IF4020 Kriptografi

08 - Block Cipher

(Bagian 1)

Oleh: Rinaldi M

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2026

Cipher Blok (*Block Cipher*)

- Berbeda dengan *cipher* alir, pada *cipher* blok plainteks dibagi menjadi blok-blok bit dengan panjang sama. Ukuran blok yang umum adalah 64 bit, 128 bit, 256 bit, dsb.

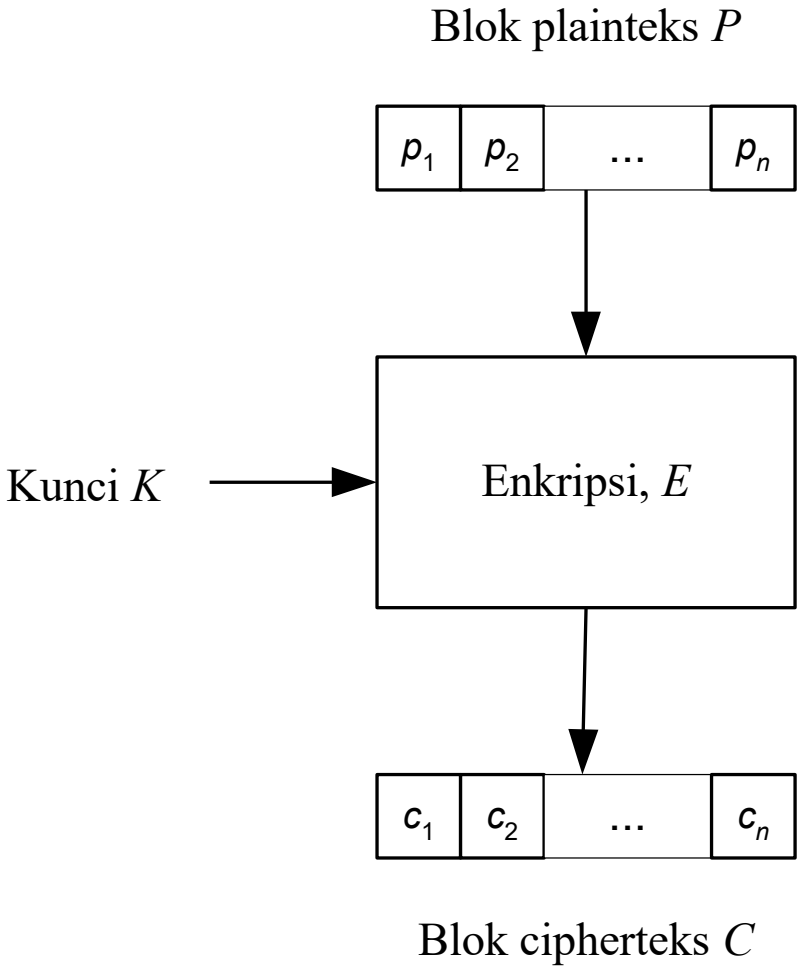
- Panjang blok cipherteks = panjang blok plainteks.

- Enkripsi dilakukan pada setiap blok plainteks dengan menggunakan bit-bit kunci

- Panjang kunci eksternal (yang diberikan oleh pengguna) tidak harus sama dengan panjang blok plainteks. Pada beberapa *cipher* blok, panjang kunci = panjang blok, tetapi pada *cipher* blok yang lain tidak sama.

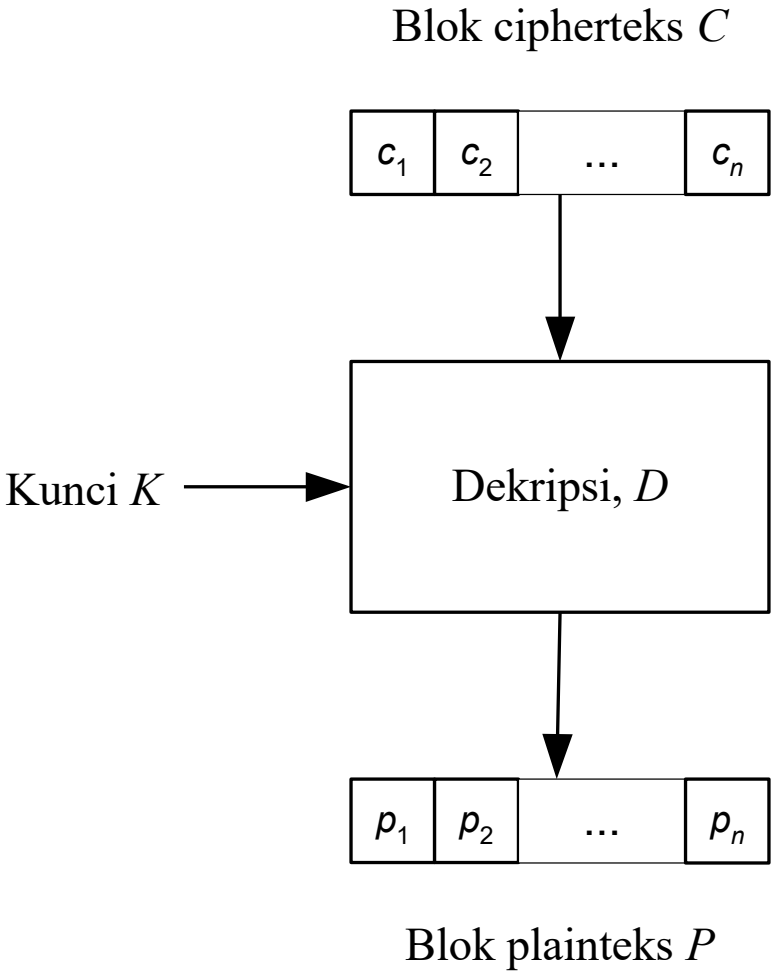
Blok plainteks berukuran *n* bit:

$P = (p_1, p_2, \ldots, p_n)$, $p_i \in \{0, 1\}$



Blok cipherteks berukuran *n* bit:

$C = (c_1, c_2, \ldots, c_n)$, $c_i \in \{0, 1\}$



- *E* dan *D* adalah fungsi enkripsi dan dekripsi dari suatu *cipher* blok dengan parameter kunci *K*:

$$C = E_K(P) \qquad \text{dan } P = D_K(C)$$

- Dimisalkan contoh sebuah fungsi E yang sederhana, tapi tidak cukup aman, sbb:

1. XOR-kan blok plainteks *P* dengan *K*
2. lalu geser secara *wrapping* bit-bit dari hasil langkah 1 satu posisi ke kiri

$$C = E_K(P) = (P \oplus K) << 1$$

- D adalah kebalikan (*invers*) dari E. Contoh fungsi D yang sederhana adalah sbb:

1. Geser secara *wrapping* bit-bit ciphertes C satu posisi ke kanan
2. Lalu XOR-kan blok hasil Langkah 1 dengan *K*

$$P = D_K(C) = (C >> 1) \oplus K$$

Contoh: Misalkan plainteks adalah 110111010001000101000101, dibagi menjadi tiga buah blok masing-masing berukuran 8 bit:

11011101	00010001	01000101
P1	P2	P3

Kunci yang digunakan adalah K = 01010110

Enkripsi blok pertama, 11011101, dengan fungsi E sebagai berikut:

1. P1 ⊕ K = 11011101 ⊕ 01010110 = 10001011
2. 10001011 << 1 = 00010111

Jadi, C1 = 00010111. Cara yang sama dilakukan untuk P2 dan P3.

Dekripsi blok cipherteks pertama, 00010111, dengan fungsi D sebagai berikut:

1. 00010111 >> 1 = 10001011
2. 10001011 ⊕ K = 10001011 ⊕ 01010110 = 11011101 = P1

- Lakukan proses yang sama untuk blok P2, P3, dst.

- Tentu saja algoritma enkripsi E dan D di atas sangat lemah karena mudah dipecahkan.

- *Cipher* blok modern membuat E dan D sangat rumit prosesnya sehingga sangat sukar dipecahkan oleh kriptanalis.

- Fungsi E dan D melibatkan sejumlah teknik seperti teknik substitusi, permutasi, pergeseran (*shifting*), kompresi, ekspansi, dsb.

- Setiap blok tidak dienkripsi satu kali, tetapi berulang kali untuk mendapatkan cipherteks yang kuat.

- *Daftar sebagian block cipher yang telah dipublikasikan:*

1. Lucifer
2. DES
3. GOST
4. 3DES (Triple-DES)
5. RC2
6. RC5
7. Blowfish
8. AES
9. IDEA
10. LOKI
11. FEAL
12. CAST-128
13. CRAB
14. SAFER
15. Twofish
16. Serpent
17. RC6
18. Camellia
19. 3-WAY
20. MMB
21. Skipjack
22. TEA
23. XTEA
24. SEED
25. Coconut
26. Cobra
27. MARS
28. BATON
29. CRYPTON
30. LEA, dll

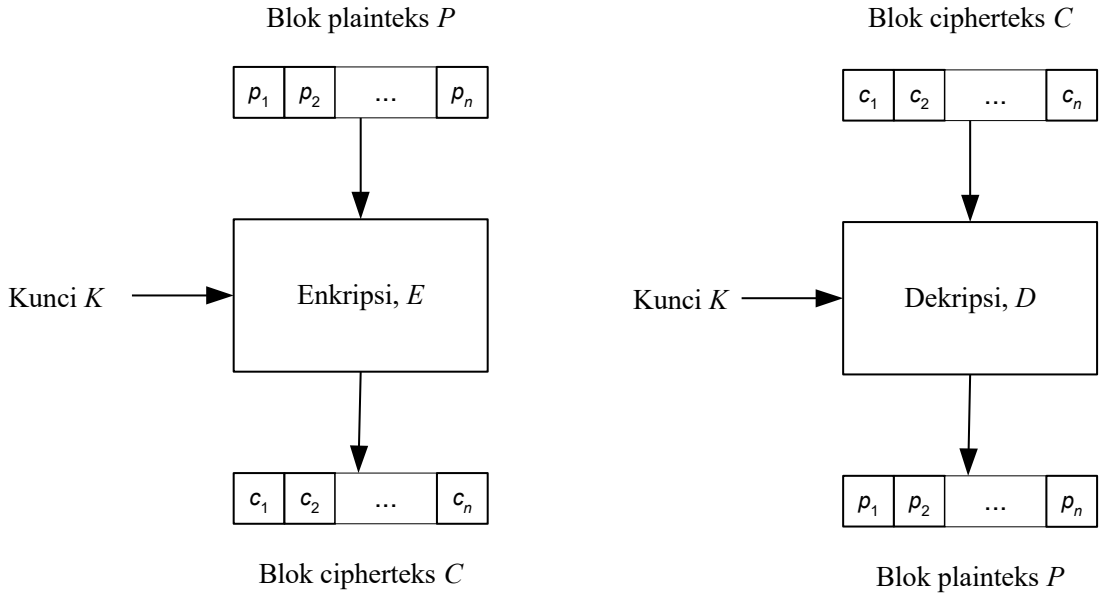
v·t·e	Block ciphers (security summary)
Common algorithms	AES · Blowfish · DES (internal mechanics, Triple DES) · Serpent · Twofish
Less common algorithms	ARIA · Camellia · CAST-128 · GOST · IDEA · LEA · RC2 · RC5 · RC6 · SEED · Skipjack · TEA · XTEA
Other algorithms	3-Way · Akelarre · Anubis · BaseKing · BassOmatic · BATON · BEAR and LION · CAST-256 · Chiasmus · CIKS-1 · CIPHERUNICORN-A · CIPHERUNICORN-E · CLEFIA · CMEA · Cobra · COCONUT98 · Crab · Cryptomeria/C2 · CRYPTON · CS-Cipher · DEAL · DES-X · DFC · E2 · FEAL · FEA-M · FROG · G-DES · Grand Cru · Hasty Pudding cipher · Hierocrypt · ICE · IDEA NXT · Intel Cascade Cipher · Iraqi · Kalyna · KASUMI · KeeLoq · KHAZAD · Khufu and Khafre · KN-Cipher · Kuznyechik · Ladder-DES · LOKI (97, 89/91) · Lucifer · M6 · M8 · MacGuffin · Madryga · MAGENTA · MARS · Mercy · MESH · MISTY1 · MMB · MULTI2 · MultiSwap · New Data Seal · NewDES · Nimbus · NOEKEON · NUSH · PRESENT · Prince · Q · REDOC · Red Pike · S-1 · SAFER · SAVILLE · SC2000 · SHACAL · SHARK · Simon · SM4 · Speck · Spectr-H64 · Square · SXAL/MBAL · Threefish · Treyfer · UES · xmx · XXTEA · Zodiac
Design	Feistel network · Key schedule · Lai–Massey scheme · Product cipher · S-box · P-box · SPN · Confusion and diffusion · Avalanche effect · Block size · Key size · Key whitening (Whitening transformation)
Attack (cryptanalysis)	Brute-force (EFF DES cracker) · MITM (Biclique attack · 3-subset MITM attack) · Linear (Piling-up lemma) · Differential (Impossible · Truncated · Higher-order) · Differential-linear · Distinguishing (Known-key) · Integral/Square · Boomerang · Mod *n* · Related-key · Slide · Rotational · Side-channel (Timing · Power-monitoring · Electromagnetic · Acoustic · Differential-fault) · XSL · Interpolation · Partitioning · Rubber-hose · Black-bag · Davies · Rebound · Weak key · Tau · Chi-square · Time/memory/data tradeoff
Standardization	AES process · CRYPTREC · NESSIE
Utilization	Initialization vector · Mode of operation · Padding
v·t·e	Cryptography [show]

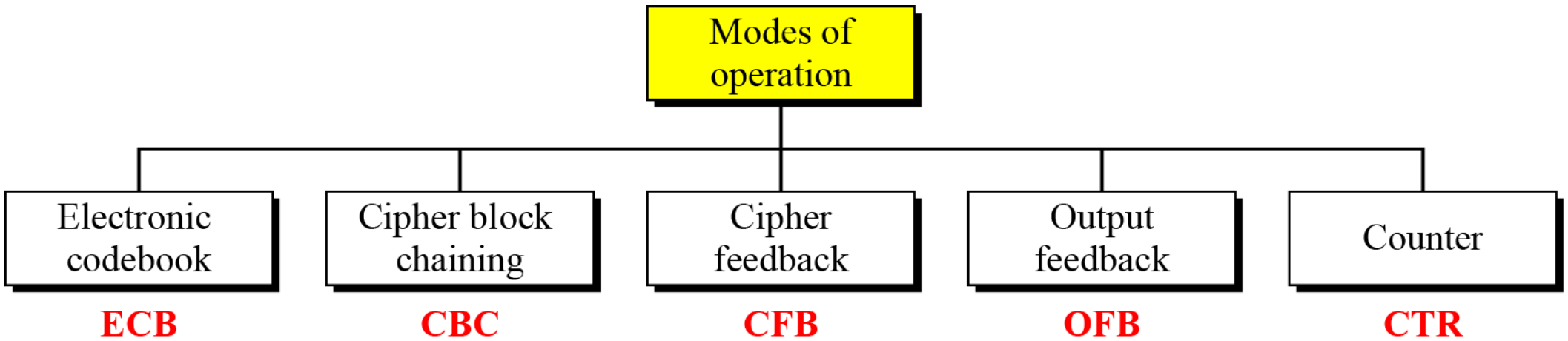
Sumber: https://en.wikipedia.org/wiki/Block_cipher

Mode Operasi *Cipher* Blok

- Mode operasi: berkaitan dengan cara blok pesan dioperasikan sebelum dienkripsi/dekripsi oleh fungsi E dan D.

- Ada 5 mode operasi *cipher* blok:
  1. *Electronic Code Book* (*ECB*)
  2. *Cipher Block Chaining* (*CBC*)
  3. *Cipher Feedback* (*CFB*)
  4. *Output Feedback (OFB)*
  5. *Counter Mode*




Modes of operation
Electronic codebook
Cipher block chaining
Cipher feedback
Output feedback
Counter
ECB
CBC
CFB
OFB
CTR

1. Electronic Code Book (ECB)

- Setiap blok plainteks P_i dienkripsi secara individual dan independen dari blok lainnya menjadi blok cipherteks C_i .

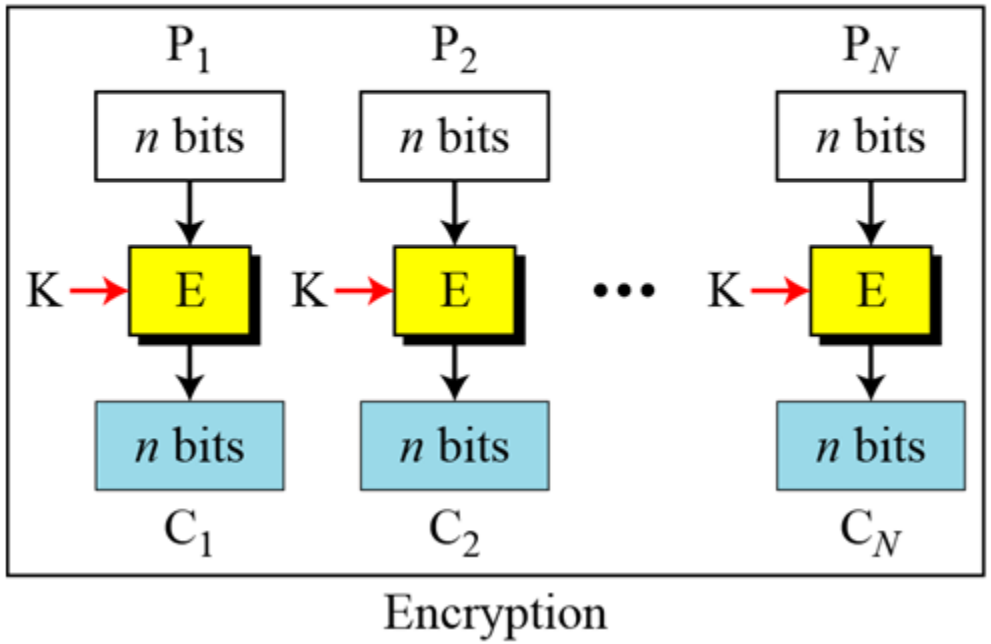
- Enkripsi: $C_i = E_K(P_i)$

  Dekripsi: $P_i = D_K(C_i)$

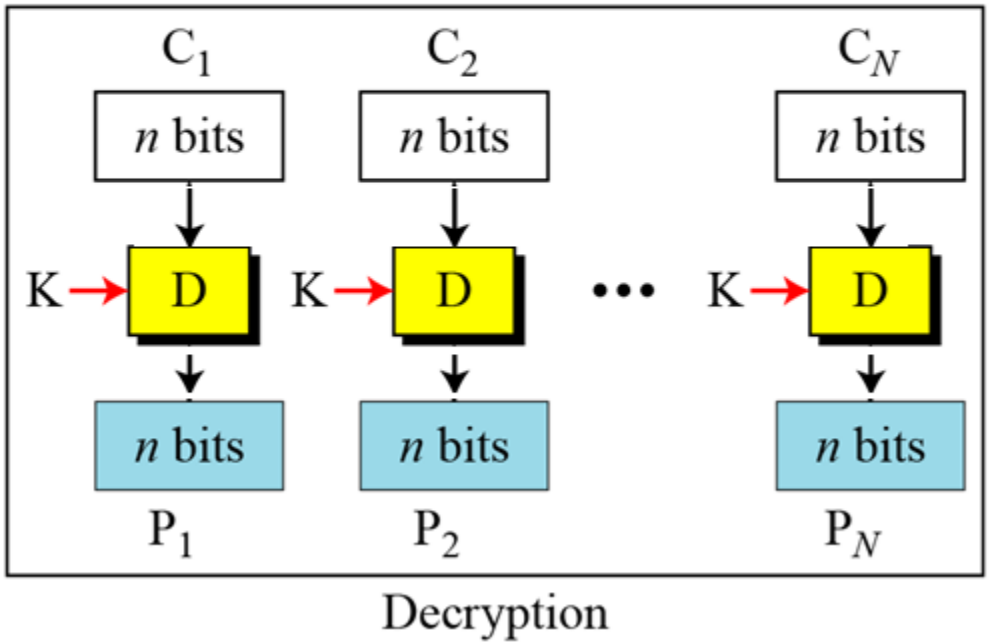
  yang dalam hal ini, P_i dan C_i masing-masing blok plainteks dan cipherteks ke-*i*.

Mode ECB

E: Encryption D: Decryption
P_i: Plaintext block i C_i: Ciphertext block i
K: Secret key



Encryption



Decryption

- Contoh:

  Plainteks: 10100010000111010101001

  Bagi plainteks menjadi blok-blok 4-bit:

  1010 0010 0011 1010 1001

  (dalam notasi HEX :A23A9)

- Kunci (juga 4-bit): 1011

- Misalkan fungsi enkripsi *E* yang sederhana algoritmanya sbb:
  1. XOR-kan blok plainteks P_i dengan *K*
  2. geser secara *wrapping* bit-bit dari hasil langkah 1 satu posisi ke kiri

$$E_K(P) = (P \oplus K) << 1$$

$$E_K(P) = (P \oplus K) << 1$$

Enkripsi:

	1010	0010	0011	1010	1001
	1011	1011	1011	1011	1011 ⊕
Hasil *XOR*:	0001	1001	1000	0001	0010
Geser 1 bit ke kiri:	0010	0011	0001	0010	0100
Dalam notasi HEX:	2	3	1	2	4

Jadi, hasil enkripsi plainteks

`10100010001110101001` (`A23A9` dalam notasi HEX)

adalah

`00100011000100100100` (`23124` dalam notasi HEX)

- Pada mode ECB, blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama.

	1010	0010	0011	1010	1001	
	1011	1011	1011	1011	1011	⊕
Hasil *XOR*:	0001	1001	1000	0001	0010	
Geser 1 bit ke kiri:	0010	0011	0001	0010	0100	
Dalam notasi HEX:	2	3	1	2	4	

- Pada contoh di atas, blok `1010` muncul dua kali dan selalu dienkripsi menjadi `0010`.

- Karena setiap blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama, maka secara teoritis dimungkinkan membuat buku kode plainteks dan cipherteks yang berkoresponden (asal kata "*code book*" di dalam *ECB*). Enkripsi/dekripsi dilakukan dengan *look up table*.

Plainteks	Cipherteks
0000	0100
0001	1001
0010	1010
…	…
1111	1010

- Untuk setiap kunci K yang berbeda, dibuat buku kode yang berbeda pula. Jika panjang kunci n bit, maka terdapat 2^n buku kode.

- Jumlah entri (baris) di dalam setiap buku kode untuk adalah 2^n.

- Namun, semakin besar ukuran blok, semakin besar pula ukuran buku kodenya.

- Misalkan jika blok berukuran 64 bit, maka buku kode terdiri dari 2^{64} buah kode (*entry*), yang berarti terlalu besar untuk disimpan. Lagipula, setiap kunci mempunyai buku kode yang berbeda.

- Jika panjang plainteks tidak habis dibagi dengan ukuran blok, maka blok terakhir berukuran lebih pendek daripada blok-blok lainnya.

- Untuk itu, kita tambahkan bit-bit *padding* untuk menutupi kekurangan bit blok.

- Bit-bit padding misalnya bit 0 semua, atau bit 1 semua, atau bit 0 dan bit 1 berselang-seling.

- Contoh: Ukuran blok 8 bit: 10001101 00101001 10110000

  Blok terakhir hanya 5 bit, ditambah 3 bit *padding* (warna biru)

Kelebihan Mode *ECB*

1. **Karena tiap blok plainteks dienkripsi secara independen, maka kita tidak perlu mengenkripsi pesan secara sekuensial/linier.**

- Kita dapat mengenkripsi 5 blok pertama, kemudian blok-blok di akhir, dan kembali ke blok-blok di tengah dan seterusnya.

- Mode *ECB* cocok untuk mengenkripsi isi arsip (*file*) yang diakses secara acak, misalnya arsip-arsip basisdata.

- Jika basisdata dienkripsi dengan mode *ECB*, maka sembarang *record* dapat dienkripsi secara independen dari *record* lainnya (dengan asumsi setiap *record* terdiri dari sejumlah blok diskrit yang sama banyaknya).

2. **Kesalahan 1 atau lebih bit pada blok cipherteks hanya mempengaruhi cipherteks yang bersangkutan pada proses dekripsi.**

   Blok-blok cipherteks lainnya bila didekripsi tidak terpengaruh oleh kesalahan bit cipherteks tersebut.

Kelemahan Mode ECB

1. **Karena plainteks sering mengandung bagian yang berulang (sehingga terdapat blok-blok plainteks yang sama), maka enkripsinya menghasilkan blok cipherteks yang sama pula**

   ➔ contoh berulang: spasi panjang

   ➔ mudah diserang secara statisitik dengan analisis frekuensi

2. **Pihak lawan dapat memanipulasi cipherteks untuk “membodohi” atau mengelabui penerima pesan.**

Contoh: Seseorang mengirim pesan

“Uang ditransfer lima satu juta rupiah”

Andaikan kriptanalis mengetahui ukuran blok = 2 karakter (16 bit), spasi diabaikan.

Blok-blok cipherteks:

$C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10}, C_{11}, C_{12}, C_{13}, C_{14}, C_{15}, C_{16}$

Misalkan kriptanalis mengethaui posisi pesan yang berkaitan dengan nominal uang, yaitu blok C_8 dan C_9.

Kriptanalis membuang blok cipherteks C_8 dan C_9 :

$C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_{10}, C_{11}, C_{12}, C_{13}, C_{14}, C_{15}, C_{16}$

Penerima pesan mendekripsi cipherteks yang sudah dimanipulasi dengan kunci yang benar menjadi

Uang ditransfer satu juta rupiah

Karena dekripsi menghasilkan pesan yang bermakna, maka penerima menyimpulkan bahwa uang yang dikirim kepadanya sebesar satu juta rupiah.

- Cara mengatasi kelemahan ini: enkripsi tiap blok individual bergantung pada semua blok-blok sebelumnya.

- Prinsip ini mendasari mode *Cipher Block Chaining* (CBC).

Cipher Block Chaining(CBC)

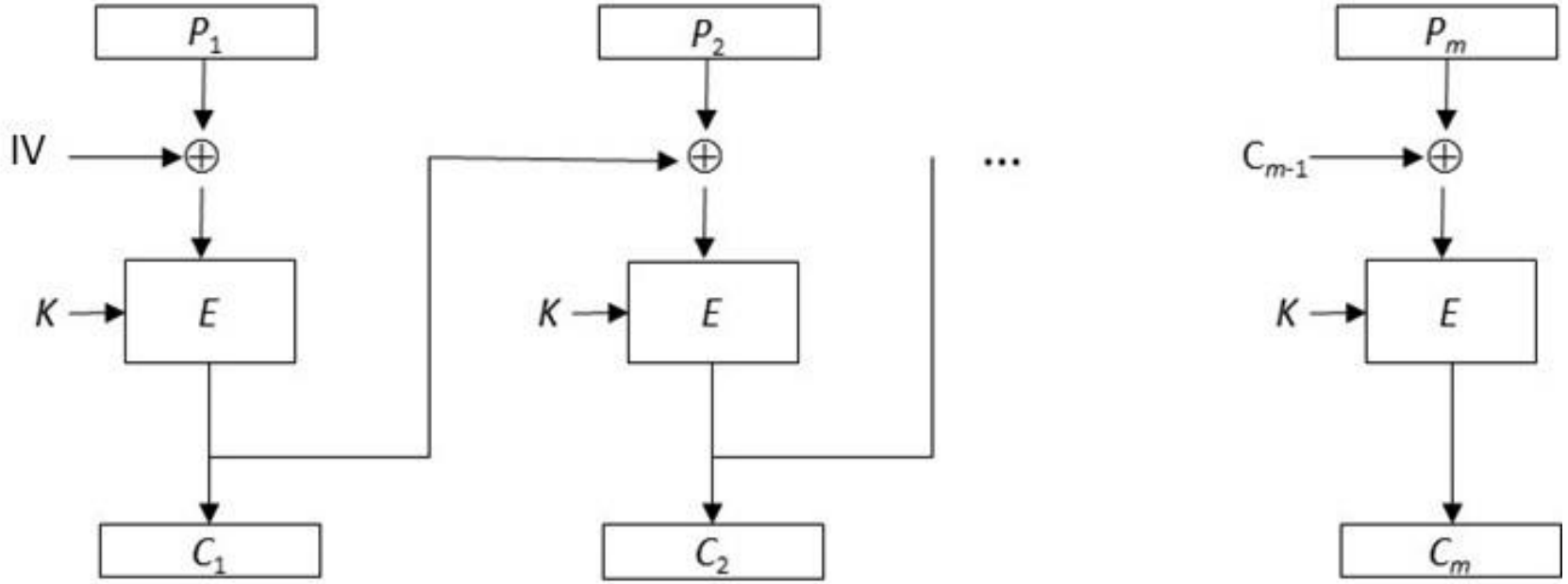
- Tujuan: membuat ketergantungan antar blok (mengatasi kelemahan mode ECB).
- Setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.
- Hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current*.
- Enkripsi blok pertama memerlukan blok semu (C_0) yang disebut *IV* (*initialization vector*).
- *IV* dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh program.
- Pada dekripsi, blok plainteks diperoleh dengan cara meng-*XOR*-kan *IV* dengan hasil dekripsi terhadap blok cipherteks pertama.

(a) Skema enkripsi mode CBC

Encryption:

$C_0 = IV$

$C_i = E_K (P_i \oplus C_{i-1})$

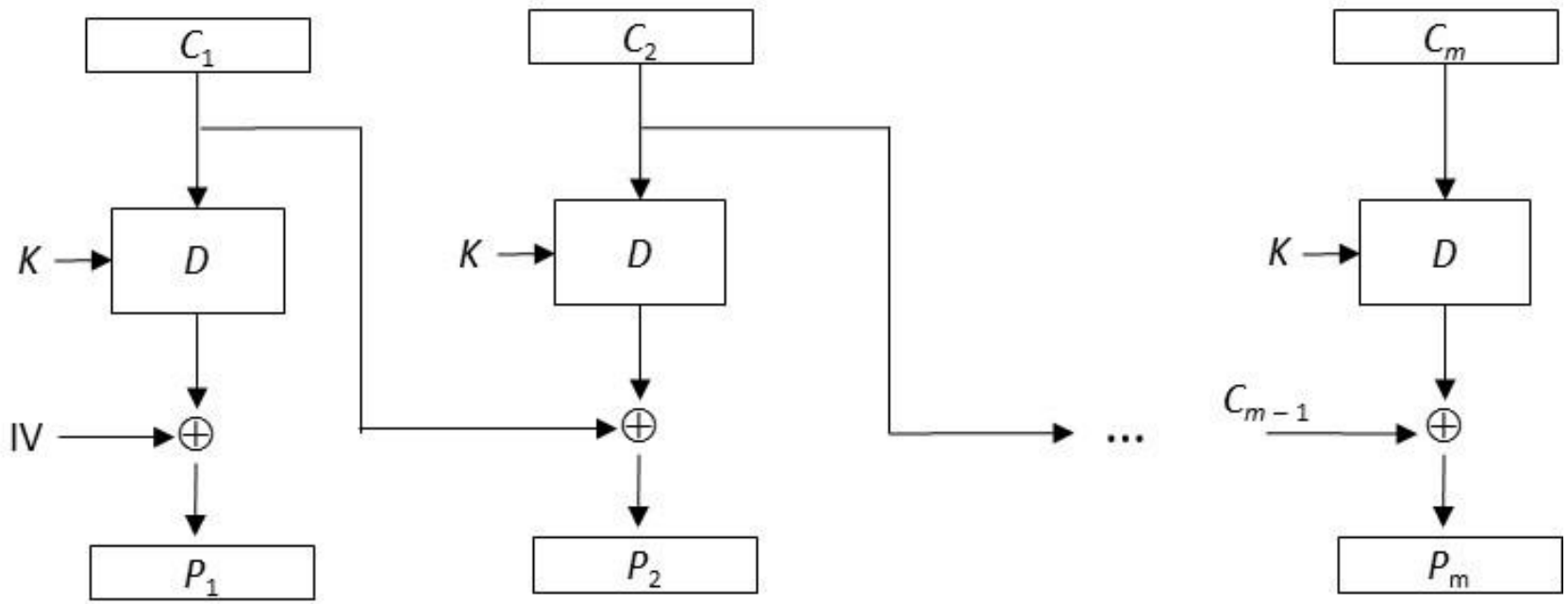


(b) Skema dekripsi mode CBC

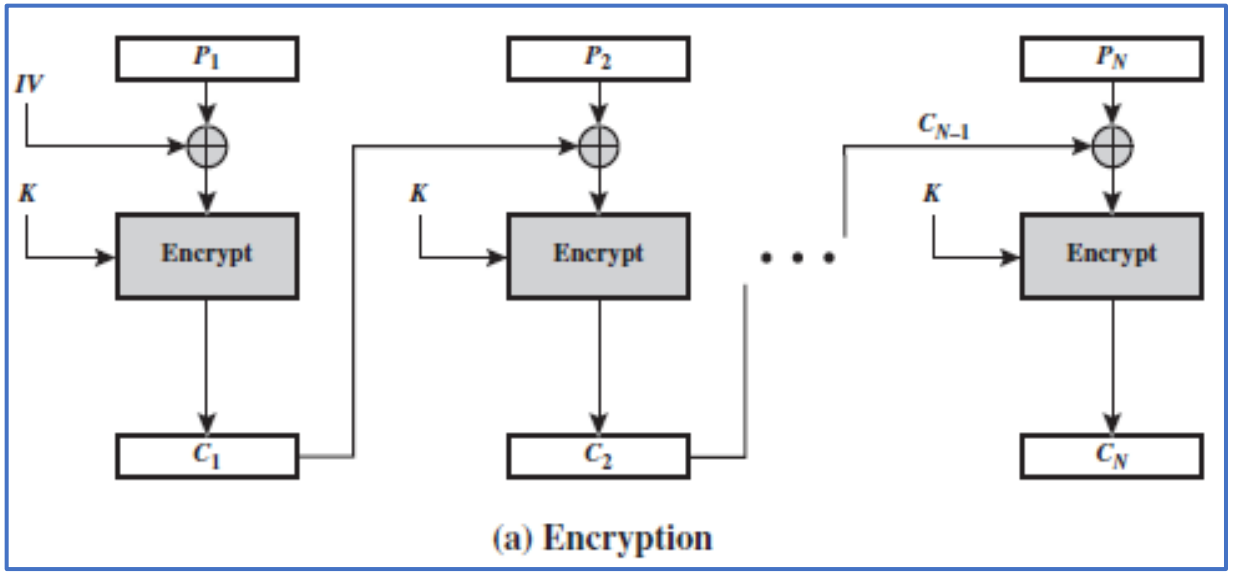
Decryption:

$C_0 = IV$

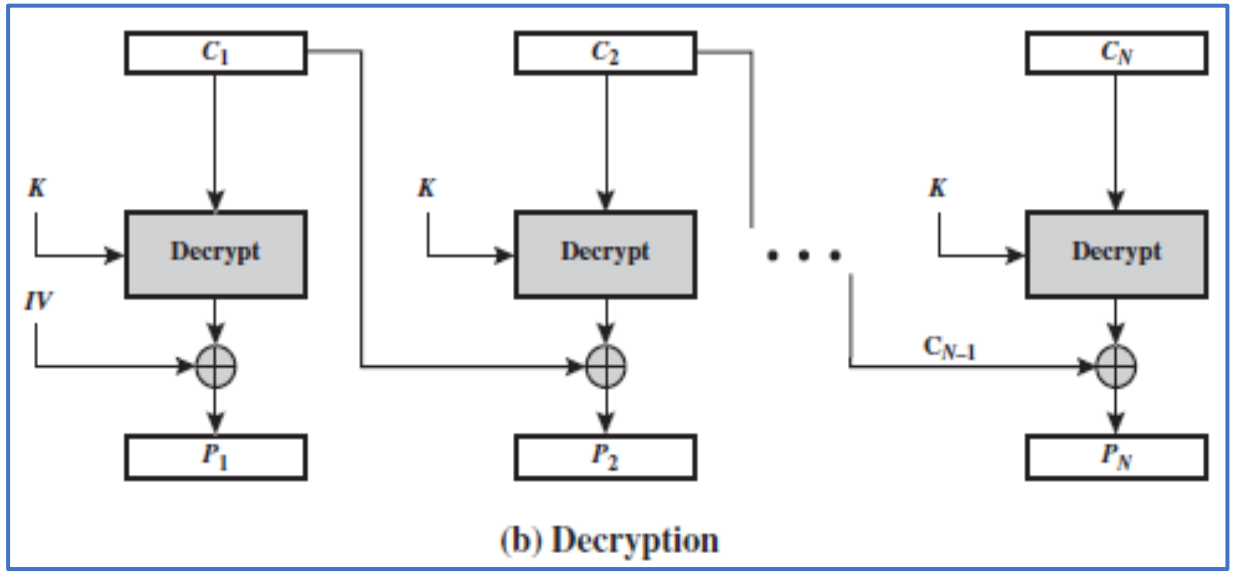
$P_i = D_K (C_i) \oplus C_{i-1}$



Mode CBC



(a) Encryption



(b) Decryption

CBC	$C_1 = \mathrm{E}(K, [P_1 \oplus \mathrm{IV}])$ $C_j = \mathrm{E}(K, [P_j \oplus C_{j-1}])\ j = 2, \ldots, N$	$P_1 = \mathrm{D}(K, C_1) \oplus \mathrm{IV}$ $P_j = \mathrm{D}(K, C_j) \oplus C_{j-1}\ j = 2, \ldots, N$

Contoh 9.8. Tinjau kembali plainteks dari Contoh 9.6:

```
10100010001110101001
```

Bagi plainteks menjadi blok-blok yang berukuran 4 bit:

```
1010   0010   0011   1010   1001
```

atau dalam notasi HEX adalah `A23A9`.

Misalkan kunci (K) yang digunakan adalah (panjangnya juga 4 bit)

```
1011
```

atau dalam notasi HEX adalah `B`. Sedangkan IV yang digunakan seluruhnya bit 0 (Jadi, C_0 = 0000)

Fungsi enkripsi E yang digunakan sama seperti sebelumnya: XOR-kan blok plainteks P_i dengan K, kemudian geser secara *wrapping* bit-bit dari $P_i \oplus K$ satu posisi ke kiri.

$$E_K(P) = (P \oplus K) << 1$$

C_1 diperoleh sebagai berikut:

$P_1 \oplus C_0 = 1010 \oplus 0000 = 1010$

Enkripsikan hasil ini dengan fungsi E sbb:

$1010 \oplus K = 1010 \oplus 1011 = 0001$

Geser (*wrapping*) hasil ini satu bit ke kiri: 0010

Jadi, $C_1 = 0010$ (atau 2 dalam HEX)

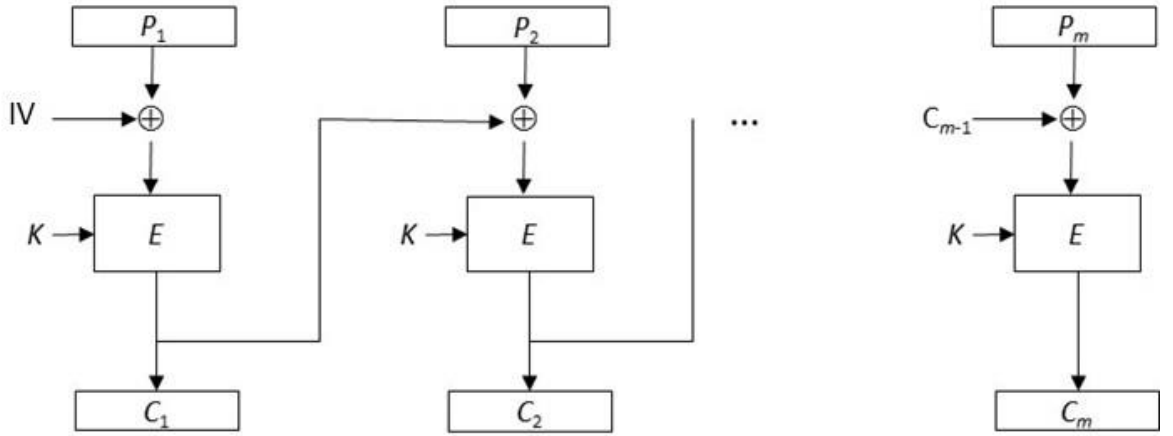
C_2 diperoleh sebagai berikut:

$P_2 \oplus C_1 = 0010 \oplus 0010 = 0000$

$0000 \oplus K = 0000 \oplus 1011 = 1011$

Geser (*wrapping*) hasil ini satu bit ke kiri: 0111

Jadi, $C_2 = 0111$ (atau 7 dalam HEX)



C_3 diperoleh sebagai berikut:

$P_3 \oplus C_2 = 0011 \oplus 0111 = 0100$

$0100 \oplus K = 0100 \oplus 1011 = 1111$

Geser (*wrapping*) hasil ini satu bit ke kiri: 1111

Jadi, $C_3 = 1111$ (atau F dalam HEX)

Demikian seterusnya, sehingga plainteks dan cipherteks hasilnya adalah:

Pesan (plainteks): `A23A9`

Cipherteks (mode *ECB*): `23124`

Cipherteks (mode *CBC*): `27FBF`

Kelebihan Mode CBC

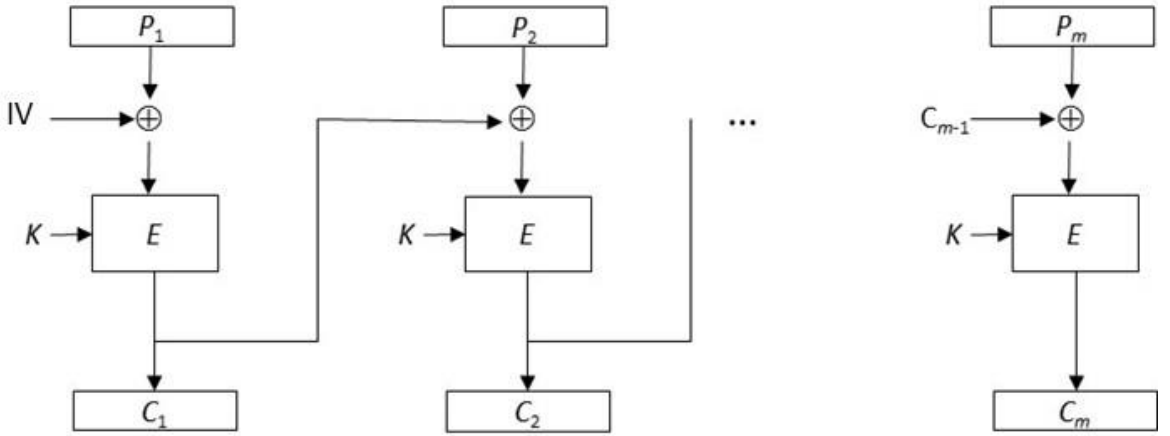
*B*lok-blok plainteks yang sama tidak selalu menghasilkan blok-blok cipherteks yang sama

Oleh karena blok-blok plainteks yang sama tidak menghasilkan blok-blok cipherteks yang sama, maka kriptanalisis menjadi lebih sulit.

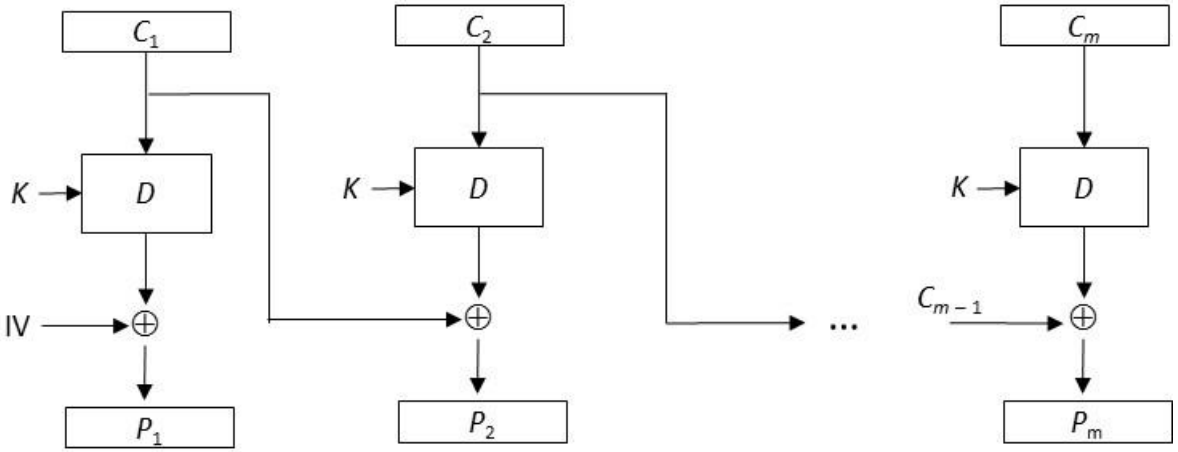
Inilah alasan utama penggunaan mode *CBC*.

Kelemahan Mode CBC

1. Kesalahan satu bit pada sebuah blok plainteks akan menghasilkan kesalahan pada blok cipherteks yang berkoresponden dan kesalahan tersebut merambat ke semua blok cipherteks berikutnya.



2. Tetapi, hal ini berkebalikan pada proses dekripsi. Kesalahan satu bit pada blok cipherteks hanya mempengaruhi blok plainteks yang berkoresponden dan satu bit pada blok plainteks berikutnya (pada posisi bit yang berkoresponden pula).



Cipher-Feedback (CFB)

- Mengatasi kekurangan pada mode *CBC* apabila diterapkan pada pengiriman data yang belum mencapai ukuran satu blok
- Data dienkripsi dalam unit yang lebih kecil (*s*) daripada ukuran blok (*b*).
- Unit data yang dienkripsi panjangnya bisa 1 bit, 2 bit, 4-bit, 8 bit, dan lain-lain.
- Bila unit yang dienkripsi adalah satu karakter setiap kalinya, maka mode *CFB*-nya disebut *CFB* 8-bit.

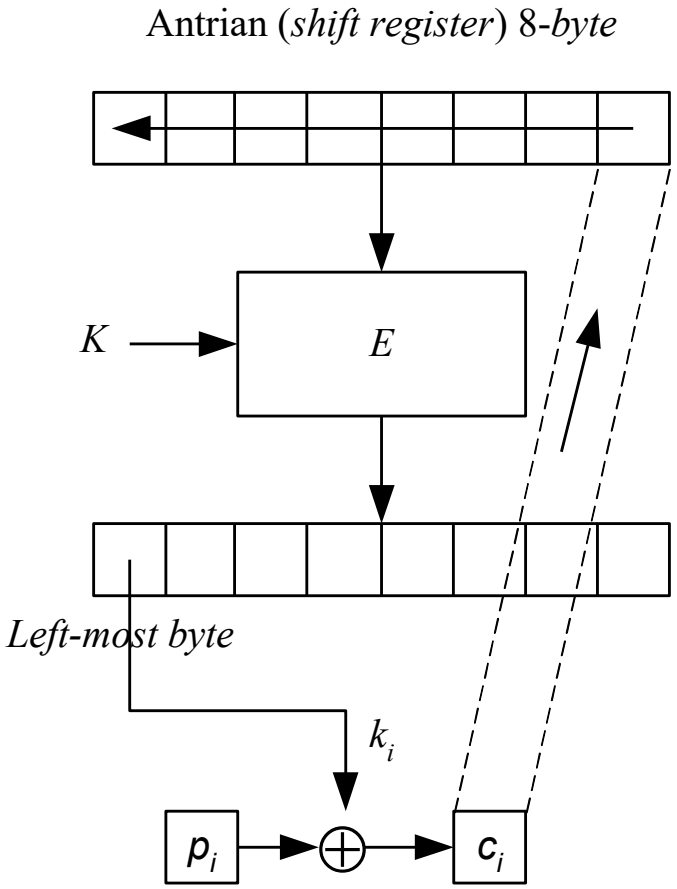
- *CFB* *s*-bit mengenkripsi plainteks berukuran *s* bit setiap kalinya, $s \leq b$ (*b* = ukuran blok dalam satuan bit).

- Dengan kata lain, *CFB* *s*-bit memperlakukan *cipher* blok sama seperti pada *cipher* alir.

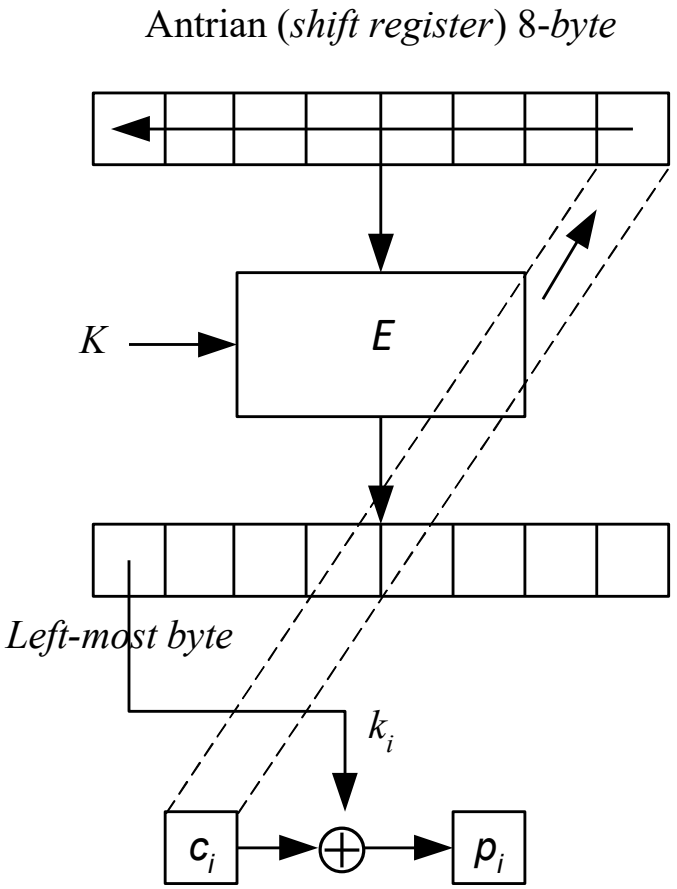
- Mode *CFB* membutuhkan sebuah antrian (*shift register*) yang berukuran sama dengan ukuran blok masukan (*b* bit) .

- Tinjau mode *CFB* 8-bit yang bekerja pada blok berukuran 64-bit pada gambar berikut (*s* = 8, *b* = 64):

Mode CFB-8 bit untuk ukuran blok 64 bit (= 8 byte)



(a) Enkripsi



(b) Dekripsi

Secara matematis, mode *CFB s*-bit dapat dinyatakan sebagai:

Enkripsi:

$C_j = P_j \oplus MSB_s(E_K(X_j))$

$X_{j+1} = LSB_{b-s}(X_j) \,||\, C_i$

Dekripsi:

$P_j = C_i \oplus MSB_s(E_K(X_j))$

$X_{j+1} = LSB_{b-s}(X_j) \,||\, C_i$

yang dalam hal ini,

$j = 1, 2, 3, \ldots, m$.

X_j = antrian bergeser, dengan $X_1 = IV$

E = fungsi enkripsi

K = kunci

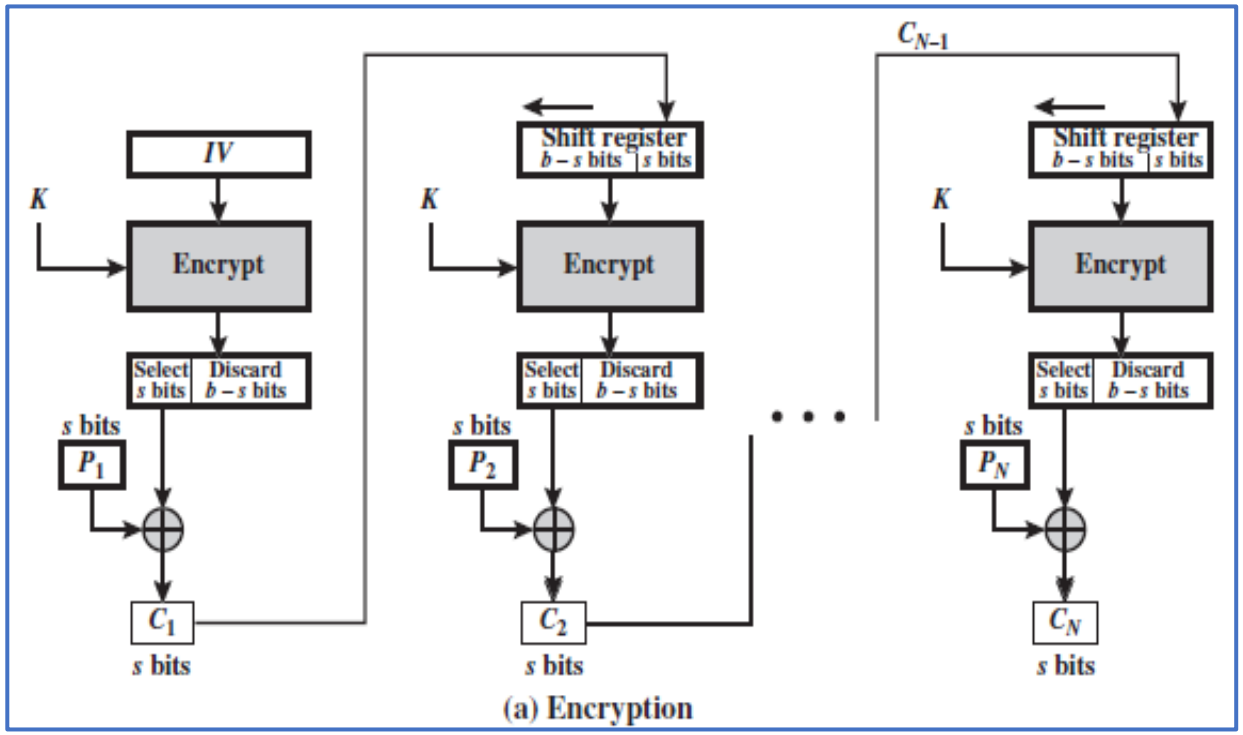
b = panjang blok enkripsi

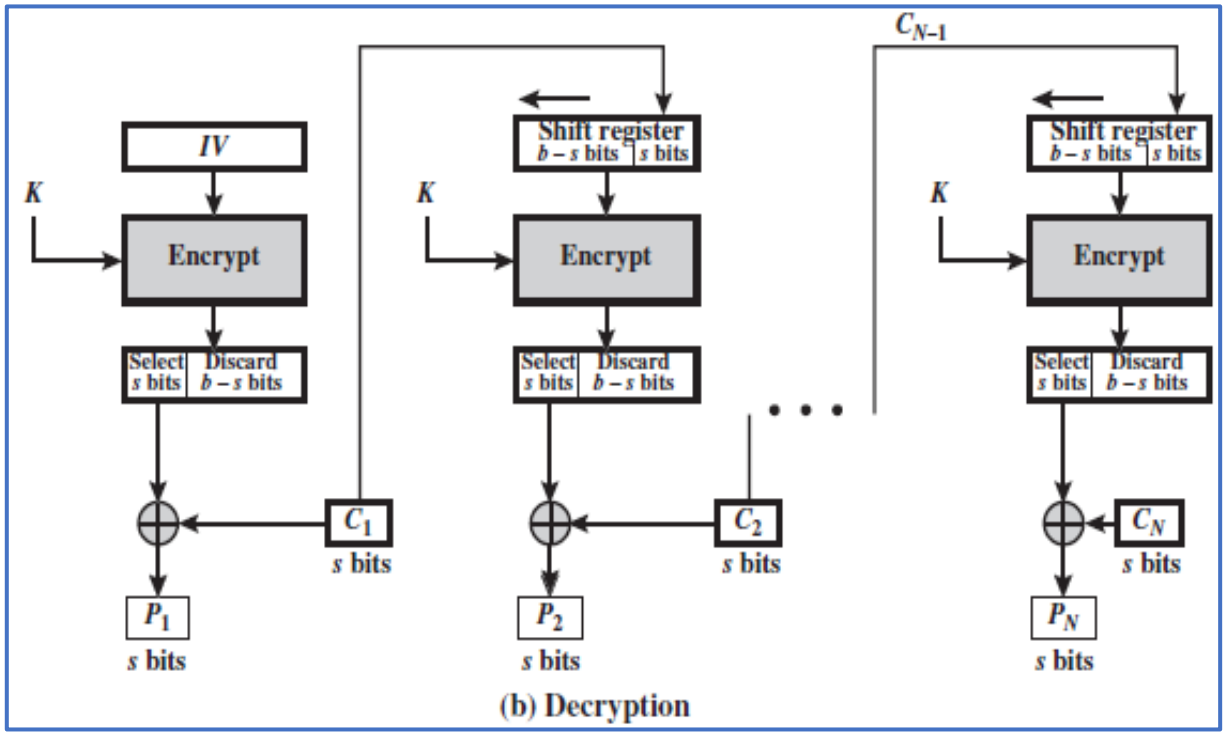
s = panjang unit enkripsi

|| = operator penyambungan (*concatenation*)

MSB = *Most Significant Byte*

Mode CFB





Enkripsi:

$C_j = P_j \oplus MSB_s(E_K(X_j))$

$X_{j+1} = LSB_{b-s}(X_j) \,||\, C_i$

Dekripsi:

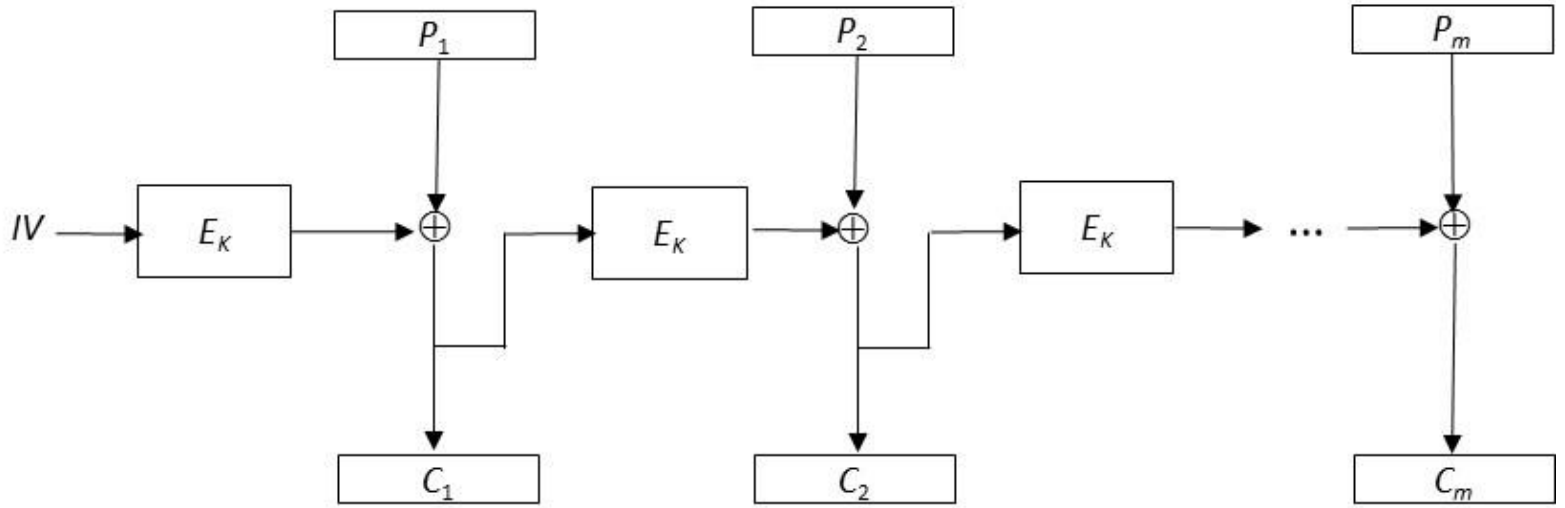
$P_j = C_i \oplus MSB_s(E_K(X_j))$

$X_{j+1} = LSB_{b-s}(X_j) \,||\, C_i$

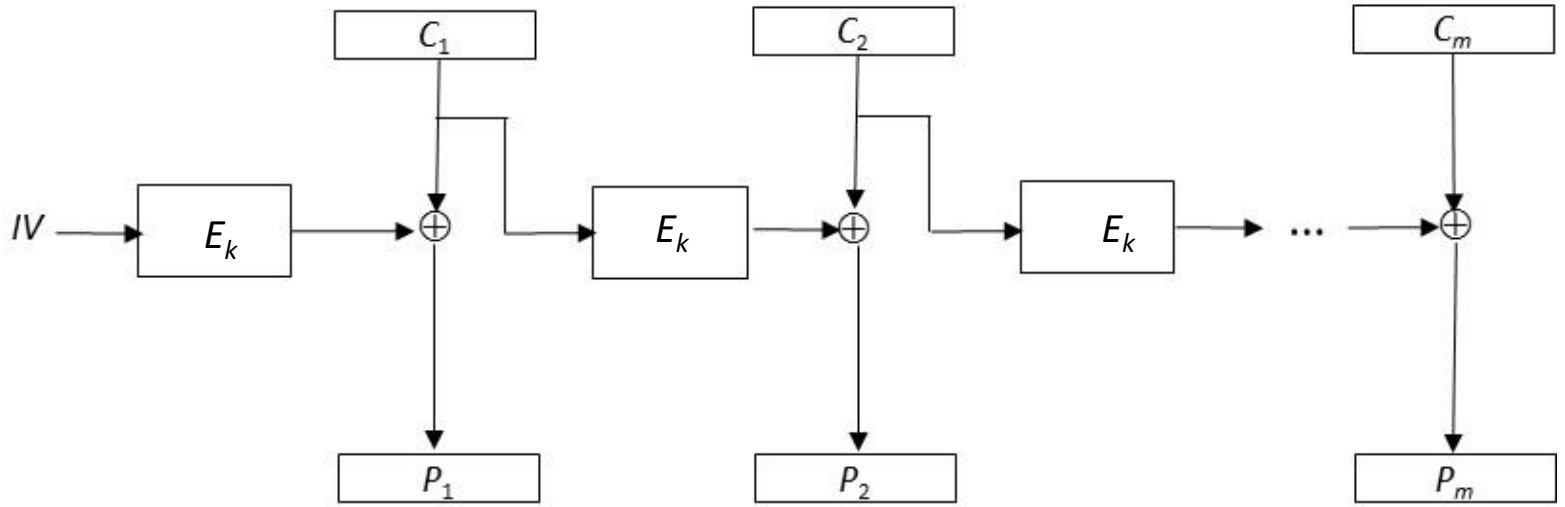
Mode CFB mengoperasikan *block cipher* seperti *stream cipher*!!

- Jika *b* = *s*, maka mode *CFB b*-bit adalah sbb:

(a) Enkripsi



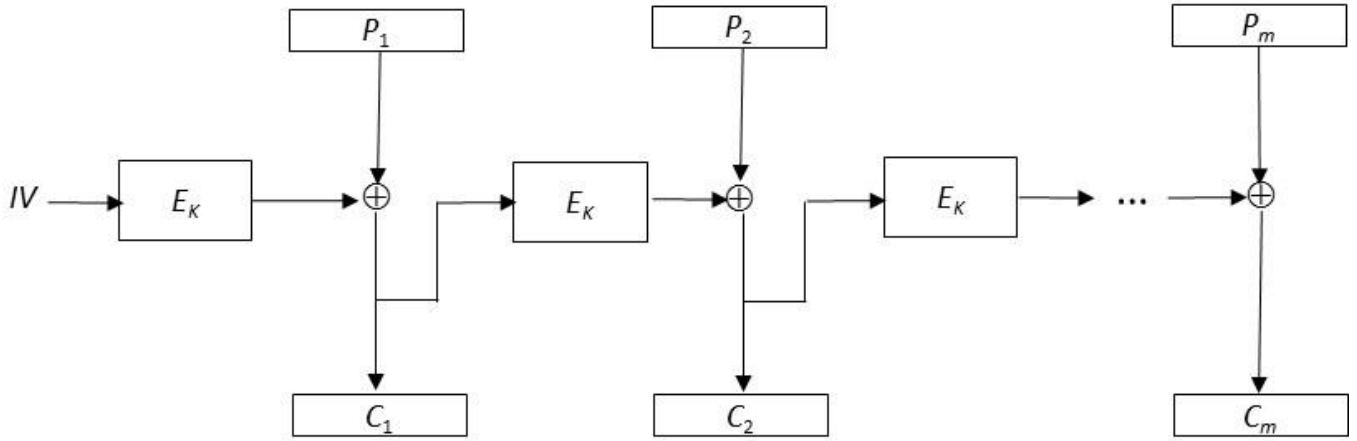
(b) Dekripsi



- Dari Gambar tersebut dapat dilihat bahwa:

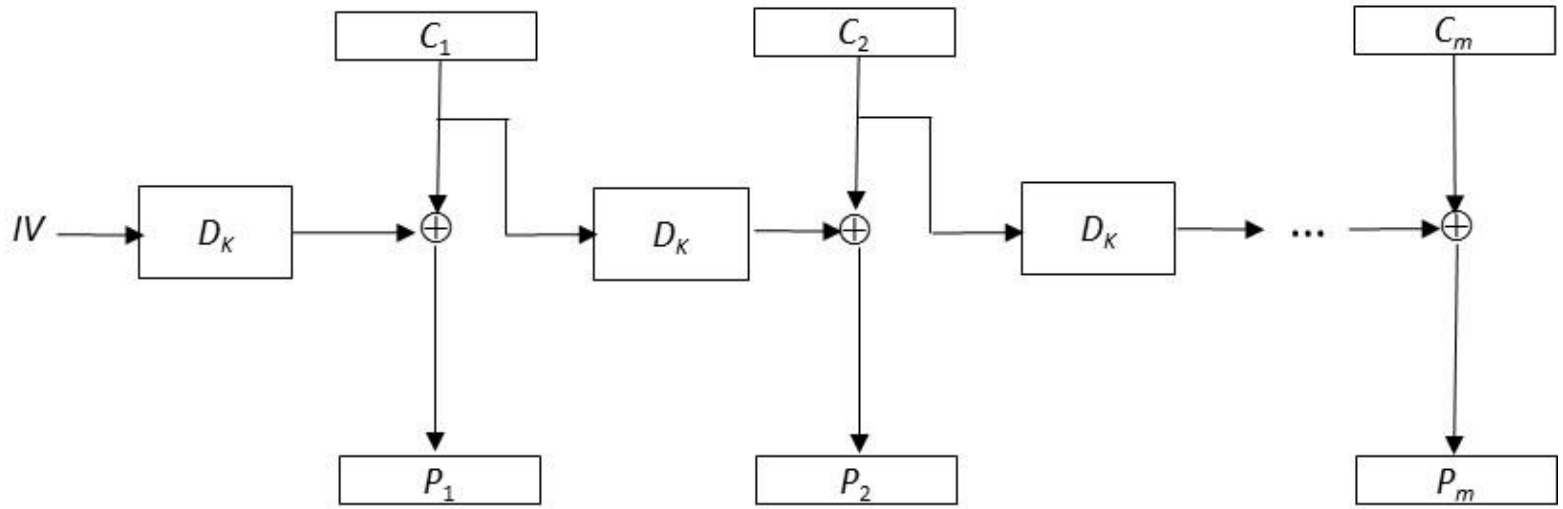
$$C_i = P_i \oplus E_k (C_{i-1})$$
$$P_i = C_i \oplus D_k (C_{i-1})$$

yang dalam hal ini, $C_0 = IV$.



(a) Enkripsi

- Kesalahan 1-bit pada suatu blok plainteks tertentu akan merambat pada blok cipherteks yang berkoresponden dan blok-blok cipherteks selanjutnya pada proses enkripsi.

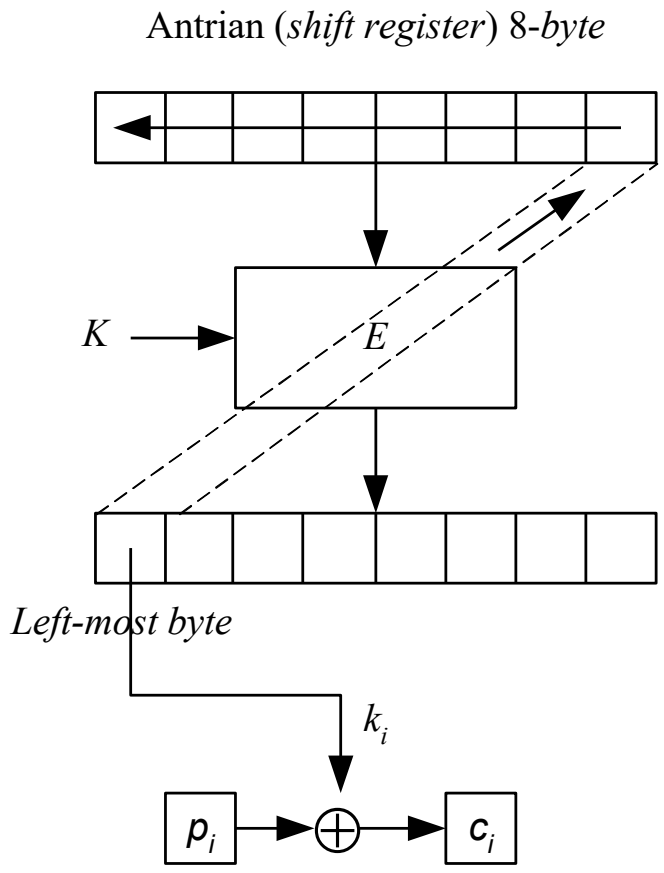


(b) Dekripsi

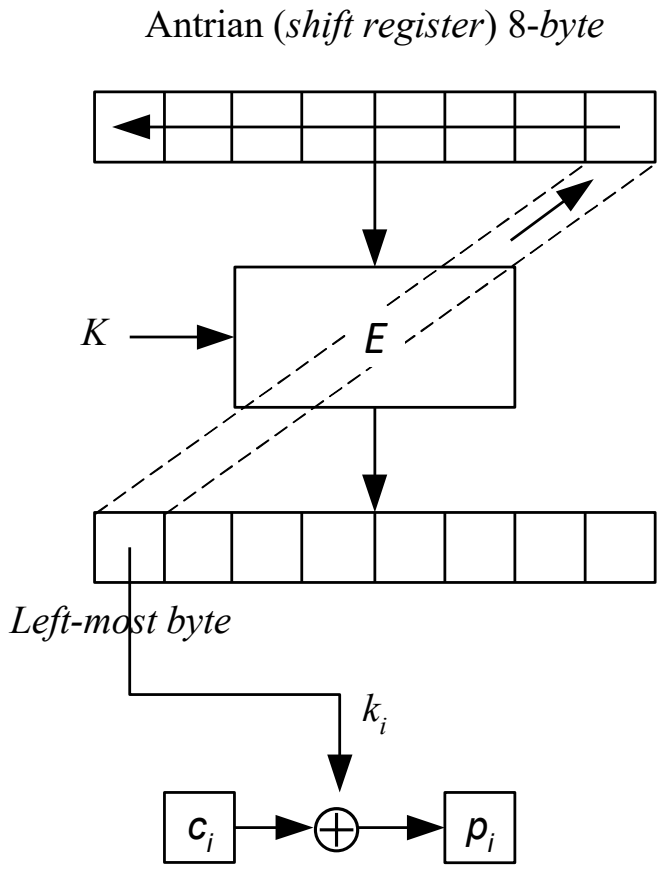
Hal yang kebalikan terjadi pada proses dekripsi. Kesalahan 1 bit pada suatu blok cipherteks tertentu hanya menghasilkan kesalahan dekripsi pada blok plainteks yang bersangkutan dan satu blok plainteks berikutnya.

Output-Feedback (OFB)

- Mode *OFB* mirip dengan mode *CFB*, kecuali *s*-bit dari hasil enkripsi antrian disalin menjadi elemen posisi paling kanan di antrian.

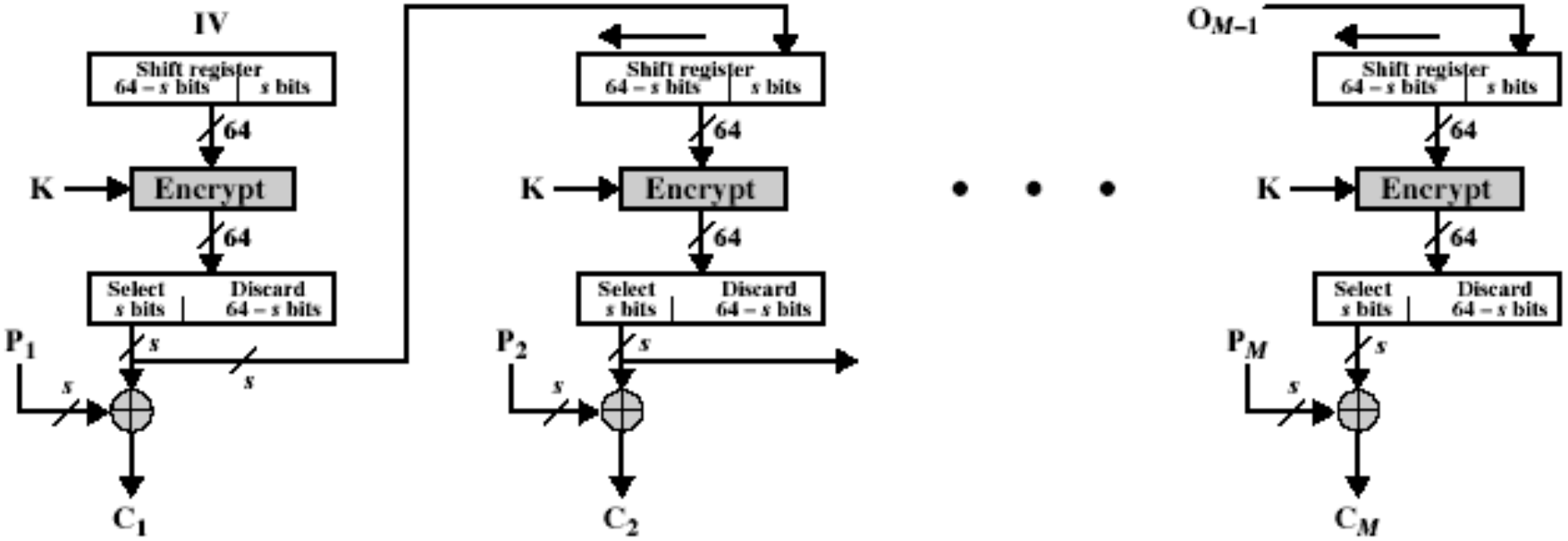


(a) Enkripsi

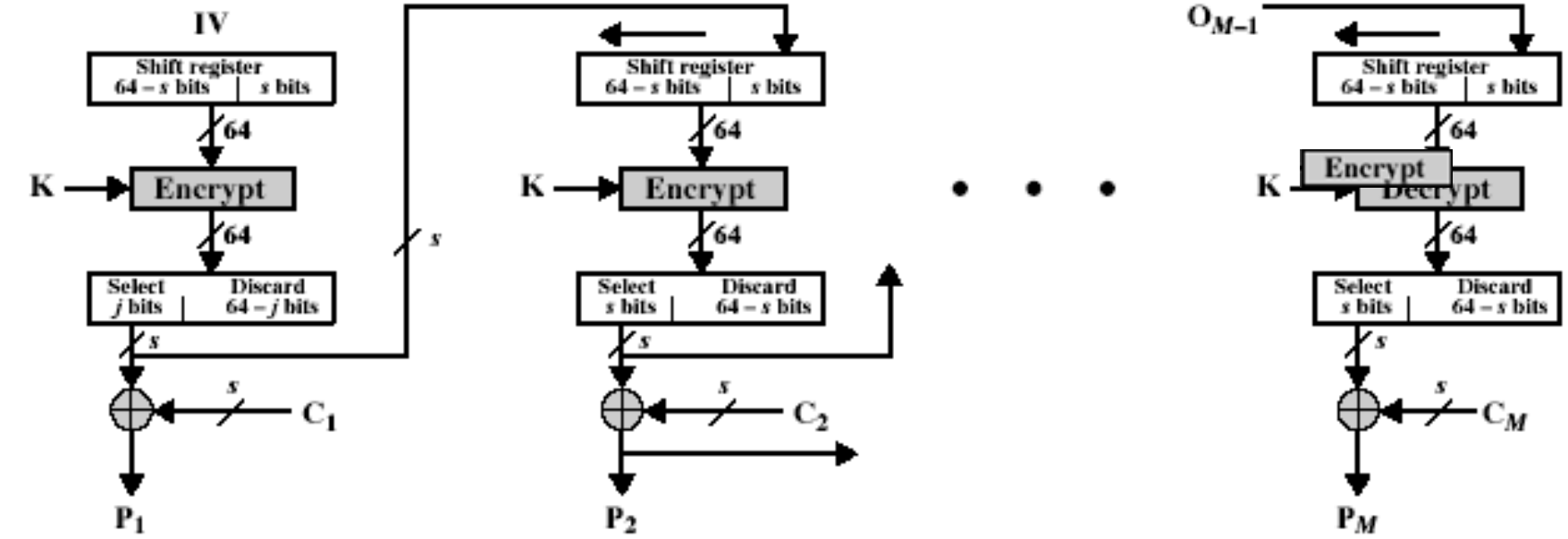


(b) Dekripsi

OFB 8-bit

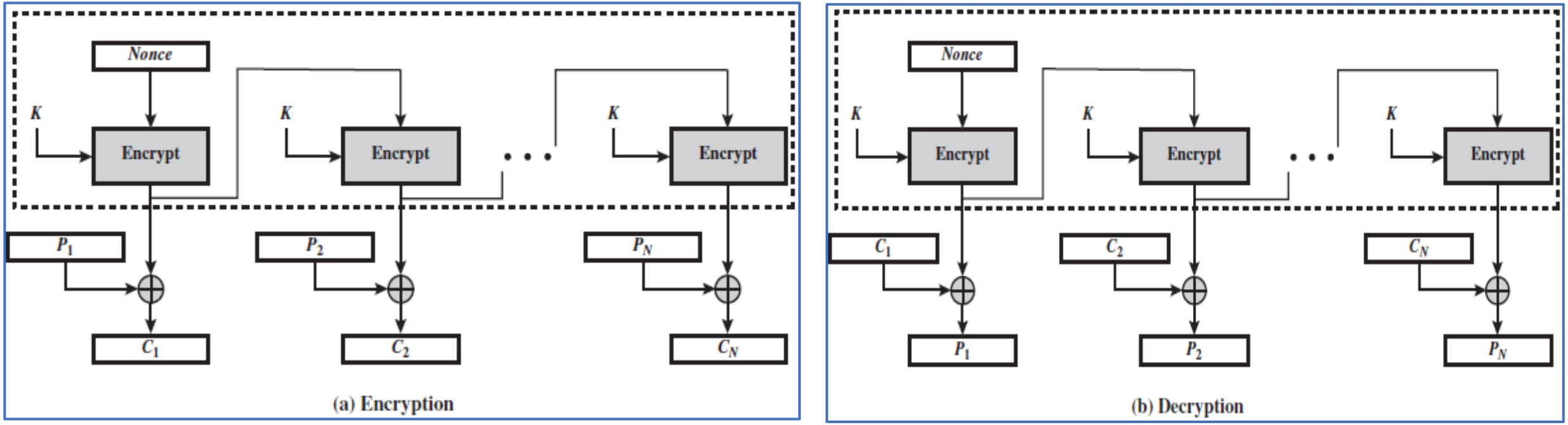


(a) Encryption

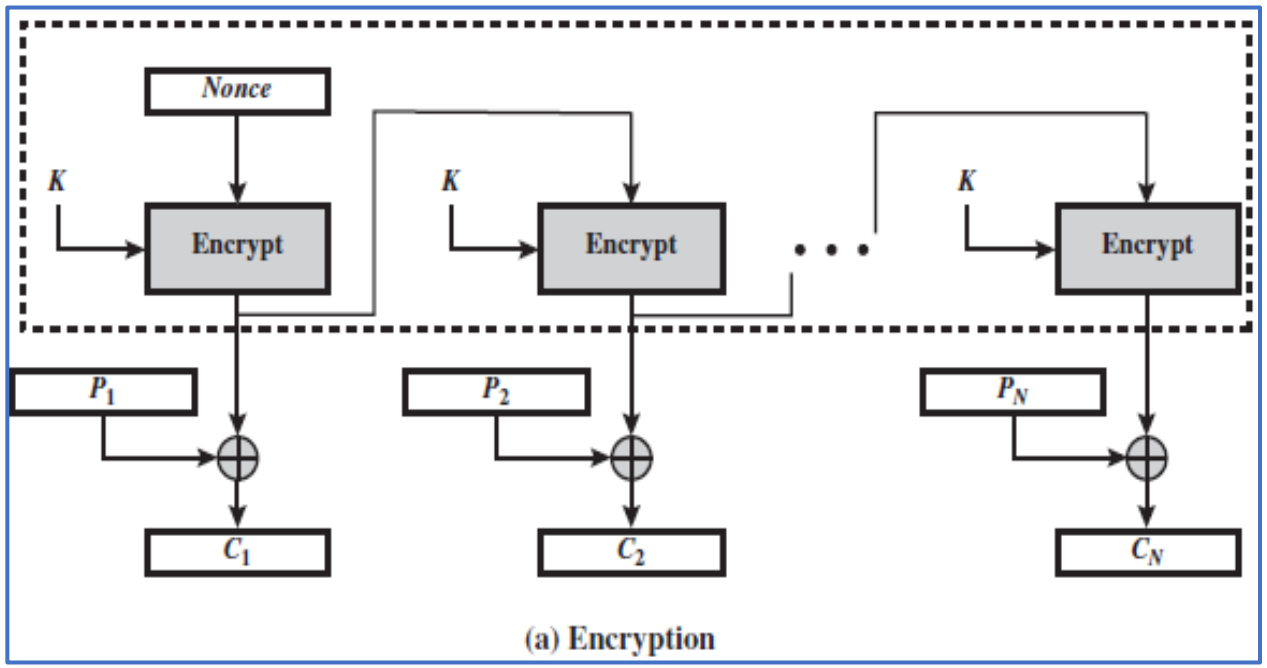


(b) Decryption

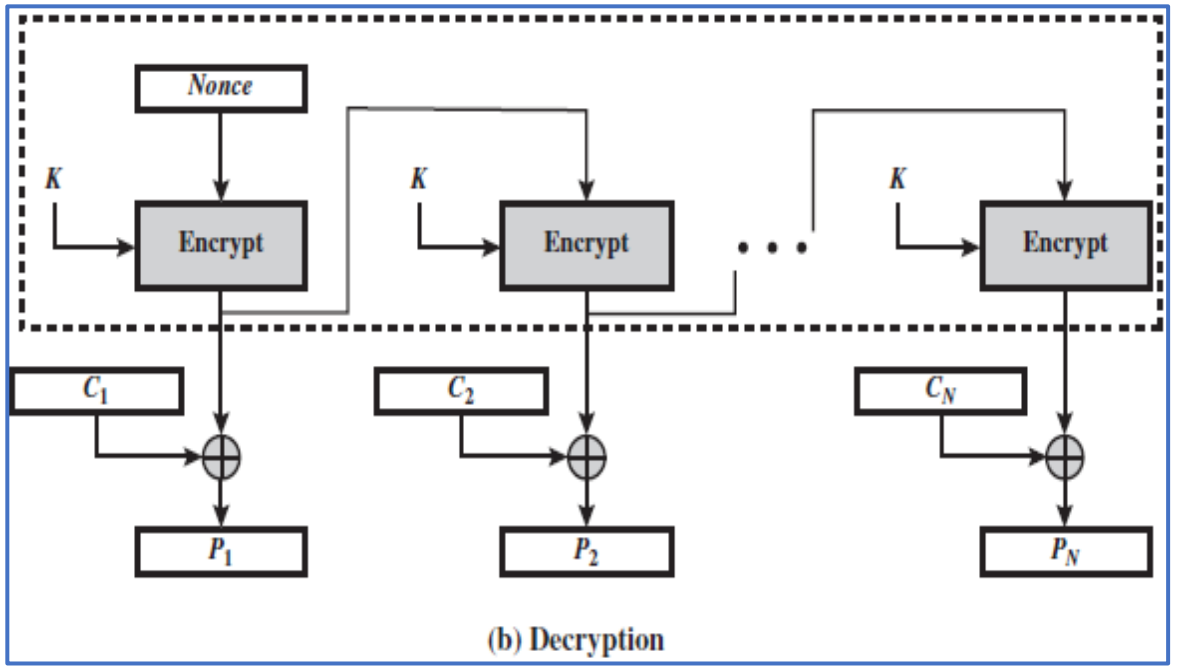
Jika $s = b$, maka mode *OFB* s-bit adalah seperti pada Gambar berikut



- Kesalahan 1-bit pada blok plainteks hanya mempengaruhi blok cipherteks yang berkoresponden saja; begitu pula pada proses dekripsi, kesalahan 1-bit pada blok cipherteks hanya mempengaruhi blok plainteks yang bersangkutan saja.



(a) Encryption



(b) Decryption

- Karakteristik kesalahan semacam ini cocok untuk transmisi analog yang di-digitisasi, seperti suara atau video, yang dalam hal ini kesalahan 1-bit dapat ditolerir, tetapi penjalaran kesalahan tidak dibolehkan.

Counter Mode

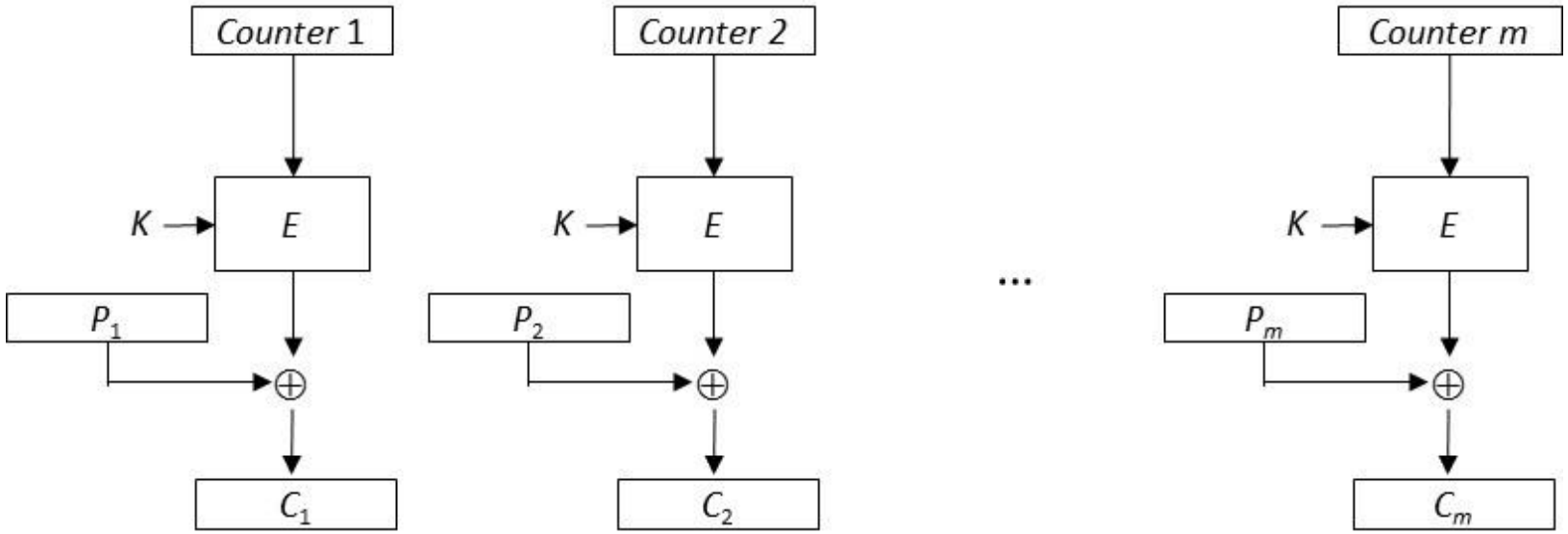
- Mode *counter* tidak melakukan perantaian (*chaining*) seperti pada *CBC*.

- *Counter* adalah sebuah nilai berupa blok bit yang ukurannya sama dengan ukuran blok plainteks.

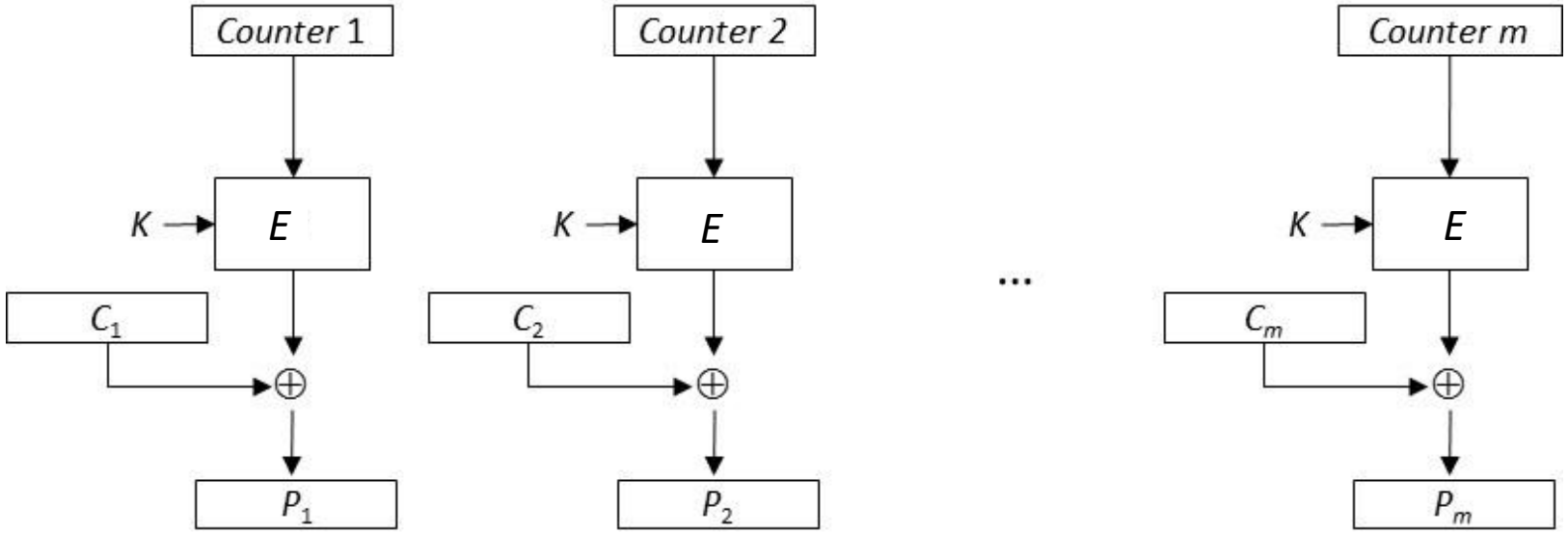
- Nilai *counter* harus berbeda dari setiap blok yang dienkripsi. Pada mulanya, untuk enkripsi blok pertama, *counter* diinisialisasi dengan sebuah nilai.

- Selanjutnya, untuk enkripsi blok-blok berikutnya *counter* dinaikkan (*increment*) nilainya satu (counter $\leftarrow$ counter + 1).

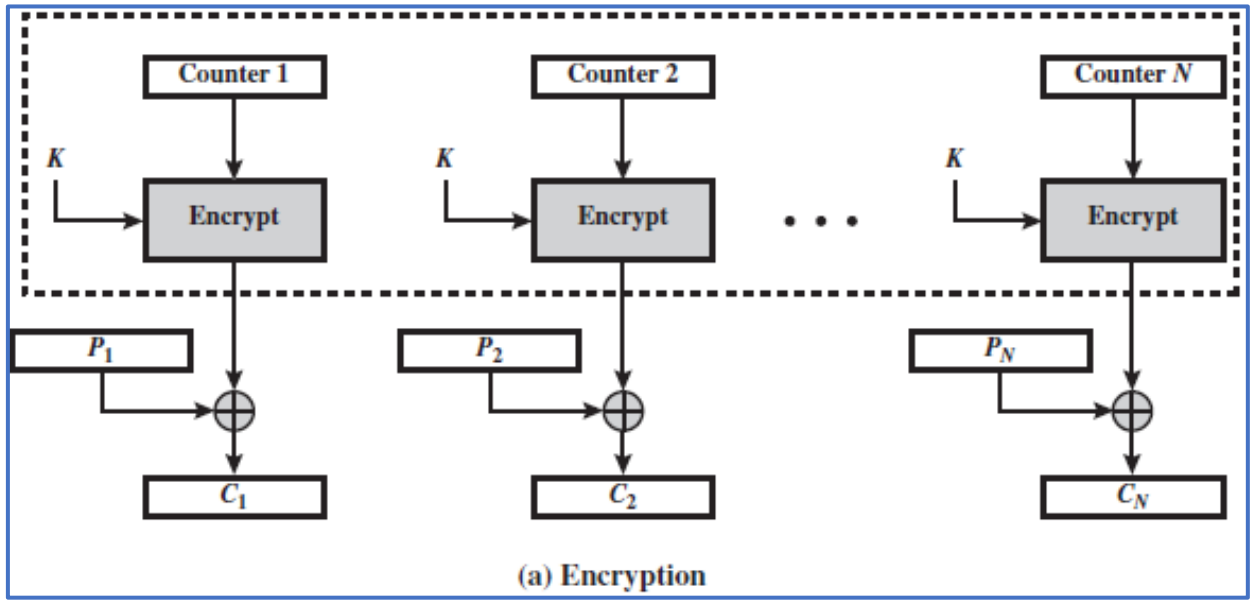
(a) Enkripsi



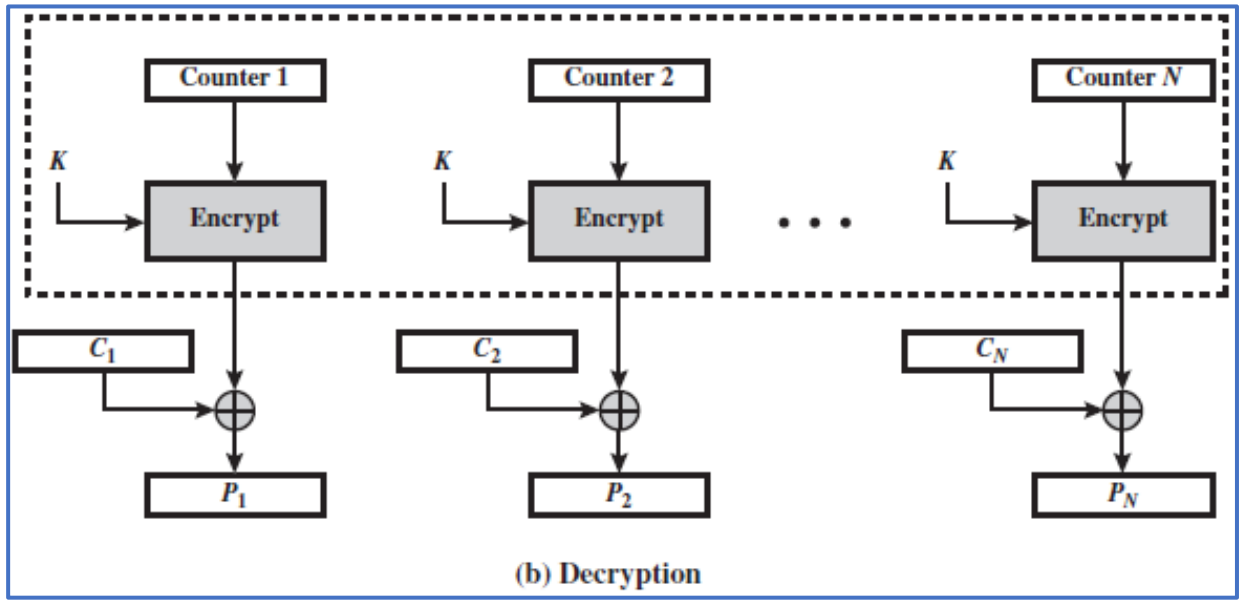
(b) Dekripsi



Mode Counter



(a) Encryption



(b) Decryption

CTR	$C_j = P_j \oplus \mathrm{E}(K, T_j) \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$	$P_j = C_j \oplus \mathrm{E}(K, T_j) \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$

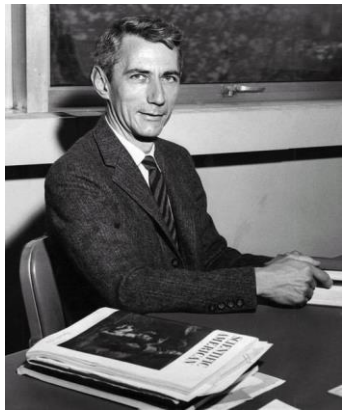
T_j adalah counter, nilainya bertambah satu untuk enkripsi blok berikutnya

- Kelebihan:
  - Hanya perlu algoritma enkripsi saja
  - Dapat mengenkripsi blok data secara acak (tidak harus sekuensial)
    - Blok plainteks/cipherteks dapat diproses(enkripsi atau dekrpsi) secara paralel
  - Sederhana, enkripsi dan dekripsi cepat

- Counter haruslah:
  - Tidak diketahui atau tidak dapat diprediksi nilainya

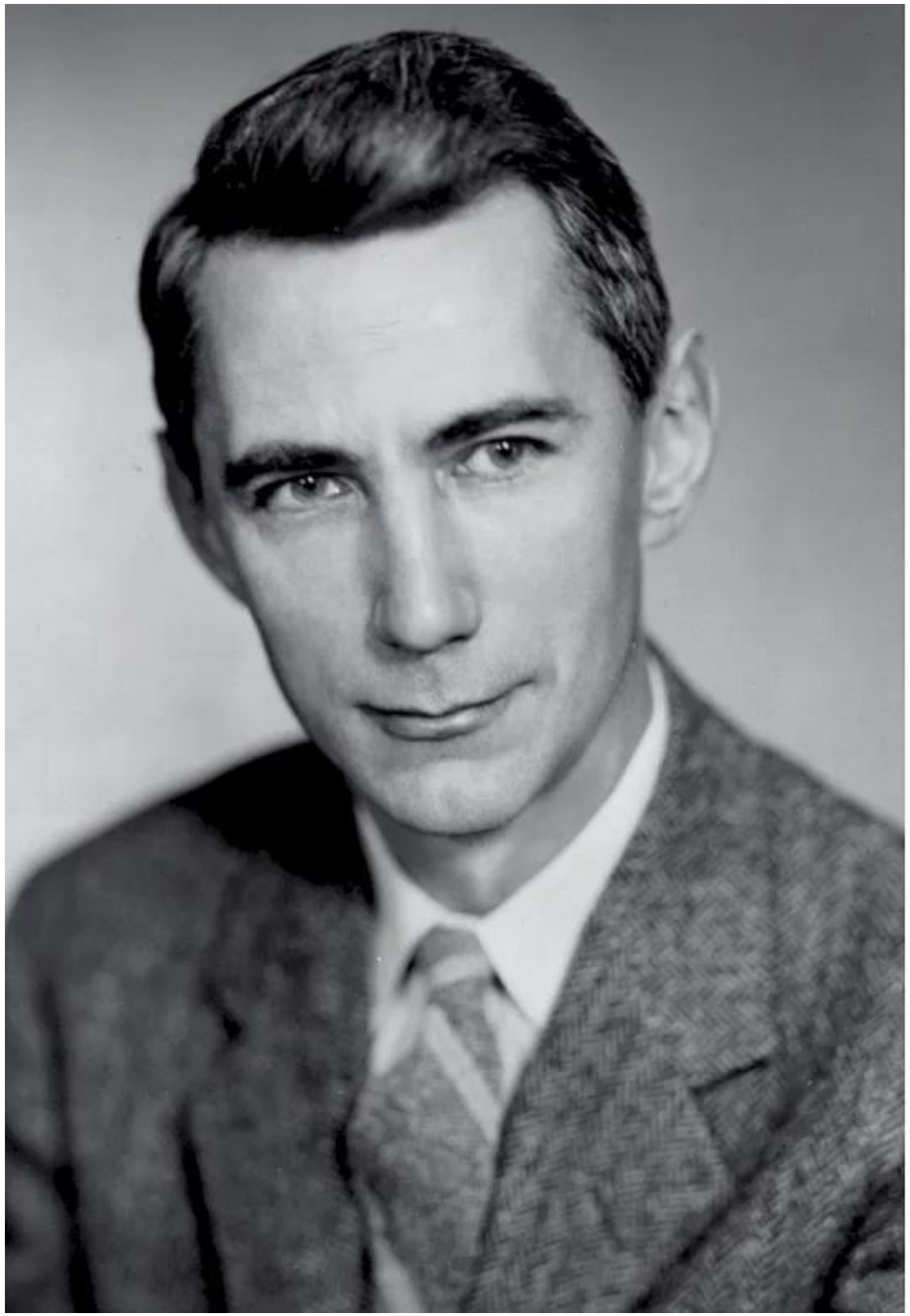
Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Prinsip *Confusion* dan *Diffusion*



- Claude Shannon dalam makalah klasiknya tahun 1949, *Communication theory of secrecy systems*, memperkenalkan prinsip *confusion* dan *diffusion* untuk membuat serangan berbasis statistik terhadap *cipher* menjadi lebih sulit dilakukan.

- Dua prinsip tersebut, *confusion* dan *diffusion*, menjadi panduan dalam merancang algoritma kriptografi, baik *stream cipher* maupun *block cipher*.



Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. Introduction and Summary

THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment systems are primarily a psychological problem, and privacy systems a technological one.

Secondly, the treatment is limited to the case of discrete information, where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.

The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to

* The material in this paper appeared originally in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1945, which has now been declassified.

[1] Shannon, C. E., "A Mathematical Theory of Communication," *Bell System Technical Journal*, July 1948, p. 379; Oct. 1948, p. 623.

[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

1. Confusion

- Prinsip ini menyembunyikan hubungan statistik yang ada diantara plainteks, cipherteks, dan kunci.

- Prinsip *confusion* membuat kriptanalis frustasi untuk mencari pola-pola statistik yang muncul di dalam cipherteks.

- *Confusion* dapat direalisasikan dengan menggunakan teknik substitusi yang nirlanjar (*non-linear*), biasanya dengan operasi *lookup table*.

Contoh substitusi di dalam *block cipher* DES:

- Misalkan 6-bit masukan adalah 110100

  Substitusi 6-bit masukan dengan menggunakan tabel substitusi (*S-Box*).
  Caranya: Nomor baris tabel (bit ke-1 dan bit ke-6) = 10 (baris 2)

  Nomor kolom tabel (bit ke-2, 3, 4, dan 5) = 1010 (kolom 10)

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

  Jadi, substitusi untuk 110100 adalah *entry* pada baris 2 dan kolom 10, yaitu entri bernillai 4 atau 0100 dalam biner.

Contoh substitusi di dalam *block cipher* AES:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	**26**	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Input: 23 (Hexadecimal)
Output: 26 (Hexadecimal)

Cara substitusi;
- Cari perpotongan baris 2 dengan kolom 3
- hasilnya adalah 26

2. Diffusion

- Prinsip ini menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin bit-bit cipherteks.

  Contoh: satu huruf plainteks mempengaruhi nilai banyak huruf cipherteks

- Sebagai efek difusi, maka pengubahan kecil pada plainteks sebanyak satu atau dua bit menghasilkan perubahan pada bit-bit cipherteks yang tidak dapat diprediksi.

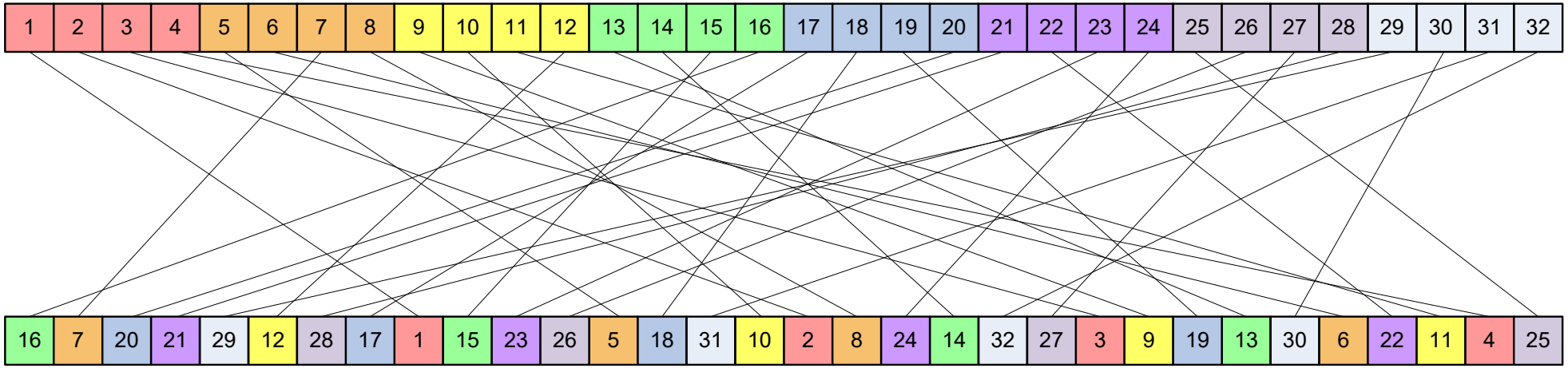
- Contoh: mengenkripsi plainteks 111111111111111

  menghasilkan cipherteks 011011000010100 1.

  Misalkan 1 bit pertama plainteks diubah menjadi **0**111111111111111. Jika difusi bekerja, maka cipherteksnya berubah signifikan menjadi 101100101110111 1

- *Diffusion* did alam block cipher dapat direalisasikan dengan menggunakan teknik permutasi atau transposisi secara berulang-ulang. Permutasi adalah mengacak susunan bit atau *byte* di dalam plainteks.

- Permutasi adalah teknik untuk mengacak susunan bit di dalam sebuah blok bit menghasilkan susunan baru.



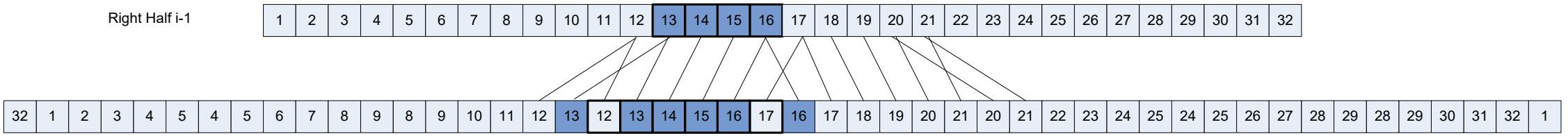
- Pada gambar di atas, posisi bit-bit di dalam blok input 32-bit dipermutasi menjadi susunan baru.

- Di dalam beberapa *cipher* blok, permutasi direalisasikan dengan menggunakan matriks permutasi yang dinamakan *P-box*. Entri di dalam *P-box* menyatakan bit dari posisi sebelumnya.
- Contoh P-box di dalam DES:

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Artinya, bit ke 58 dari bit-bit input dipindahkan ke posisi pertama, bit ke-50 pada posisi kedua, dst

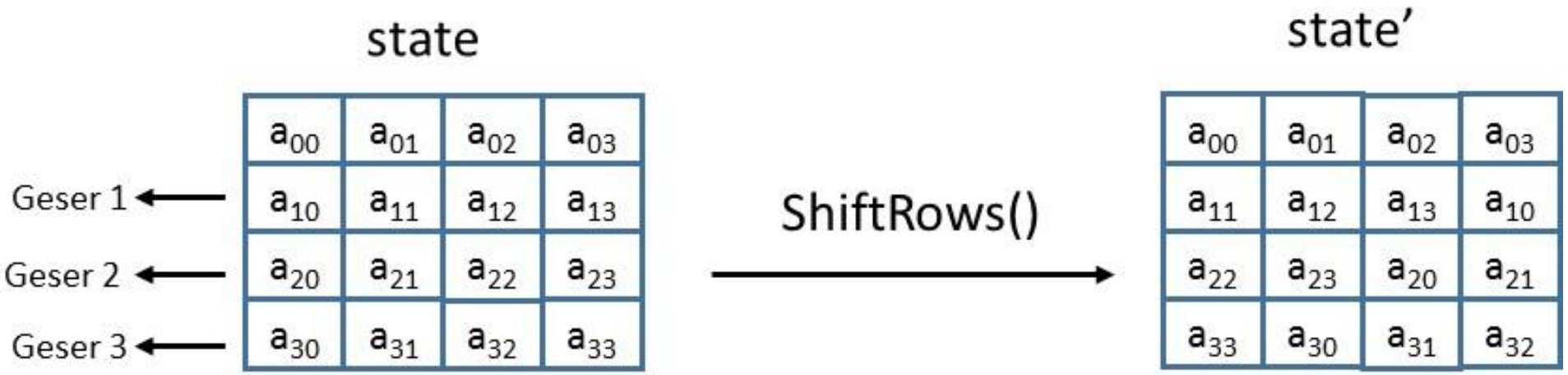
- Beberapa skema permutasi juga melakukan kompresi (mengurangi bit-bit input) atau ekspansi (memperbanyak bit-bit) pada operasi permutasi.



- Sedangkan di dalam *cipher* blok yang lain, permutasi tidak menggunakan P-box, tetapi melakukan pergeseran bit ke kiri atau ke kanan sejauh k bit.

- Pergeseraran bersifat siklik, yaitu bit yang paling ujung muncul pada ujung yag lain

- Contoh pergeseran *byte* di dalam AES:

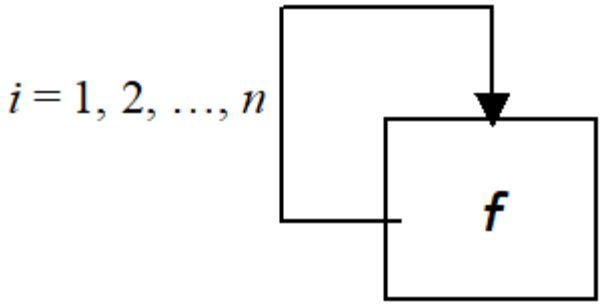


Cipher Berulang (*Iterated Cipher*)

- Untuk menghasilkan *cipher* yang lebih kuat, maka dilakukan *enciphering* sejumlah kali (sejumlah putaran) .

- Caranya adalah dengan melakukan berulang kali suatu fungsi transformasi *f* (disebut juga fungsi putaran atau *round function*) yang mengubah blok plainteks menjadi blokcipherteks.

- Pada setiap putaran digunakan upa-kunci (*subkey*) atau kunci putaran (*round key*) yang dikombinasikan dengan plainteks.



- *Cipher* berulang dinyatakan sebagai

$$C_i = f(C_{i-1}, K_i)$$

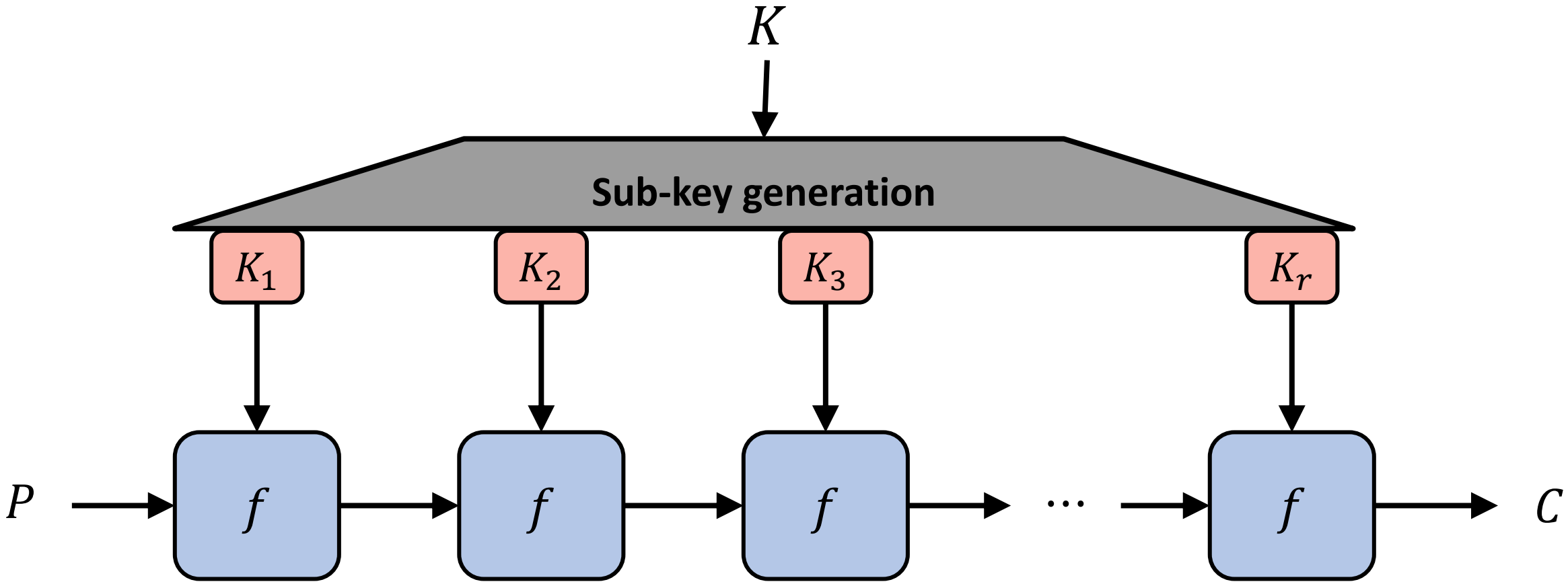
yang dalam hal ini,

i = 1, 2, …, *r* (*r* adalah jumlah putaran).

K_i = kunci putaran (*round key*) pada putaran ke-*i*

f = fungsi transformasi (*round function*), di dalamnya terdapat operasi substitusi, permutasi, dan/atau ekspansi, kompresi).

- Plainteks dinyatakan dengan C_0 dan cipherteks dinyatakan dengan C_r.



$f(K_i, P)$ dinamakan fungsi putaran, *r* adalah jumlah putaran

DES: $r = 16$

AES-128/192/256: $r = 10/12/14$

62

- Biasanya, plainteks dimanipulasi dulu dengan kunci (umumnya di-XOR-kan dengan kunci eksternal, atau dengan kunci putaran pertama), lalu hasilnya ditransformasikan dengan fungsi *f* berulang kali.

$$C_0 = P \oplus K_0$$
$$C_i = f(C_{i-1}, K_i) \quad , i = 1, 2, \ldots, r-1$$
$$C = C_r = C_{r-1} \oplus K_r$$

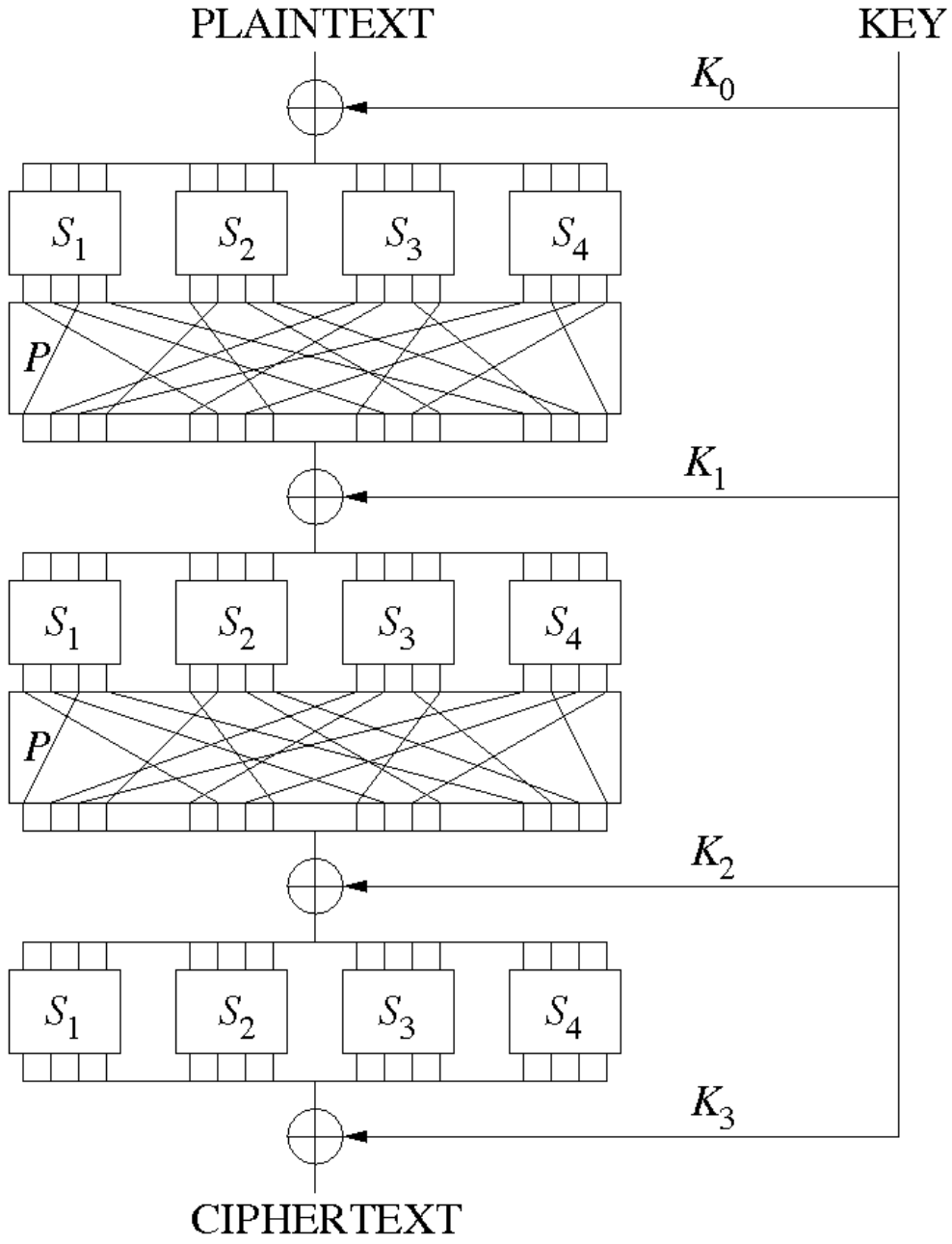
- Semakin banyak jumlah putaran, efek diffusi semakin bertambah, namun jumlah putaran yang besar dapat mempuat komputasi menjadi tidak sangkil (efisien).

- Jumlah putaran harus dipertimbangkan untuk mempertemukan kriteria keamanan dan efisiensi.

- Pada setiap putaran, proses *enciphering* melibatkan operasi substitusi dan permutasi. Operasi substitusi dilakukan dengan cara operasi *look-up* tabel S

- Operasi substitusi, diikuti dnegan oeprasi permutasi dilakukan pada setiap putaran. Setiap putaran menggunakan kunci putaran yang berbeda-beda (K_1, K_2, K_3, dst).

- Operasi substitusi menghasilkan efek *confusion*, sedangkan operasi permutasi menghasilkan efek *diffusion*.



https://commons.wikimedia.org/w/index.php?curid=6420152

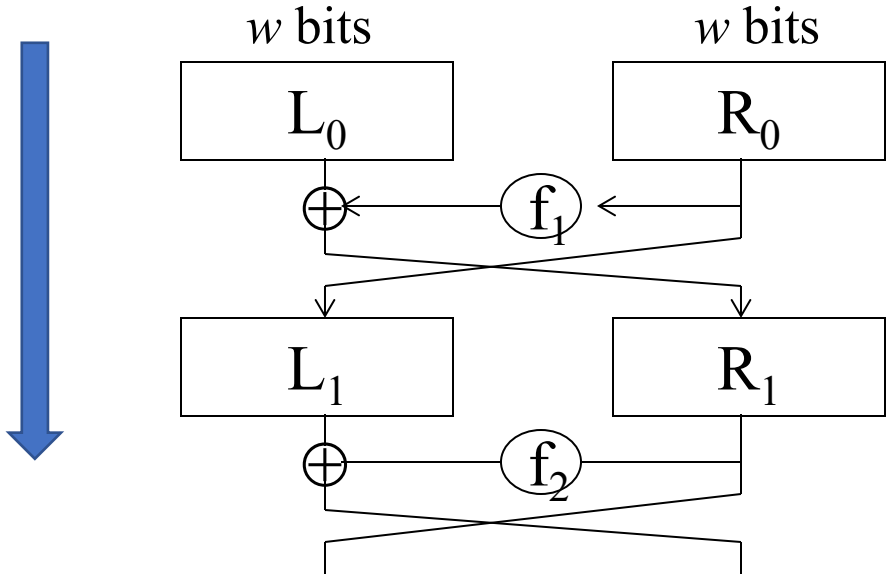
Jaringan Feistel

- Beberapa cipher blok seperti DES, GOST, Feal, Lucifer, RC5, RC6, dan lain-lain menggunakan struktur *enciphering* pada setiap putaran yang dinamakan **jaringan Feistel** (*Feistel Network*).

- Dalam hal ini, blok plainteks dibagi menjadi dua bagian, dan pada masing-masing bagian dilakukan proses transformasi menjadi upa-bagian pada putaran selanjutnya.

- Struktur ini bersifat *reversible*, yaitu untuk melakukan dekripsi maka jaringan Feistel dieksekusi dari “bawah” ke “atas”.

Feistel Network



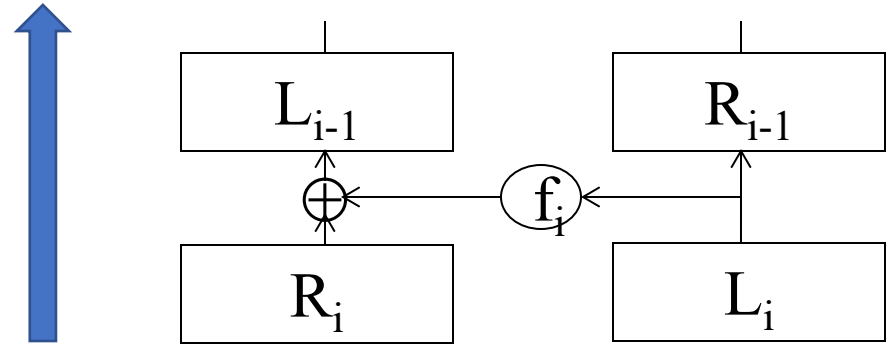
Encryption:

$$L_1 = R_0 \qquad R_1 = L_0 \oplus f_1(R_0)$$

$$L_2 = R_1 \qquad R_2 = L_1 \oplus f_2(R_1)$$

$$\ldots$$

$$L_i = R_{i-1} \qquad R_i = L_{i-1} \oplus f_i(R_{i-1})$$



Decryption:

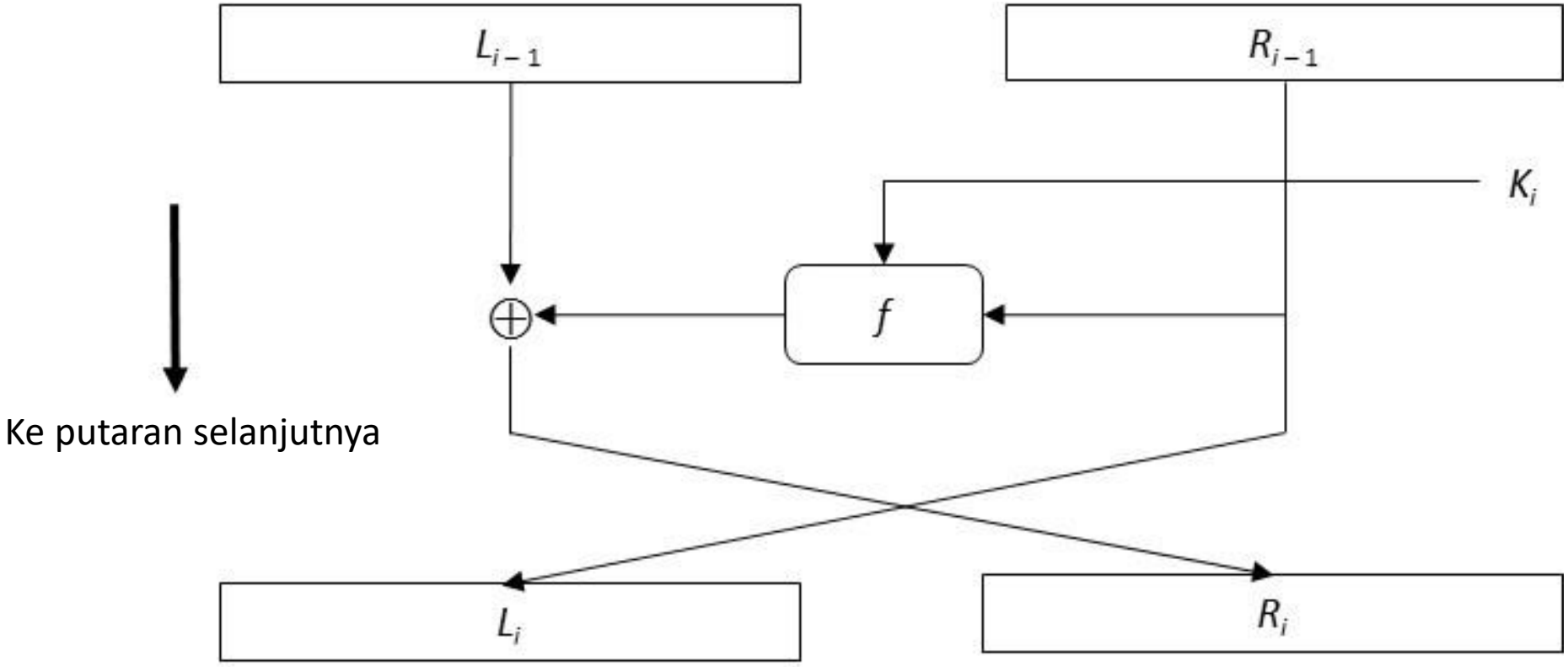
$$R_{i-1} = L_i \qquad L_{i-1} = R_i \oplus f_i(L_i)$$

$$\ldots$$

$$R_0 = L_1; \qquad L_0 = R_1 \oplus f_1(L_1)$$

Sumber: Cryptography CS 555

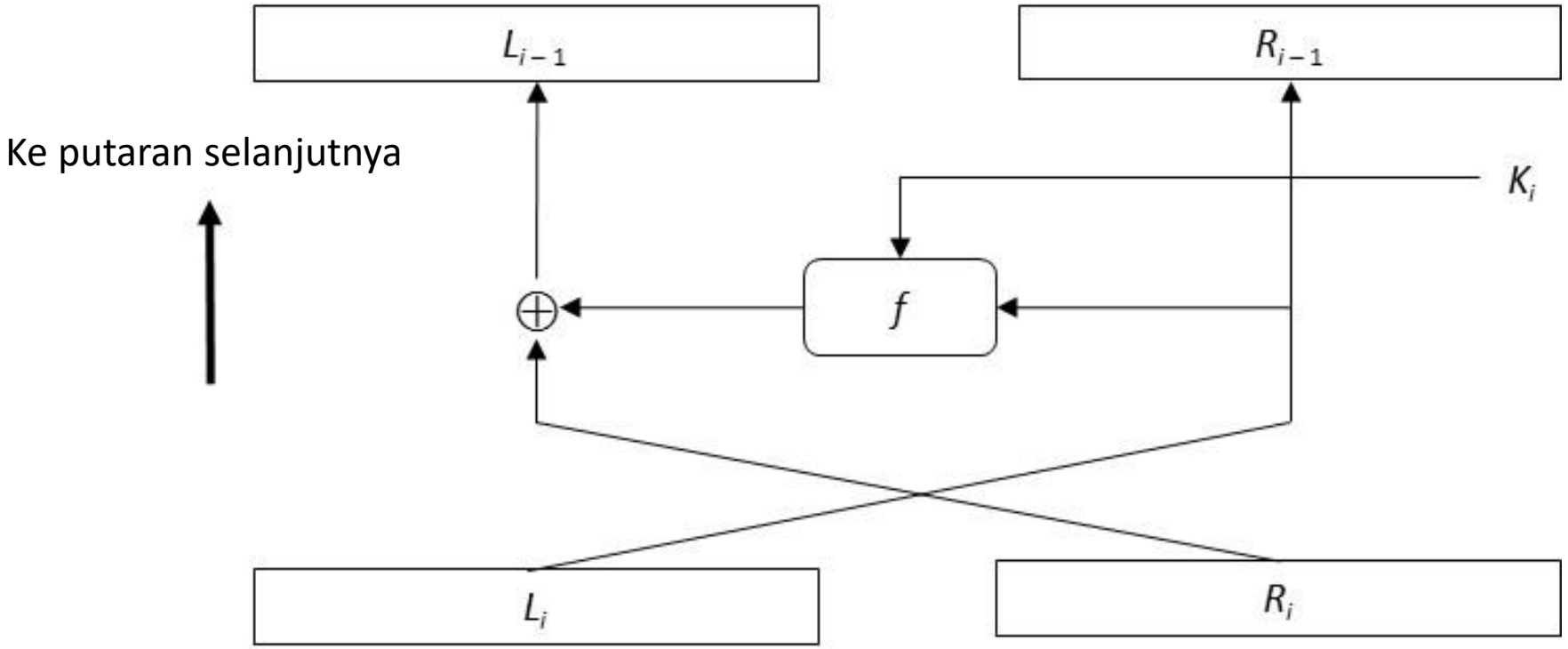
Contoh jaringan Feistel di dalam DES:



Jaringan *Feistel* pada enkripsi putaran ke-i

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

- Untuk melakukan dekripsi, maka urutan komputasi di dalam Feistel dibalik (dari "bawah" ke "atas"), itulah sebabnya dinamakan *reversible*.



Jaringan *Feistel* pada dekripsi putaran ke-i

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

- Sifat *reversible* ini membuat perancang cipher blok tidak perlu membuat algoritma baru untuk mendekripsi cipherteks menjadi plainteks.

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

- Sifat *reversible* tidak bergantung pada fungsi *f* sehingga fungsi *f* dapat dibuat serumit mungkin.

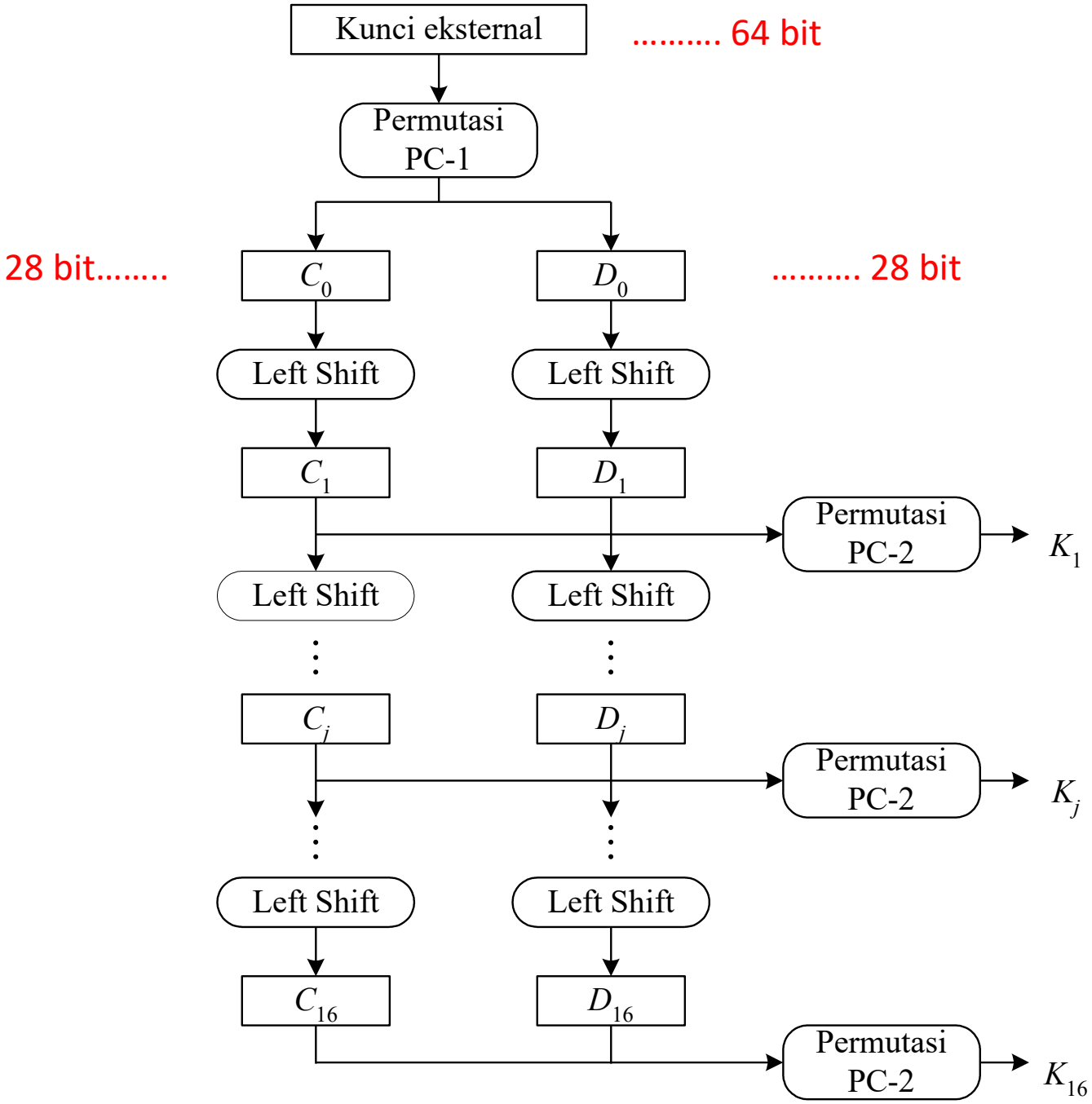
Pembangkitan kunci putaran

- Setiap putaran di dalam *iterated cipher* menggunakan kunci internal (*subkey*) yang dinamakan kunci putaran (*round key*).

- Kunci putaran dibangkitkan dari kunci eksternal yang diberikan oleh *user* melalui proses yang dinamakan *key expansion* atau *key scheduling*.

- Di dalam *key expansion* dilakukan komputasi yang kompleks untuk menghasilkan sejumlah kunci putaran yang berbeda-beda.

- Panjang kunci putaran tidak selalu sama dengan panjang kunci eksternal.



Gambar pembangkitan kunci putaran di dalam DES

Ukuran blok dan kunci

- Ukuran blok pesan (n) yang diproses selama enkripsi/dekripsi selalu tetap.

  Contoh: DES (n = 64), AES (n = 128, 192, 256)
- Makin besar ukuran blok mengarah ke efek *diffusion* yang lebih besar.
- Ukuran kunci (m) bisa sama dengan ukuran blok atau berbeda dengan ukuran blok

  Contoh: DES (m = 56), AES (m = 128, 192, 256)
- Makin besar ukuran kunci mengarah ke efek *confusion* yang lebih besar dan lebih tahan terhadap serangan *brute force*.

Bersambung

Bersambung