

Bahan kuliah IF4020 Kriptografi

Review Beberapa Block Cipher dan Stream Cipher (Bagian 2: GOST)

Oleh: Dr. Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
ITB



GOST

Tinjauan Umum GOST

- *GOST* = *Gosudarstvenny Standard*, artinya standard pemerintah,
- Merupakan algoritma enkripsi dari negara Uni Soviet dahulu
- Dikembangkan pada tahun 1970.
- Dibuat oleh Soviet sebagai alternatif terhadap algoritma enkripsi standard Amerika Serikat, *DES*.
- *GOST* secara struktural mirip dengan *DES*

- Ukuran blok pesan = 64 bit
- Panjang kunci = 256 bit
- Jumlah putaran = 32 putaran
- Setiap putaran menggunakan kunci internal.
- Kunci internal sebenarnya hanya ada 8 buah, K_1 sampai K_8 ,
- Karena ada 32 putaran, maka 8 buah kunci internal 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

- Pembangkitan kunci internal 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 .

- *GOST* menggunakan Jaringan *Feistel*

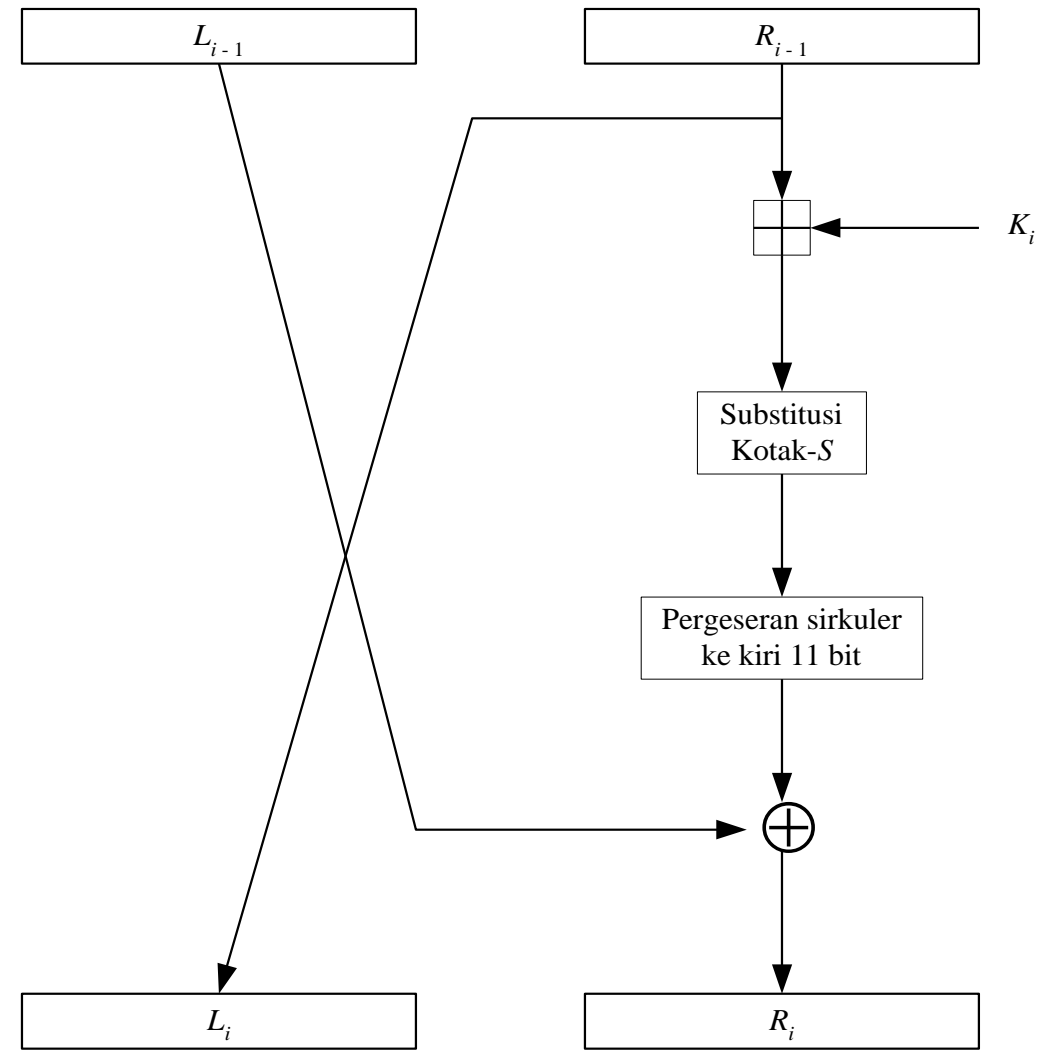
- Satu putaran *GOST*:


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

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

- Fungsi *f* terdiri dari

- penjumlahan modulo 2^{32}
- substitusi
- pergeseran



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

- Hasil penjumlahan R_{i-1} dengan kunci internal ke- i menghasilkan luaran yang panjangnya 32 bit.
- Luaran ini dibagi mejadi 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:

0000 (nilai desimal 0)

maka luarannya: nilai di dalam elemen ke-0:

4 atau 0100

- 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.

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 6×4), sedangkan kotak *S* di dalam GOST menerima masukan 4 bit dan luaran 4 bit (berukuran 4×4)
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

- GOST adalah *cipher* yang aman. Hal ini mungkin disebabkan jumlah putaran dan panjang kunci yang lebih banyak dari DES.
- Belum ada publikasi kriptanalisis tentang *GOST*.