No.

Date . .

Nama : Muh. Rahmat dhyan f
Nim : E1E120084
kelas : GENAP

Tugas 3 kriptografi

Plainteks : 0011 0101 0011 0110 / 56 (char)
Block : P1 P2 P3 P4
Chiper 4bit : 0011 0101 0011 0110
Code Hexa : 3 5 3 6

k : 1011
Iv : 0000
m : 4
n : 2

1. Electronic Code Block (ECB)
Enkripsi : $E_k(P) : (P \oplus k) << 1$

P1 : 0011
k : 1011 ⊕
1000
C1 : 0001
Hexa : 1

P2 : 0101
k : 1011 ⊕
1110
C2 : 1101
Hexa : D

P3 : 0011
k : 1011 ⊕
1000
C3 : 10001
Hexa : 1

P4 : 0110
k : 1011 ⊕
1101
C4 : 1011
Hexa : B

Hasil enkripsi Plainteks : 0011010100110110
= 3636 (Hexa)
ECB = 0001110100011011
= 101B (Hexa)

2. Chiper Block chaining (CBC)

P1 : 0011
Iv : 0000 ⊕
0011
k : 1011 ⊕
1000
C1 : 0001
Hexa : 1

P2 : 0101
Iv : 0001 ⊕
0100
k : 1011
1111
C2 : 1111
Hexa : F

P3 : 0011
Iv : 1111 ⊕
1100
k : 1011 ⊕
0111
C3 : 1110
Hexa : E

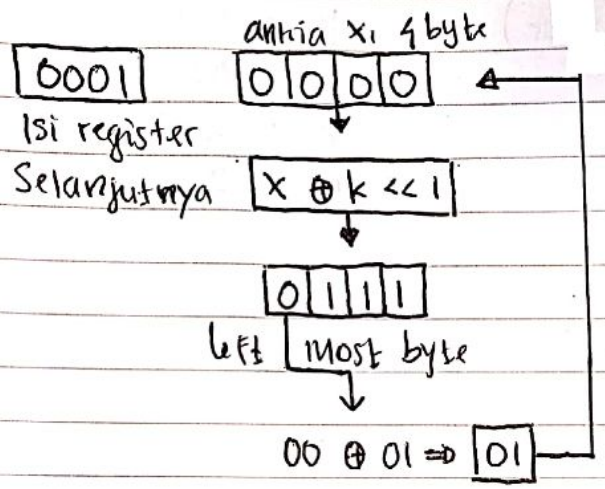
P4 : 0110
Iv : 1110 ⊕
1000
k : 1011 ⊕
0011
C4 : 0110
Hexa : 6

Date

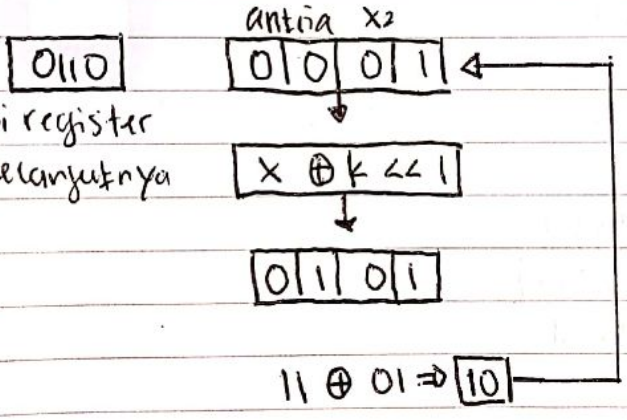
Hasil enkripsi plainteks : 0011 0101 0011 0110
: 3636 (Hexa)

CBC : 0001 1111 1100 1110
: 1 F E 6 (Hexa)

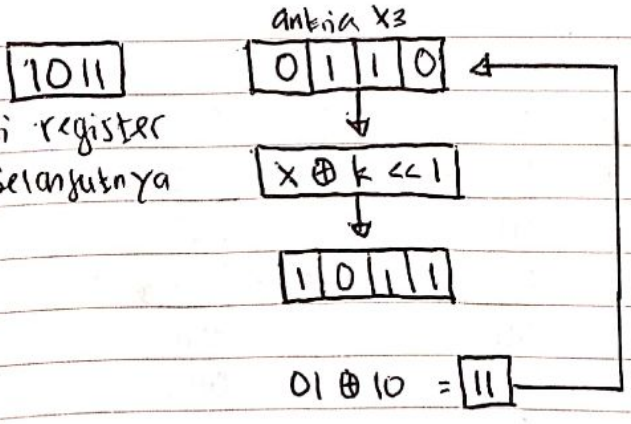
3. Chiper feedback (CFB) :



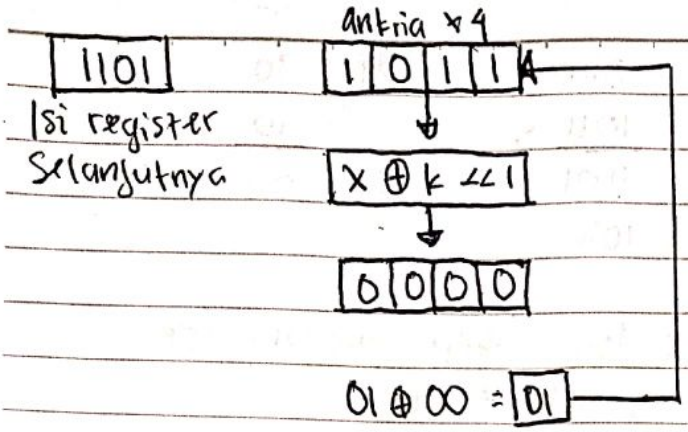
x1 : 0000 p1 : 00
k : 1011 ⊕ 01 ⊕
1011 01
Wrapping : 0111 c1 : 01
LMB : 0111



x2 : 0001 p2 : 11
k : 1011 ⊕ 01 ⊕
1010 c2 10
= 0101

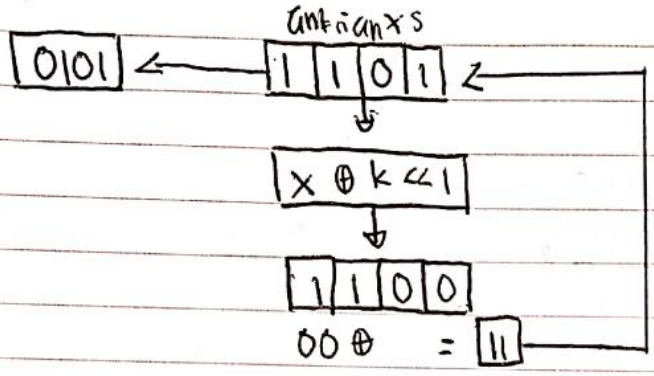


x3 : 0110 p3 : 01
k : 1011 ⊕ 10 ⊕
1101 c3 11
= 1011



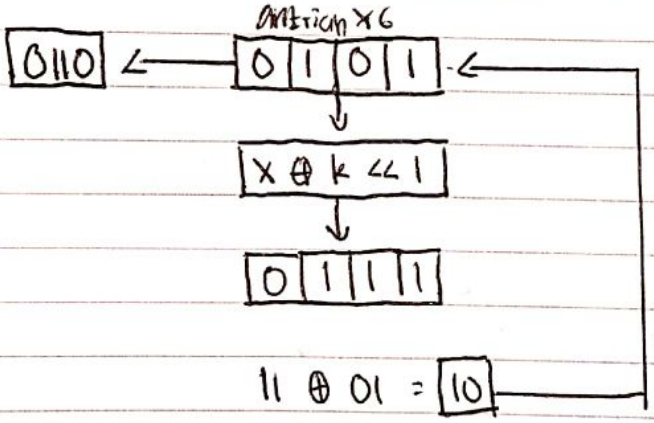
x4 : 1011
k : 1011 ⊕
0000

p4 : 01
00 ⊕
c4 01



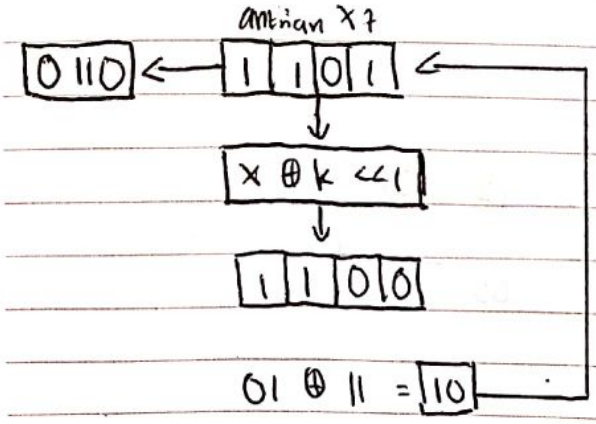
x5 : 1101
k : 1011 ⊕
0110
= 1100

p5 : 00
11 ⊕
c5 : 11



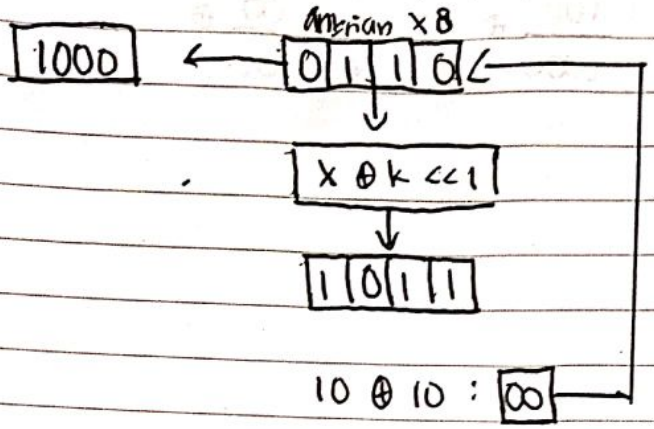
x6 : 0101
k : 1011 ⊕
1110
= 1101

p6 : 11
01 ⊕
c6 : 10



x7 : 1101
k : 1011 ⊕
0110
= 1100

p7 : 01
11 ⊕
c7 : 10

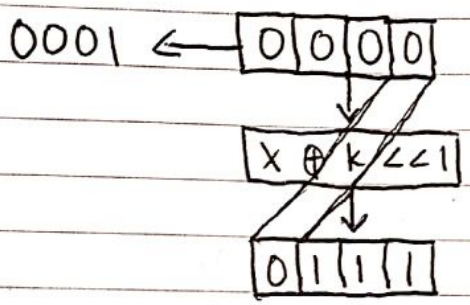


X8 : 0110
1011 ⊕
1101
= 1011

P8 : 10
10 ⊕
C8 : 00

Jadi, hasil enkripsi plainteks CFB
= 00110101 00 11 01 10
= 0101101011010 00

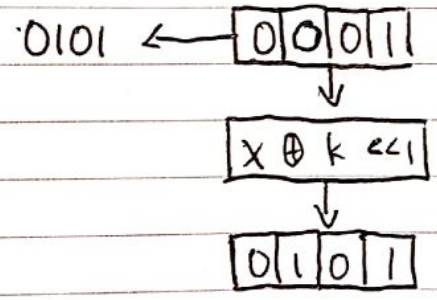
4. Output feedback (OFB)



X1 : 0000
k : 1011 ⊕
1011
= 0111

P1 : 00
01 ⊕
C1 01

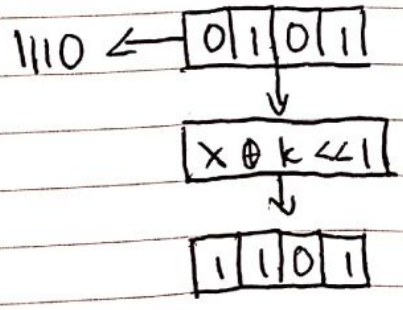
00 ⊕ 01 = 01



X2 : 0001
k : 1011 ⊕
1010
= 0101

P2 : 11
01 ⊕
C2 10

11 ⊕ 01 = 10

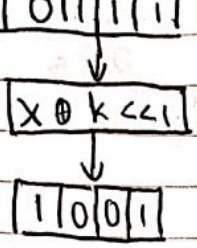


X3 : 0101
k : 1011 ⊕
1110
= 1101

P3 : 01
11 ⊕
C3 : 10

Date

1110 ← 0111

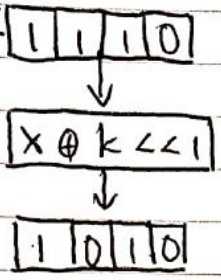


x4 : 0111
k : 1011 ⊕
1100
= 1001

p4 : 01
10 ⊕
c4 11

01 ⊕ 10 = 11

1010 ← 1110

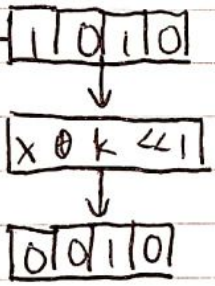


x5 : 1110
k : 1011 ⊕
0101
= 1010

p5 : 00
10 ⊕
c5 10

00 ⊕ 10 = 10

1000 ← 1010

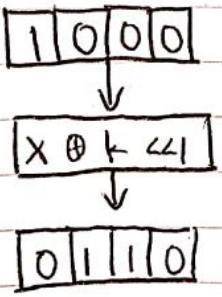


x6 : 1010
k : 1011 ⊕
0001
= 0010

p6 : 11
00 ⊕
c6 : 11

11 ⊕ 00 = 11

0001 1000



x7 : 1000
k : 1011 ⊕
0011
: 0110

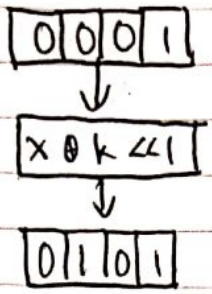
p7 : 01
01 ⊕
c7 00

01 ⊕ 01 = 00

No.

Date

0101



x8 : 0001

k : 1011 ⊕
1010

= 0101

P8 : 10

01 ⊕
e8 : 11

10 ⊕ 01 = 11