PERTEMUAN III

BLOCK-CIPHER

Dr. R. Rizal Isnanto, S.T., M.M., M.T.

Jurusan Teknik Elektro/Sistem Komputer
Fakultas Teknik
Universitas Diponegoro

Introduction

- Block-cipher adalah skema algoritma sandi yang akan membagi-bagi plaintext yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama.

- Pada umumnya, block-cipher memproses teks terang dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci.

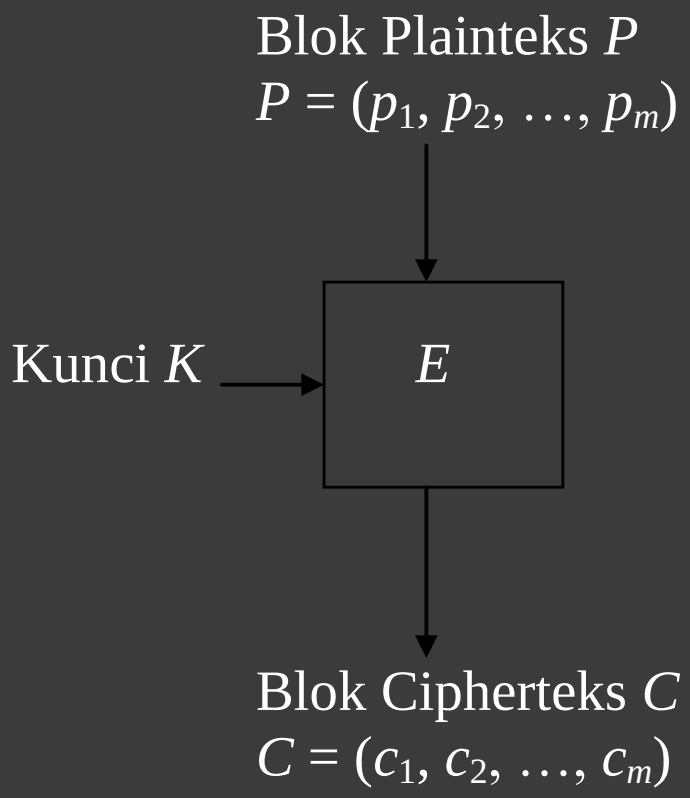
Blok plainteks berukuran m bit:

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

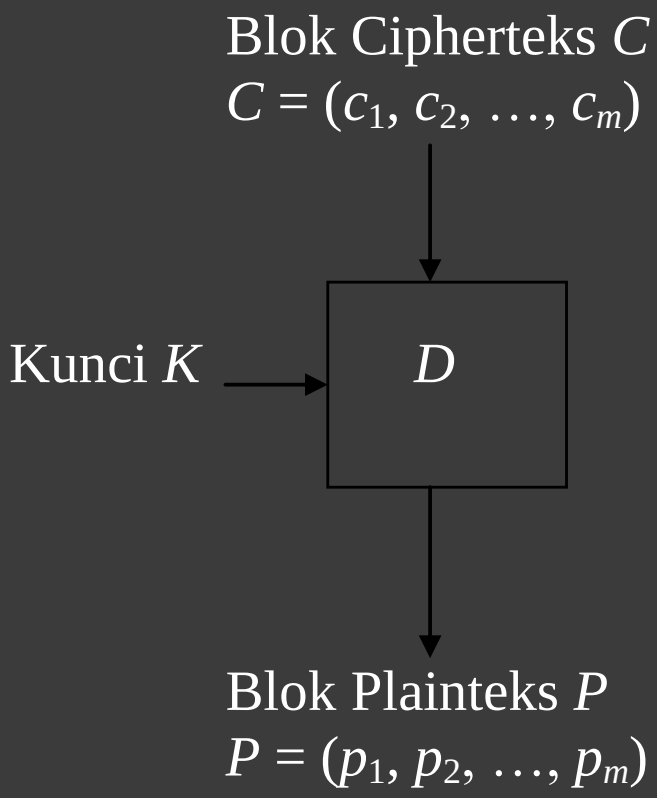
Blok cipherteks (C) berukuran m bit:

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

Enkripsi:



Dekripsi:



Gambar 2.1 Skema enkripsi dan dekripsi pada *cipher* blok

Untuk menambah kehandalan model algoritma sandi ini, dikembangkan pula beberapa tipe proses enkripsi, yaitu :

- ECB, Electronic Code Book
- CBC, Cipher Block Chaining
- CFB, Cipher Feed Back Mode
- OFB, Output Feed Back
- Feistel Cipher

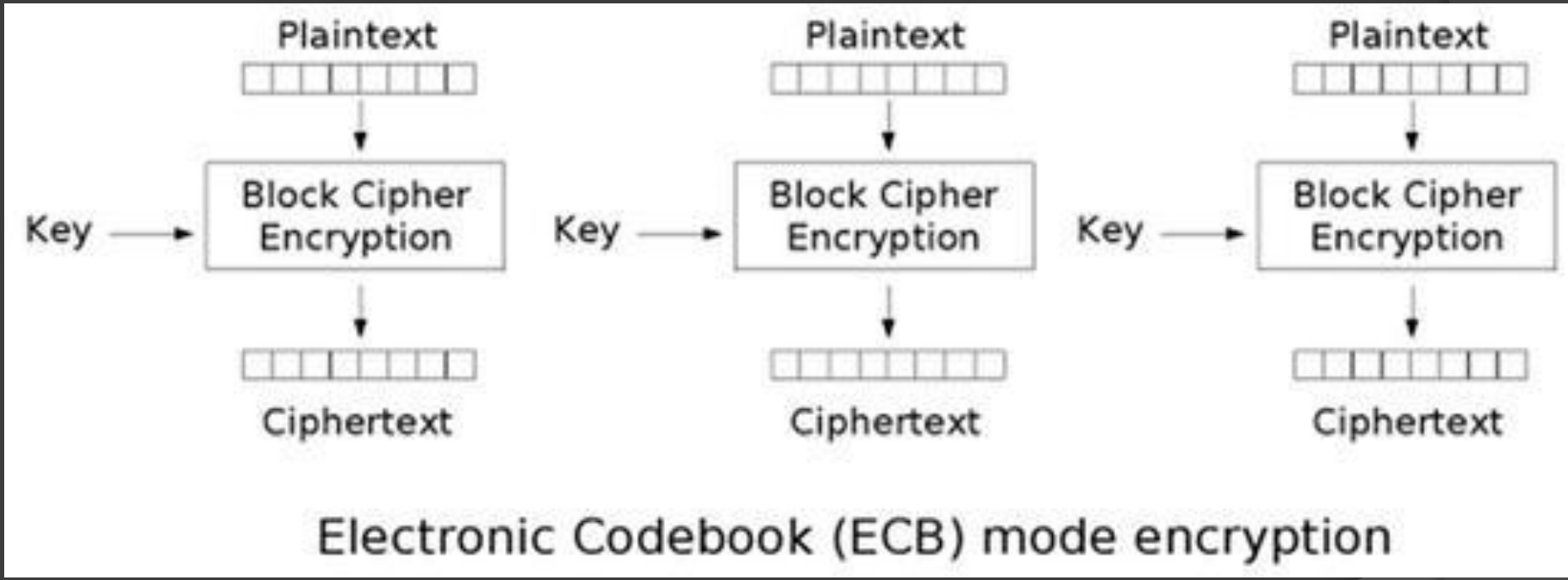
Electronic Code Book (ECB)

- Setiap blok plainteks P_i dienkripsi secara individual dan independen 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.

Diagram Blok Enkripsi ECB



- Contoh:

  Plainteks: `10100010001110101001`

  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 adalah: XOR-kan blok plainteks P_i dengan *K*, kemudian geser secara *wrapping* bit-bit dari $P_i \oplus K$ satu posisi ke kiri.

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

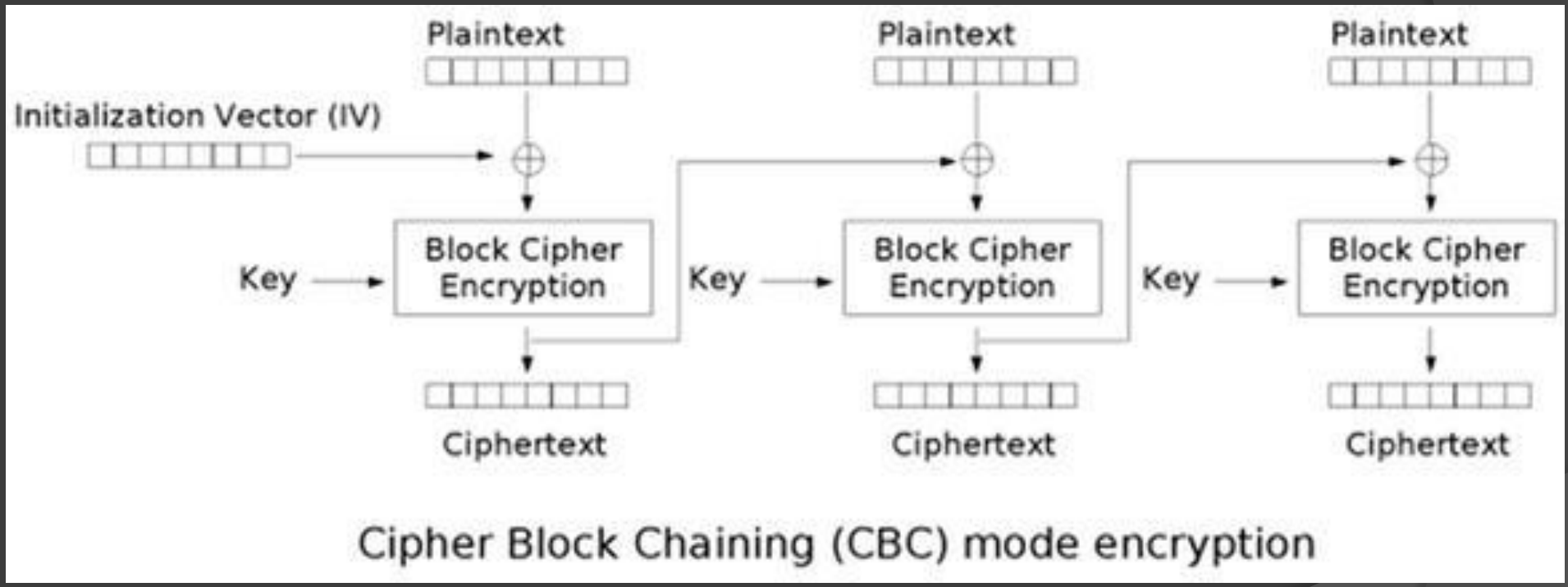
`00100011000100100100` (`23124` dalam notasi HEX)

Cipher Block Chaining (CBC)

- Mode ini menerapkan mekanisme umpan-balik (*feedback*) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current*.

- Caranya, blok plainteks yang *sedang* di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi

Blok Diagram Enkripsi CBC



- Contoh :

  Suatu pesan 110000100110 010010100110 011101101110 010101011010. Dengan panjang blok 12-bit dimasukkan ke dalam CBC dengan kunci untuk blok pertama K_1 = 110010011111 dan K_n ditentukan oleh K_{n-1} yang digeser ke kanan memutar sebanyak 3-bit. Tentukan cipher text keluaran CBC tersebut. Dengan acuan IV = 000000000000 dan blok enkripsi E merupakan fungsi XOR.

M1 = 110000100110
M2 = 010010100110
M3 = 111011001110
M4 = 101100110100

K1 = 110010011111
K2 = 111110010011
K3 = 011111110010
K4 = 010011111110

M1 = 110000100110
IV = 000000000000
K1 = 110010011111

C1 = 000010111001

M2 = 010010100110
c1 = 000010111001
k2 = 111110010011

c2 = 101110001100

M3 = 111011001110
C2 = 101110001100
k3 = 011111110010

C3 = 001010110000

M4 = 101100110100
C3 = 001010110000
K4 = 010011111110

C4 = 110101111010

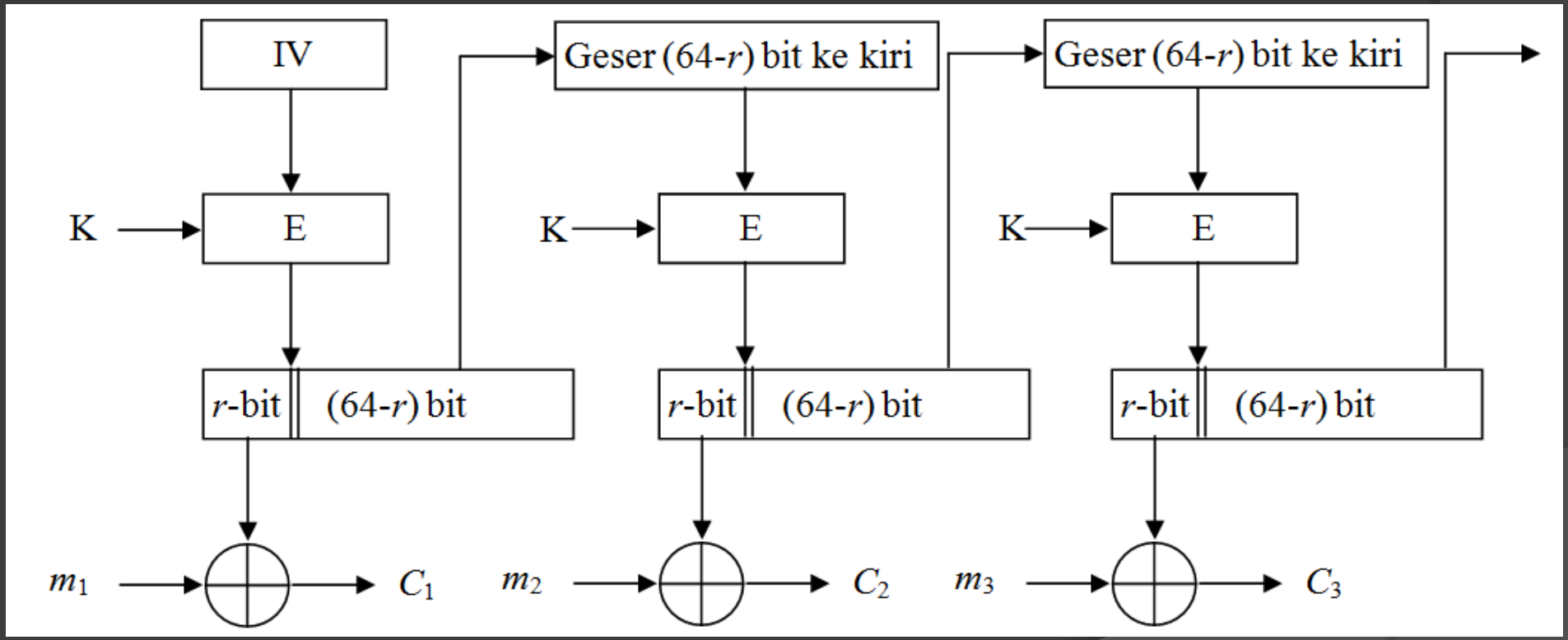
Maka hasil akhir C = 000010111001101110001100001010110000110101111010

Cipher-FeedBack Mode (CFB)

- Pada mode *CFB*, data dienkripsikan dalam unit yang lebih kecil daripada ukuran blok. Unit yang dienkripsikan dapat berupa bit per bit, 2-bit, 3-bit, dan seterusnya.

- Secara umum *CFB n*-bit mengenkrips plainteks sebanyak *n* bit setiap kalinya, yang mana $n \leq m$ (m = ukuran blok).

Mode Operasi CFB



1. Antrian diisi dengan *IV* (*initialization vector*).

2. Dekripsikan antrian dengan kunci *K*. *n* bit paling kiri dari hasil dekripsi berlaku sebagai *keystream* (*ki*) yang kemudian di-*XOR*-kan dengan *n*-bit dari cipherteks menjadi *n*-bit pertama dari plainteks. Salinan (*copy*) *n*-bit dari cipherteks dimasukkan ke dalam antrian (menempati *n* posisi bit paling kanan antrian), dan semua *m*-*n* lainnya di dalam antrian digeser ke kiri menggantikan *n* bit pertama yang sudah digunakan.

3. *m*-*n* bit cipherteks berikutnya dienkripsikan dengan cara yang sama seperti pada langkah 2.

- Contoh :

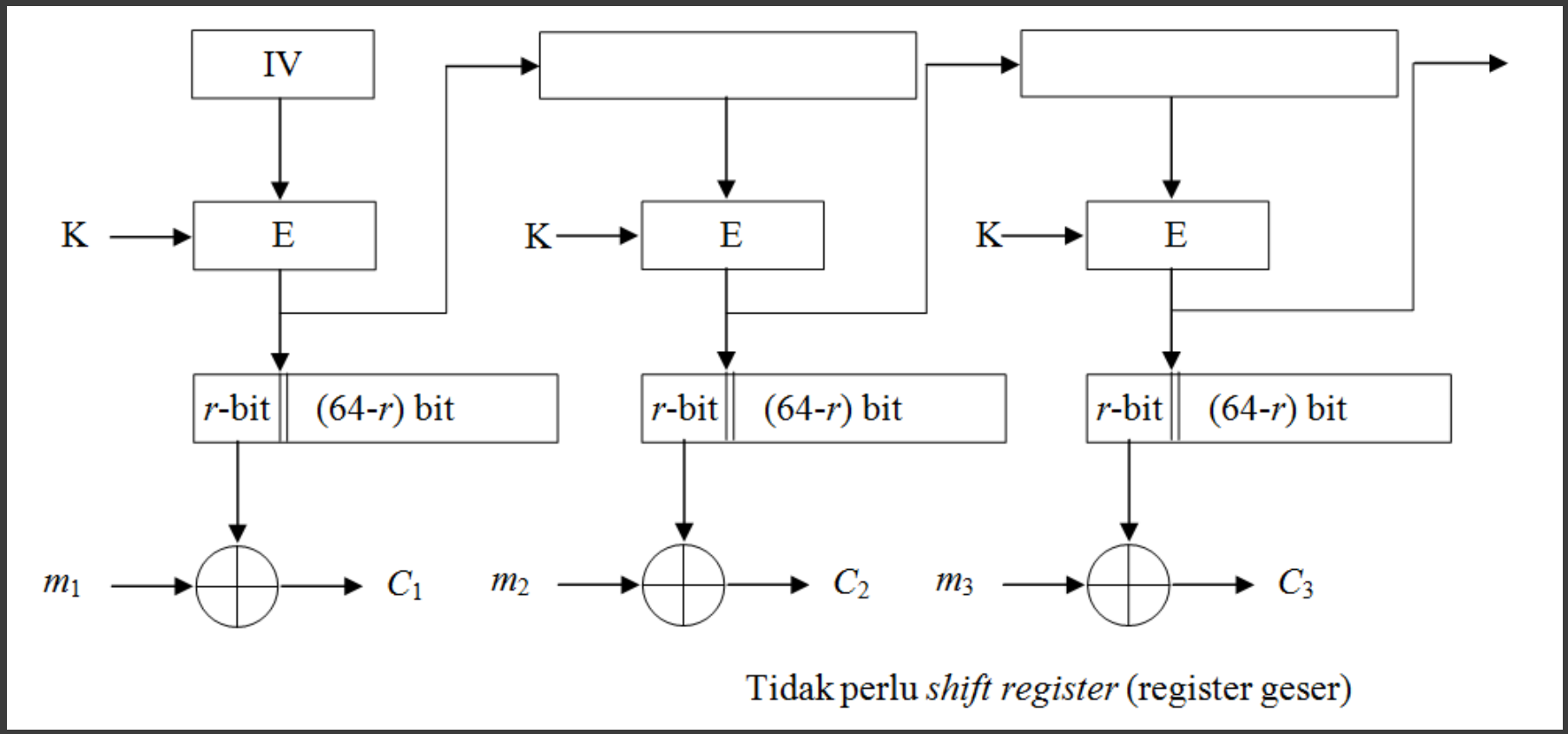
  Untuk panjang block setelah enkripsi adalah 8-bit (bukan 64-bit) dan r = 2-bit. Tentukan C_1, C_2, C_3 dan C_4 menggunakan CFB jika diketahui bahwa pesan asli m = 11010100; dengan m_1 = 11, m_2 = 01, m_3 = 01, dan m_4 = 00 dengan IV = 00000000 dan K1 = 01101101 dengan E fungs$_i$ EXOR, K_n= SHL (K_n-1) 1 –bit $_k$e k$_i$ri.

Output-FeedBack (OFB)

- Pada mode *OFB*, data dienkripsikan dalam unit yang lebih kecil daripada ukuran blok. Unit yang dienkripsikan dapat berupa bit per bit, 2-bit, 3-bit, dan seterusnya.

- Secara umum *OFB n*-bit mengenkripsi plainteks sebanyak *n* bit setiap kalinya, yang mana $n \leq m$ (m = ukuran blok).

Mode Operasi OFB *r*-bit



1. Antrian diisi dengan *IV* (*initialization vector*).

2. Dekripsikan antrian dengan kunci *K*. *n* bit paling kiri dari hasil dekripsi dimasukkan ke dalam antrian 7 (menempati *n* posisi bit paling kanan antrian), dan *m*-*n* bit lainnya di dalam antrian digeser ke kiri menggantikan *n* bit pertama yang sudah digunakan. *n* bit paling kiri dari hasil dekripsi juga berlaku sebagai *keystream* (*ki*) yang kemudian di-*XOR*-kan dengan *n*-bit dari cipherteks menjadi *n*-bit pertama dari plainteks.

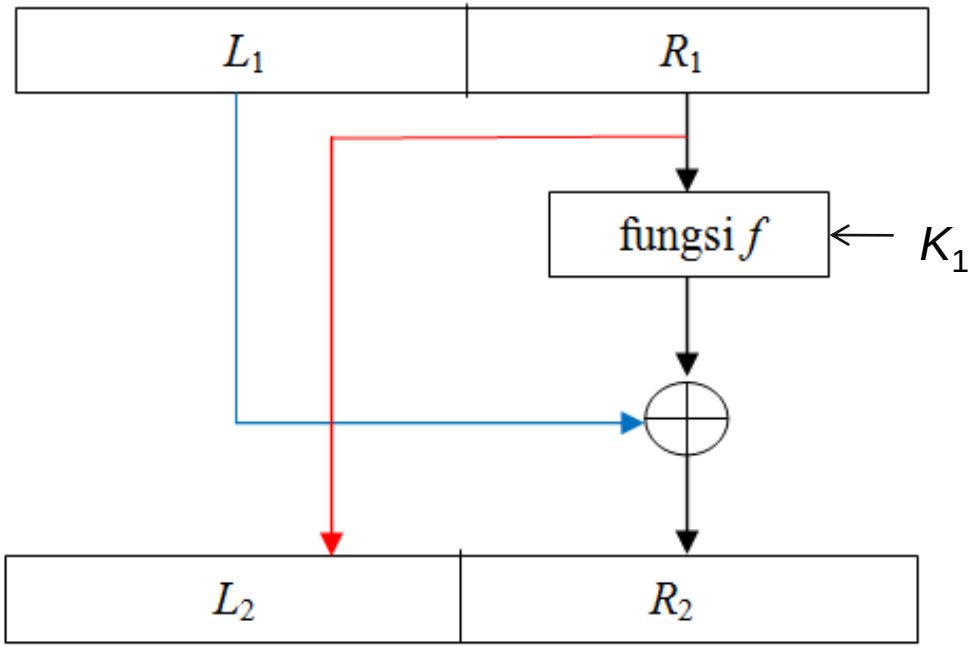
3. *m*-*n* bit cipherteks berikutnya dienkripsikan dengan cara yang sama seperti pada langkah 2.

Feistel Cipher

$L_2 = R_1$ $\qquad R_2 = L_1 \oplus f(K_1, R_1)$

$L_n = R_{n-1}$ $\qquad R_n = L_{n-1} \oplus f(K_1, R_1)$

Enkripsi



PR: Gambarkan diagram blok untuk dekripsi atas Feistel Cipher.

Tugas Kelompok

1. Koordinator MK harap membagi kelas menjadi 14 kelompok, jumlah relatif sama
2. Setiap kelompok merangkum (amanat dari Jurusan) materi matakuliah, dengan ketentuan:

   Kelompok 1 merangkum materi Pertemuan 1

   Kelompok 2 merangkum materi Pertemuan 2

   dst. sampai dengan Kelompok 14.
3. Koordinator MK harap membagi kelas menjadi 14 kelompok, jumlah relatif sama.
4. Rangkuman ditulis tangan (1 atau 2 lembar lembar buku catatan)
5. Dikumpulkan pada saat UTS (kelompok 1-7) dan saat UAS (kelompok 8-14)
6. Tugas rangkuman difoto atau di-*scan*, dikumpulkan lewat Koordinator MK
7. Butir 5 dan 6 bersifat tentatif, bisa berubah jika dari Prodi ada ketentuan lain.

Any question?

Sekian..

Terimakasih..