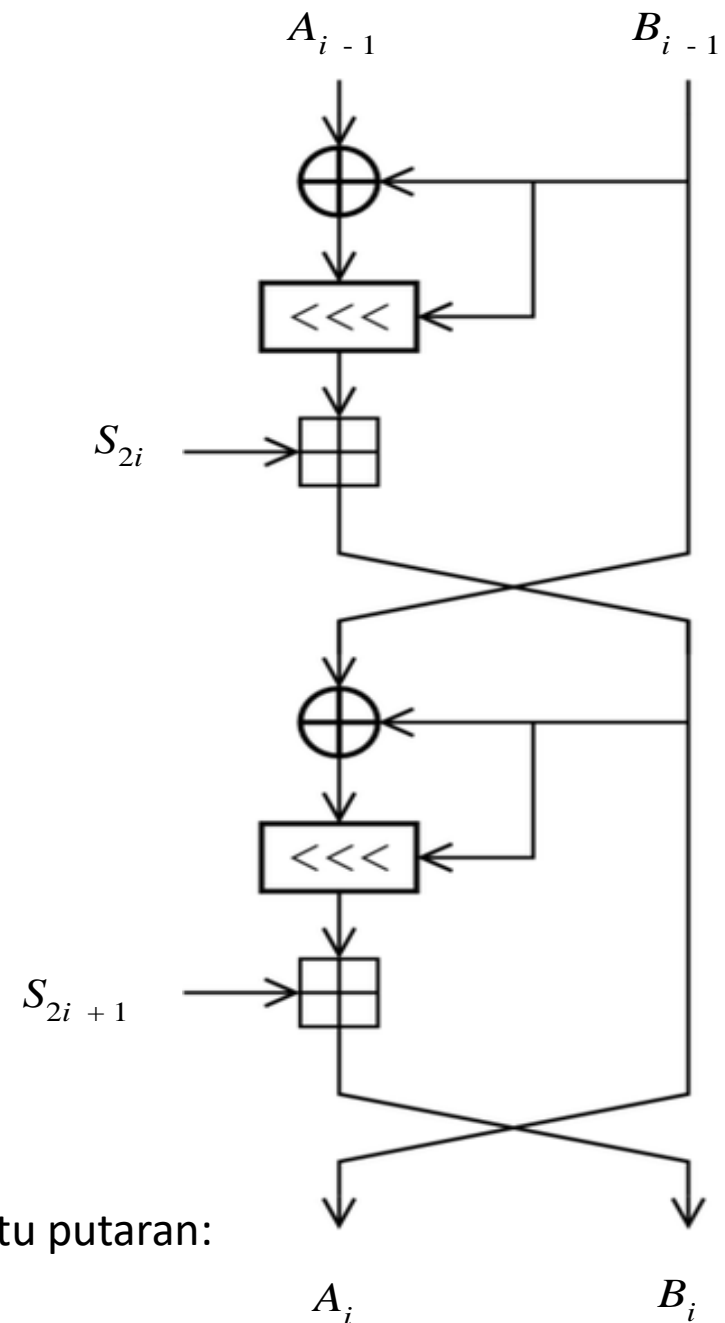
$A \leftarrow ((A \oplus B) \lll B) + S[2i]$

$B \leftarrow ((B \oplus A) \lll A) + S[2i+1]$

**endfor**

Cipherteks pada putaran terakhir disimpan di dalam  $A$  dan  $B$ .

Gabungan keduanya adalah blok cipherteks yang berukuran 64 bit.

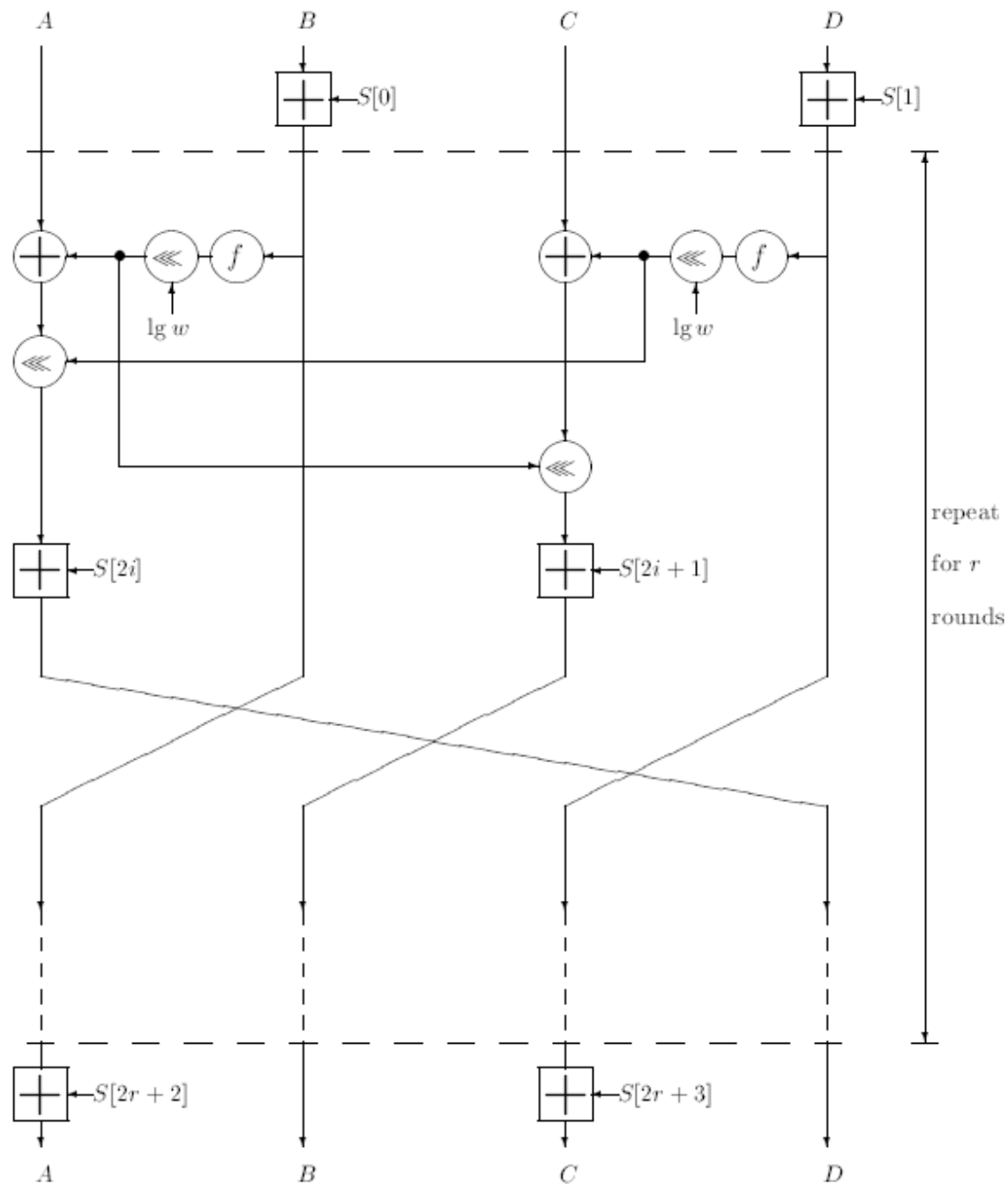


Proses enkripsi satu putaran:

# RC6

# RC6

- RC6 juga dibuat oleh Ronald Rivest, Matt Robshaw, Ray Sidney, dan Yiqun Lisa Yin dari Laboratorium RSA (Rivest, 1998).
- RC6 merupakan pengembangan RC5. RC6 dibuat untuk mengikuti kompetisi Advanced Encryption Standard atau AES (akan dijelaskan pada materi selanjutnya).
- RC6 melakukan enkripsi terhadap blok data berukuran 128 bit, sedangkan ukuran kuncinya bervariasi 128, 192, 256 sampai 2040 bit. Cara pembangkitan kunci internalnya identik dengan RC5.
- Secara struktur, RC6 mirip dengan RC5, begitu juga operasi-operasinya seperti XOR, penjumlahan, dan rotasi. RC6 mempunyai operasi tambahan yaitu perkalian.
- RC6 dapat dipandang sebagai dua buah RC5 yang dioperasikan secara parallel.



Gambar Jaringan Feistel di dalam RC6.  
 Fungsi  $f$  adalah  $f(x) = x(2x + 1)$  (Rivest, 1998)



{ Enkripsi RC6- $w/r/b$

Masukan: Plainteks disimpan di dalam empat register berukuran

$w$  bit:  $A, B, C$  dan  $D$

$r$  adalah jumlah putaran

$S[0, \dots, 2r + 3]$  adalah kunci internal, panjangnya  $w$  bit

Luaran: Cipherteks disimpan di dalam  $A, B, C, D$

}

Algoritma:

$B \leftarrow B + S[0]$

$D \leftarrow D + S[1]$

for  $i \leftarrow 1$  to  $r$  do

$t \leftarrow (B * (2B + 1)) \lll \lg w$

$u \leftarrow (D * (2D + 1)) \lll \lg w$

$A \leftarrow ((A \oplus t) \lll u) + S[2i]$

$C \leftarrow ((C \oplus u) \lll t) + S[2i + 1]$

$(A, B, C, D) = (B, C, D, A)$

end

$A \leftarrow A + S[2r + 2]$

$C \leftarrow C + S[2r + 3]$

{ Dekripsi RC6- $w/r/b$

Masukan: Cipherteks disimpan di dalam empat register berukuran

$w$  bit:  $A, B, C$  dan  $D$   $r$  adalah jumlah putaran

$S[0, \dots, 2r + 3]$  adalah kunci internal, panjangnya  $w$  bit

Luaran: Plainteks disimpan di dalam  $A, B, C, D$

}

Algoritma:

$$C \leftarrow C - S[2r + 3]$$

$$A \leftarrow A - S[2r + 2]$$

for  $i \leftarrow r$  downto 1 do

$$(A, B, C, D) \leftarrow (D, A, B, C)$$

$$u \leftarrow (D * (2D + 1)) \ll \lg w$$

$$t \leftarrow (B * (2B + 1)) \ll \lg w$$

$$C \leftarrow ((C - S[2i + 1]) \gg t) \oplus u$$

$$A \leftarrow ((A - S[2i]) \gg u) \oplus t$$

end

$$D \leftarrow D - S[1]$$

$$B \leftarrow B - S[0]$$

## Keterangan:

$a + b$  adalah penjumlahan dalam modulo  $2^w$

$a - b$  adalah pengurangan dalam modulo  $2^w$

$a \oplus b$  adalah operasi *bitwise* XOR dari word yang panjangnya  $w$  bit

$a \times b$  adalah perkalian dalam modulo  $2^w$

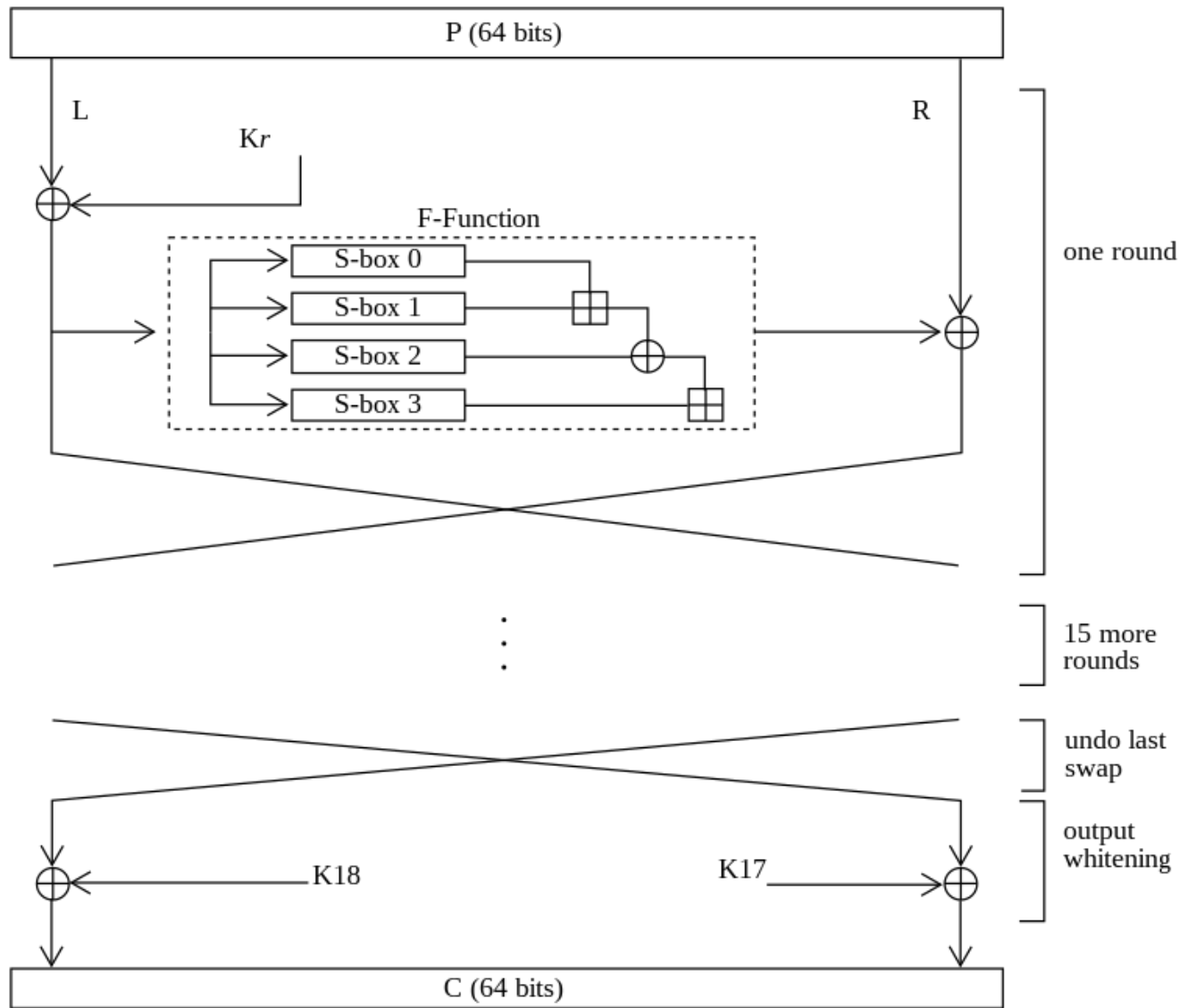
$a \lll b$  adalah operasi pergeseran  $a$  (yang panjangnya  $w$  bit) ke kiri secara sirkular sejauh  $\log w$  *least significant* bit dari  $b$

$a \ggg b$  adalah operasi pergeseran  $a$  (yang panjangnya  $w$  bit) ke kanan secara sirkular sejauh  $\log w$  *least significant* bit dari  $b$

# Cipher blok lainnya

# Blowfish

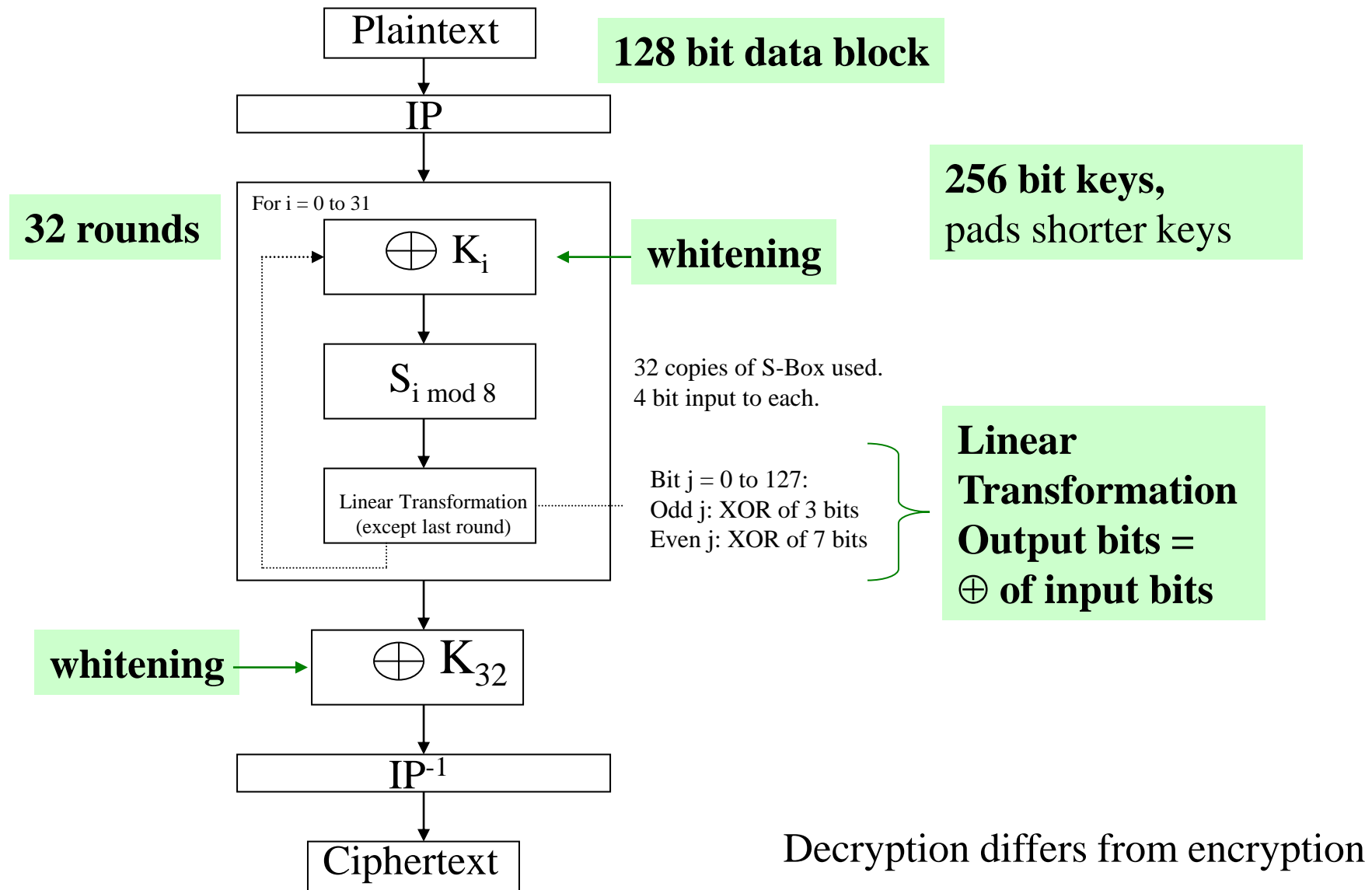
- Dirancang oleh Bruce Schneier tahun 1993.
- Ukuran blok plainteks dan cipherteks di dalam Blowfish adalah 64 bit
- Panjang kunci 32 sampai 448 bit
- Jumlah putaran 16 kali, setiap putaran melakukan operasi substitusi-permutasi
- Jumlah kotak S-box adalah 4 buah



P=Plaintext; C=Ciphertext;  $K_x$  = P-array-entry  $x$   
 $\oplus$  = xor                       $\boxplus$  = addition mod  $2^{32}$

# Serpent

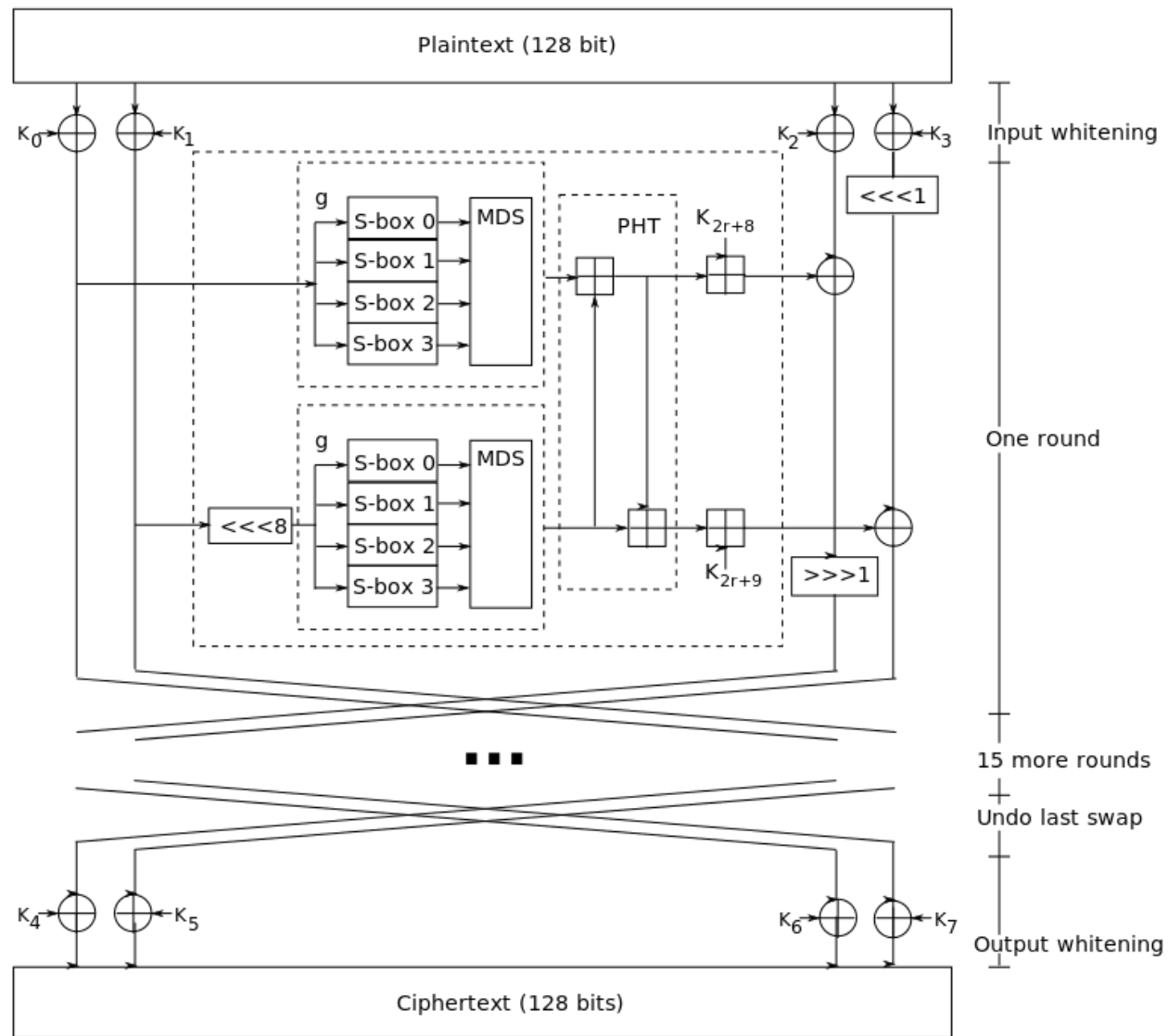
- Salah satu finalis AES (Advanced Encryption Standard)
- Dirancang oleh Ross Anderson, Eli Biham, dan Lars Knudsen.
- Ukuran blok plainteks dan cipherteks di dalam Serpent adalah 128 bit
- Panjang kunci 128, 192, dan 256 bit
- Jumlah putaran 32 kali, setiap putaran melakukan operasi substitusi-permutasi
- Jumlah kotak S-box adalah 8 buah





# Twofish

- Salah satu finalis AES (*Advanced Encryption Standard*)
- Dirancang oleh Bruce Schneier.
- Twofish dapat dianggap sebagai kelanjutan dari Blowfish
- Ukuran blok plainteks dan cipherteks di dalam Twofish adalah 128 bit
- Panjang kunci sampai 256 bit
- Jumlah putaran 16 kali, setiap putaran melakukan operasi substitusi-permutasi
- Jumlah kotak S-box adalah 5 buah



**Legend**

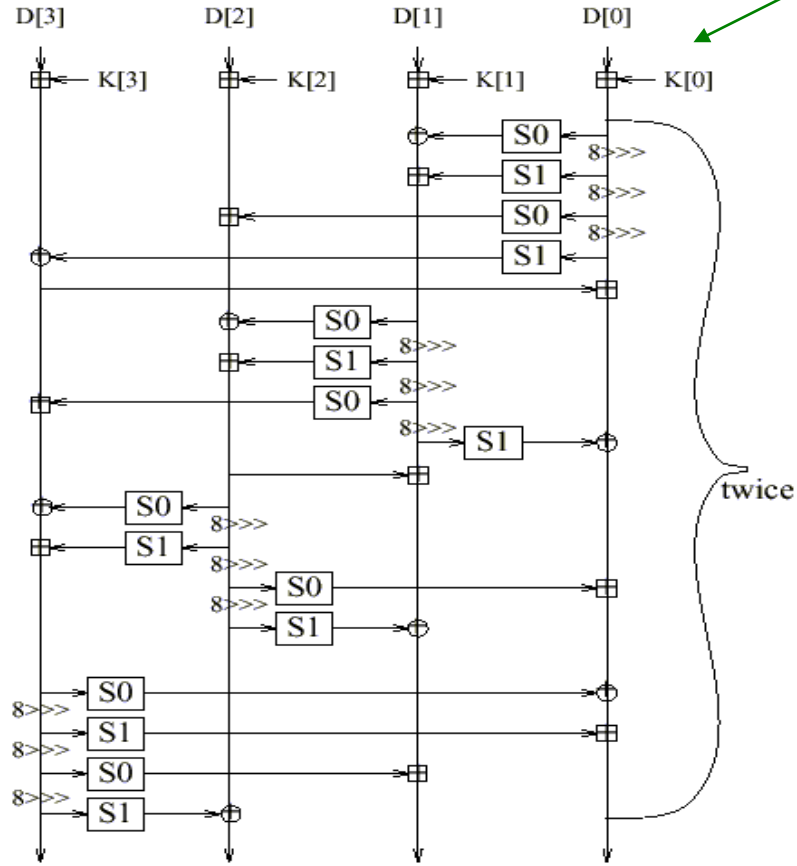
- $\oplus$  Exclusive-or
- $\boxplus$  Addition modulo  $2^{32}$
- $\lll$  Rotation

# MARS

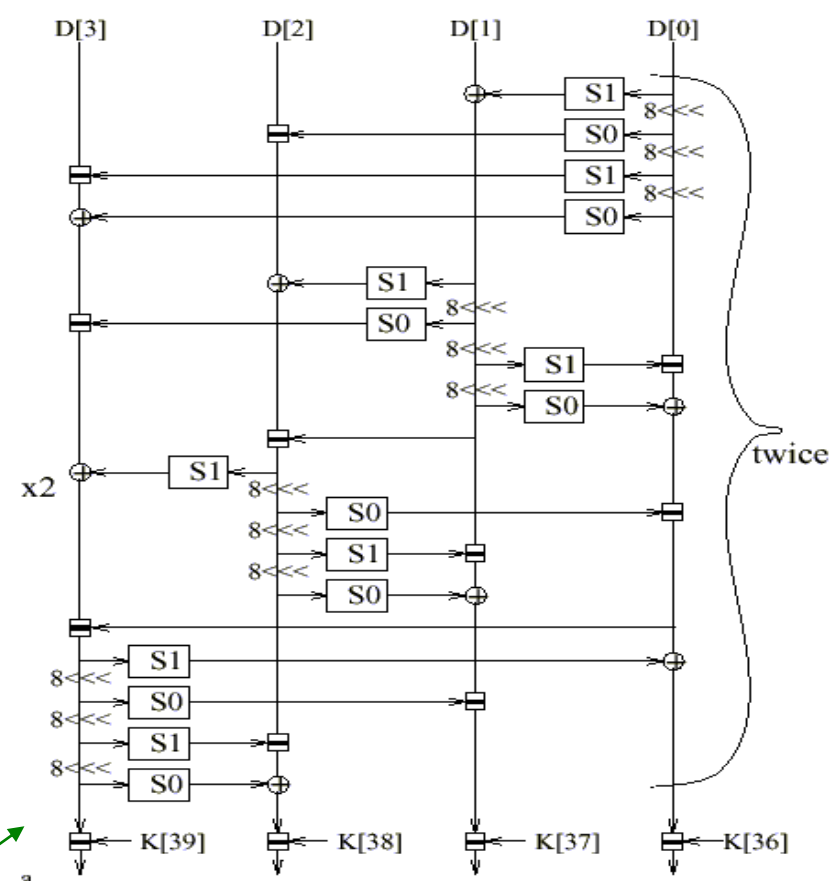
- Salah satu finalis AES (*Advanced Encryption Standard*)
- Dirancang oleh IBM.
- Ukuran blok plainteks dan cipherteks di dalam MARS adalah 128 bit
- Panjang kunci dari 128 sampai 448 bit (pertambahan 32 bit)
- Jumlah putaran 32 kali, setiap putaran melakukan operasi substitusi-permutasi

# Forward Mixing

whitening



# Backward Mixing



⊕ exclusive-or  
 ⊕ addition  
 S0 S1 8 x 32 S-boxes  
 8>>> right-rotation by 8

whitening

a  
 ⊖ subtraction (a-b)  
 ⊕ exclusive-or  
 S0 S1 8 x 32 S-boxes  
 8<<< left-rotation by 8