No :

Date:

Nama : Muhammad Ishak Jaelani

NIM : E1E120042

Matkul : Kriptografi

Soal

1. Buat contoh ECB, CBC, CFB, OFB dengan plaintext 16 bit (diambil dari 2 digit nim yaitu 42), kunci 1011, IV 0000 ! (untuk CFB dan OFB, n=2, m=4)

Jawaban

1. Diketahui plaintext = 42 (char)

= 0011 0100 0011 0010 (bit)

kunci = 1011

IV = 0000 = C0

n = 2 ; m = 4

* ECB (Electronic Code Book)

Enkripsi =

0011 0100 0011 0010

1011 1011 1011 1011 ⊕

Hasil XOR = 1000 1111 1000 1001

Desimal : 0001 1111 0001 0011

HEX : 1 F 1 3

Sehingga, chiper text = 1F13

* CBC (Ciphter Block Chaining)

Block Bit 0011 0100 0011 0010

P_1 P_2 P_3 P_4

C_1 diperoleh sebagai berikut:

$P_1 \oplus C_0 = 0011 \oplus 0000 = 0011$

$0011 \oplus K = 0011 \oplus 1011 = 1000$

Geser hasil ini satu bit ke kiri $= 0001$

Jadi, $C_1 = 0001$ (atau 1 dalam HEX)

C_2 diperoleh sebagai berikut:

$P_2 \oplus C_1 = 0100 \oplus 0001 = 0101$

$0101 \oplus K = 0101 \oplus 1011 = 1110$

Geser hasil ini satu bit ke kiri $= 1101$

Jadi, $C_2 = 1101$ (atau D dalam HEX)

C_3 diperoleh sebagai berikut:

$P_3 \oplus C_2 = 0011 \oplus 1101 = 1110$

$1110 \oplus k = 1110 \oplus 1011 = 0101$

Geser hasil ini satu bit ke kiri $= 1010$

Jadi, $C_3 = 1010$ (atau A dalam HEX)

C_4 diperoleh sebagai berikut:

$P_4 \oplus C_3 = 0010 \oplus 1010 = 1000$

$1000 \oplus k = 1000 \oplus 1011 = 0011$

Geser hasil ini satu bit ke kiri $= 0110$

Jadi, $C_4 = 0110$ (atau 6 dalam HEX)

Sehingga, chipertext = 1DA6

No.: Date:

* Cipher Feedback (CFB)

Unit bit 00 11 01 00 00 11 00 10

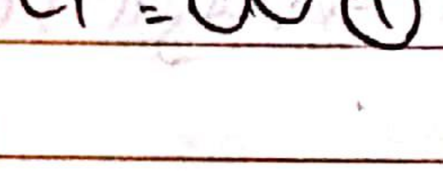
P1 P2 P3 P4 P5 P6 P7 P8

$X_1 = IV = 0000$

$K = 1011$ ⊕

1011

Geser = 0111



$C_1 = 00 \oplus 01 = 01$

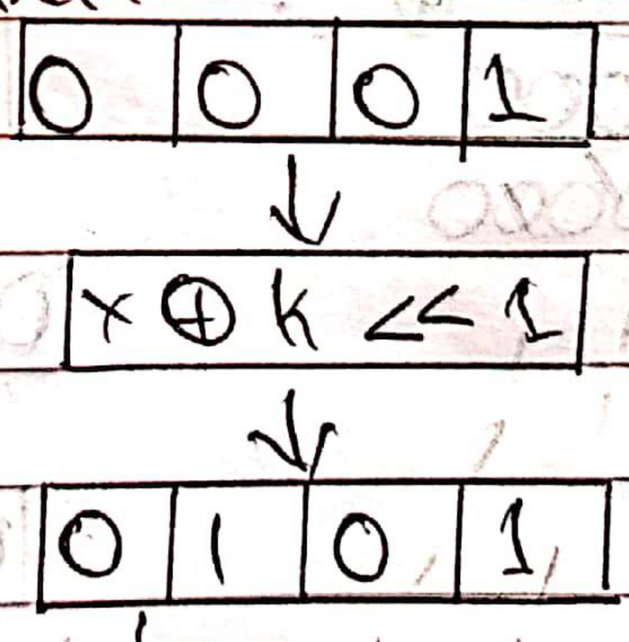
C_2 diperoleh sebagai berikut

$X_2 = 0001$

$K = 1011$ ⊕

1010

Geser = 0101



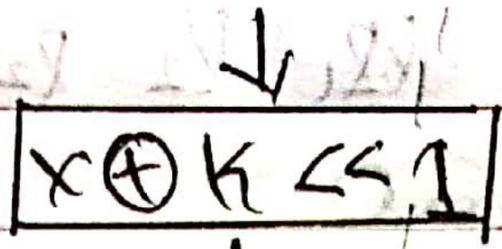
$C_2 = P_2 \oplus 01 = 11 \oplus 01 = 10$

C_3 diperoleh sebagai berikut

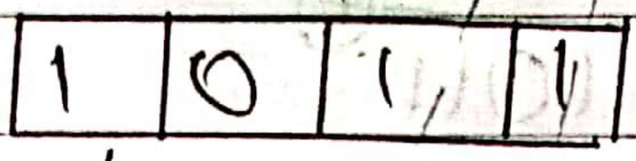
$X_3 = 0110$

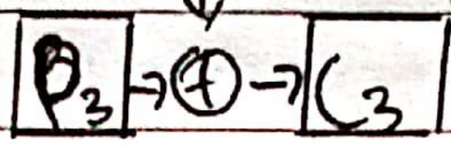
$K = 1011$ ⊕

1101



Geser = 1011

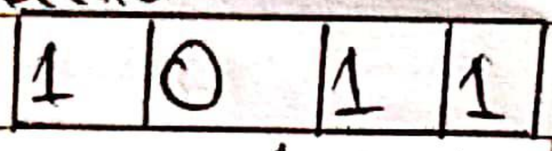




$C_3 = P_3 \oplus 10 = 01 \oplus 10 = 11$

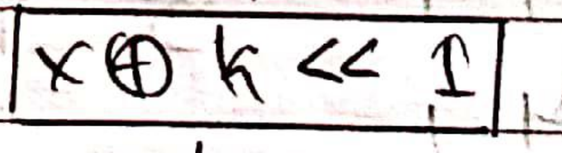
C_4 diperoleh sebagai berikut

$X_4 = 1011$

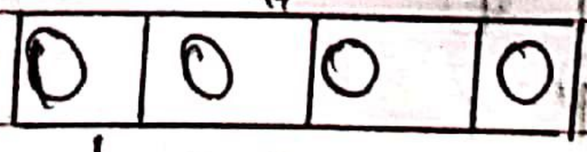


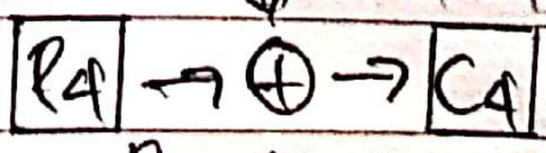
$K = 1011$ ⊕

0000



Geser = 0000





$C_4 = P_4 \oplus 00 = 00 \oplus 00 = 00$

No.: Date:

C_5 diperoleh sebagai berikut

$x_5 = 1100$

$K = 1011$ ⊕

0111

Geser = 1110

1	1	0	0

↓

$x \oplus K << 1$

↓

1	1	1	0

P_5 → ⊕ → C_5

$C_5 = P_5 \oplus 11 = 00 \oplus 11 = 11$

C_6 diperoleh sebagai berikut

$x_6 = 0011$

$K = 1011$ ⊕

1000

Geser = 0001

0	0	1	1

↓

$x \oplus K << 1$

↓

0	0	0	1

P_6 → ⊕ → C_6

$C_6 = P_6 \oplus 00 = 11 \oplus 00 = 11$

No.: Date:

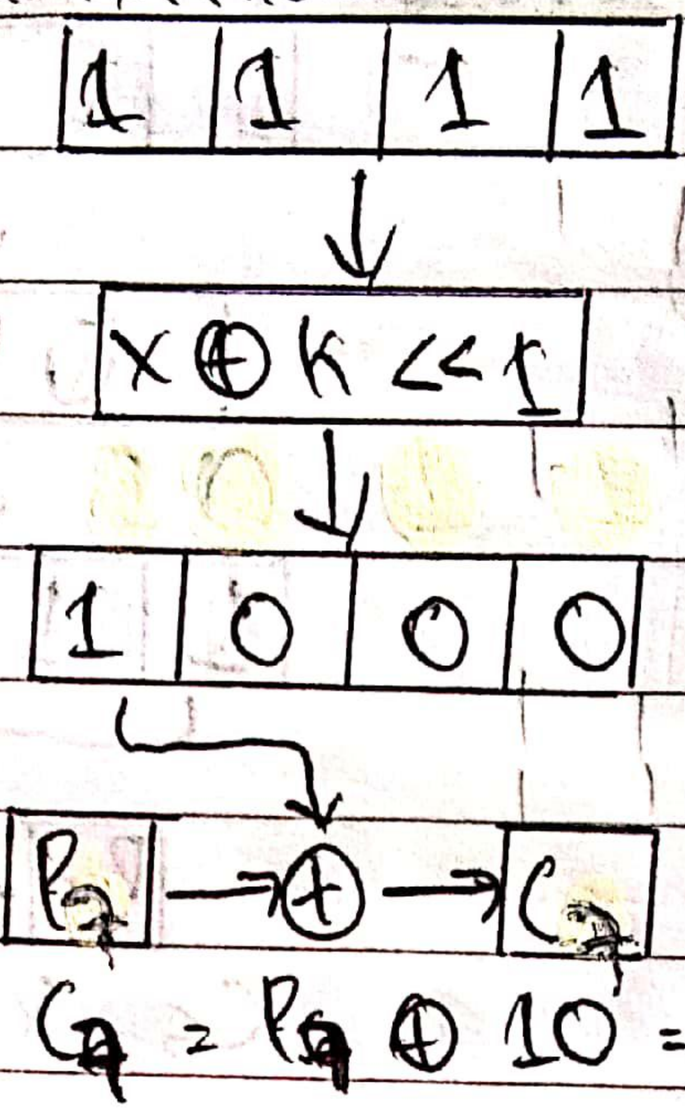
C4 diperoleh sebagai berikut

$X_7 = 1111$

$K = 1011 \oplus$

0100

Geser = 1000



$C_4 = P_4 \oplus 10 = 00 \oplus 10 = 10$

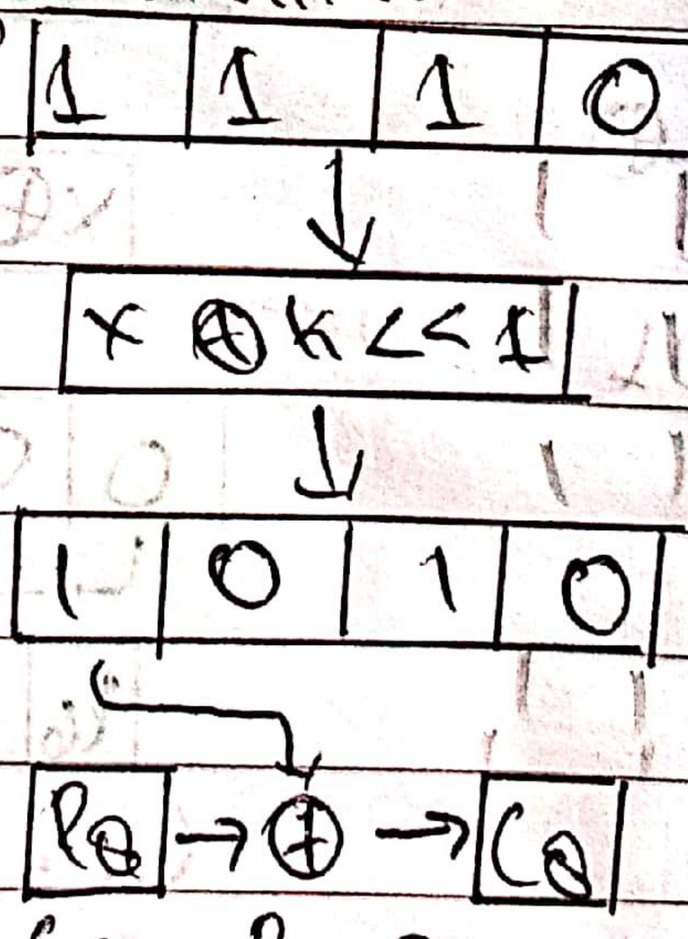
C3 diperoleh sebagai berikut

$X_6 = 1110$

$K = 1011 \oplus$

0101

Geser = 1010



$C_3 = P_3 \oplus 10 = 10 \oplus 10 = 00$

Sehingga, Ciphertext = 0110 1100 1111 1000

HEX = 6 C F 8

No.: Date:

* Output - Feedback (OFB)

Unit Blk 00 11 01 00 00 11 00 10

P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8

$X_1 = IV = 0000$

$K = 1011$

1011 ⊕

Keset = 0111

0	0	0	0

↓

$X \oplus K << 1$

↓

0	1	1	1

P_1 → ⊕ → C_1

$C_1 = P_1 \oplus 01 = 00 \oplus 01 = 01$

C_2 diperoleh sebagai berikut

$X_1 = 0001$

$K = 1011$

1010 0

Keset = 0101

0	0	0	1

↓

$X \oplus K << 1$

↓

0	1	0	1

P_2 → ⊕ → C_2

$C_2 = P_2 \oplus 01 = 11 \oplus 01 = 10$

$01 = 10 \oplus 11 =$

C_3 diperoleh sebagai berikut

$X_3 = 0101$ | 0 | 1 | 0 | 1 |

$K = 1011$ ⊕

1100

↓

$X \oplus K << 1$

Geser = 1101

↓

| 1 | 1 | 0 | 1 |

| P_3 | → ⊕ → | C_3 |

$C_3 = P_3 \oplus 11 = 01 \oplus 11 = 10$

C_4 diperoleh sebagai berikut

$X_4 = 0111$ | 0 | 1 | 1 | 1 |

$K = 1011$ ⊕

1100

↓

$X \oplus K << 1$

Geser = 1001

↓

| 1 | 0 | 0 | 1 |

| P_4 | → ⊕ → | C_4 |

$C_4 = P_4 \oplus 10 = 00 \oplus 10 = 10$

No.: Date:

C_5 diperoleh sebagai berikut

$x_5 = 1110$

$k = 1011$ ⊕
0101

1	1	1	0

↓

$x \oplus k \ll 1$

hasil = 1010

↓

1	0	1	0

P_5 → ⊕ → C_5

$C_5 = P_5 \oplus 10 = 00 \oplus 10 = 10$

C_6 diperoleh sebagai berikut

$x_6 = 1010$

$k = 1011$ ⊕
0001

1	0	1	0

↓

$x \oplus k \ll 1$

hasil = 0000

↓

0	0	1	0

P_6 → ⊕ → C_6

$C_6 = P_6 \oplus 00 = 11 \oplus 00 = 11$

No.: Date:

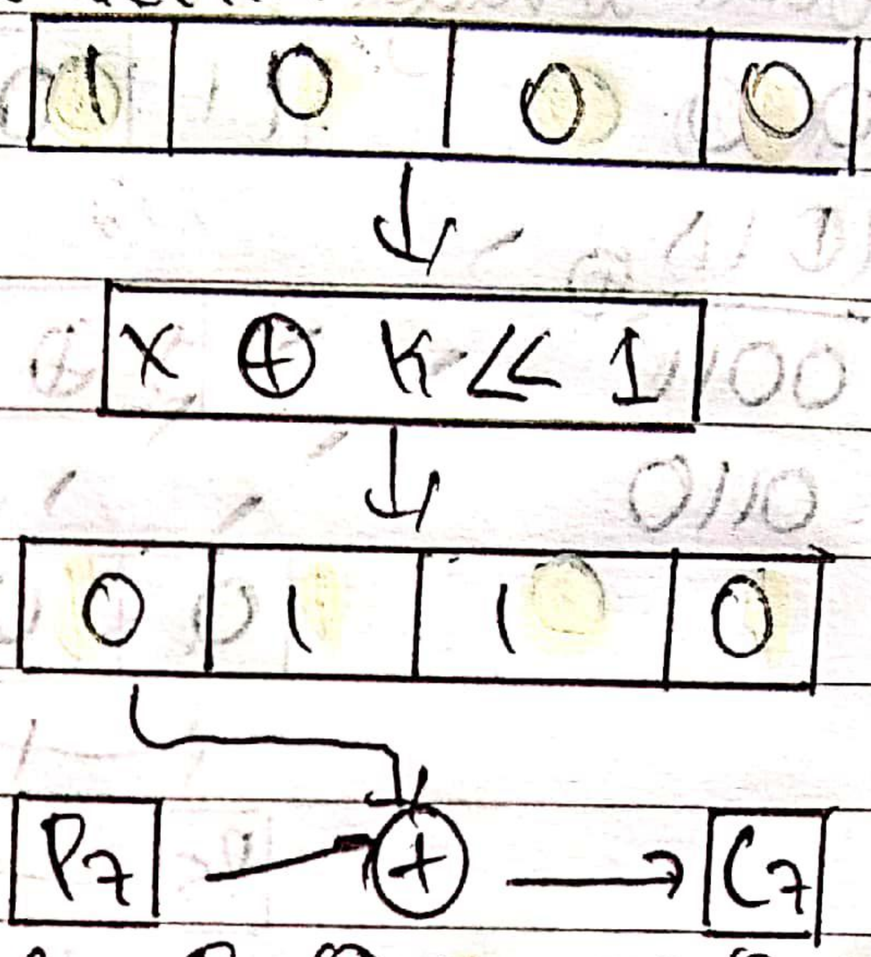
C_7 diperoleh sebagai berikut

$X_7 = 1000$

$K = 1011$ ⊕

0011

Geser = 0110



$C_7 = P_7 \oplus 01 = 00 \oplus 01 = 01$

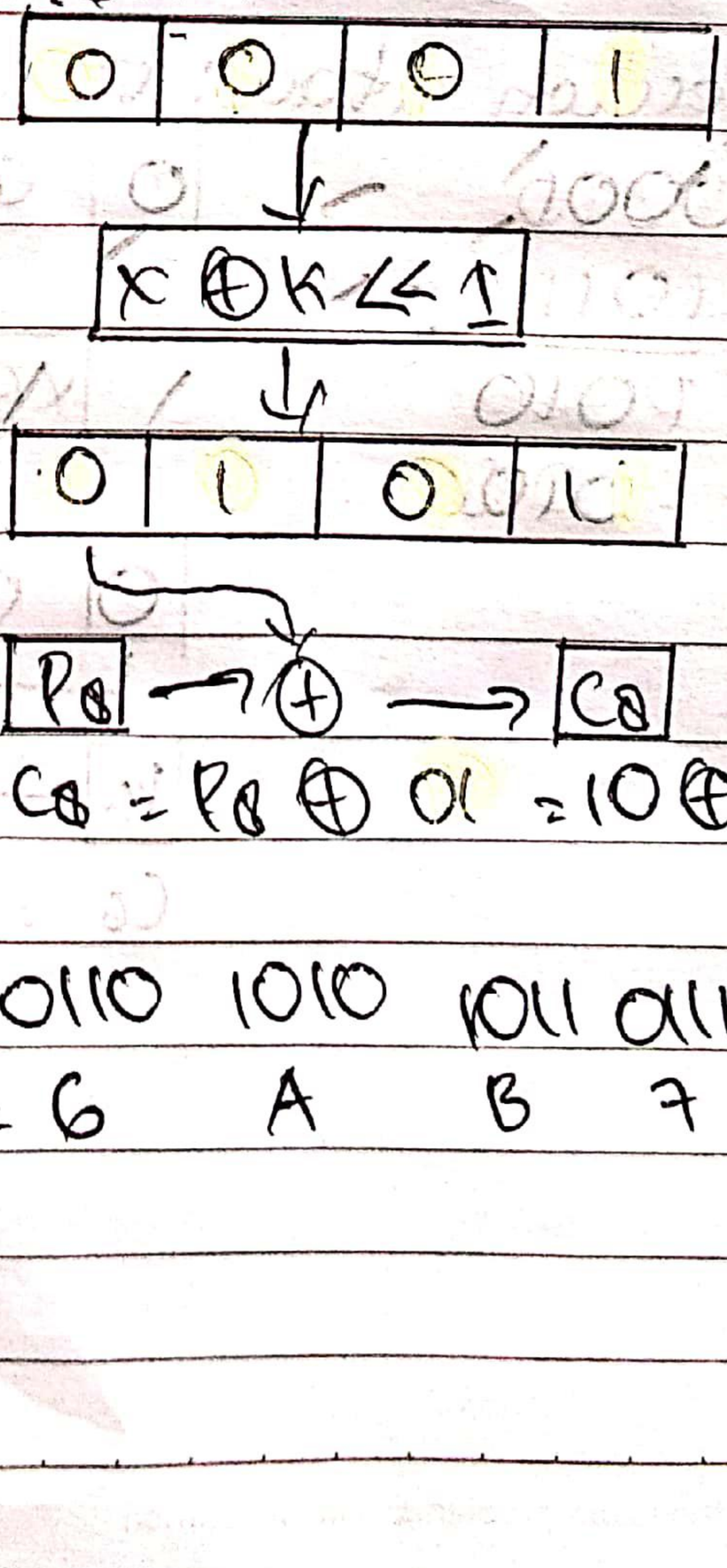
C_8 diperoleh sebagai berikut

$X_8 = 0001$

$K = 1011$ ⊕

1010

Geser = 0101



$C_8 = P_8 \oplus 01 = 10 \oplus 01 = 11$

Sehingga, ciphertext = 0110 1010 1011 0111

HEX = 6 A B 7