Nama : IAN HERLAMBANG
Nim : E1E1 20 010

Tugas 3 Kriptografi

Plainteks : 0011010100110110 / 10 (char)

Block : P_1 P_2 P_3 P_4
Chiper4bit : 0011 0101 0011 0101
Code Hexa : 3 5 3 6

K → 1011
IV → 0000
m → 4
n → 2

1. Electonic code block (ECB)
Enkripsi : $E_K(P) = (P \oplus K) << 1$

$P_1 = 0011$ $P_2 = 0101$ $P_3 = 0011$ $P_4 = 0110$

$K = \frac{1011}{1000}\oplus$ $K = \frac{1011}{1110}\oplus$ $K = \frac{1011}{1000}\oplus$ $K = \frac{1011}{1101}\oplus$

$C_1 = 0001$ $C_2 = 1101$ $C_3 = 10001$ $C_4 = 1011$
Hexa = 1 Hexa = D Hexa = 1 Hexa = B

Hasil enskripsi plainteks = 0011010100110110
= 3b3b (Hexa)
ECB = 0001110100011011
= 1D1B (Hexa)

2. Chiper block chaining (CBC)

$P_1 = 0011$ $P_2 = 0101$ $P_3 = 0011$ $P_4 = 0110$

$IV = \frac{0000}{0011}\oplus$ $IV = \frac{0001}{0100}\oplus$ $IV = \frac{1111}{1100}\oplus$ $IV = \frac{1110}{1000}\oplus$

$K = \frac{1011}{1000}\oplus$ $K = \frac{1011}{1111}\oplus$ $K = \frac{1011}{0111}\oplus$ $K = \frac{1011}{0011}\oplus$

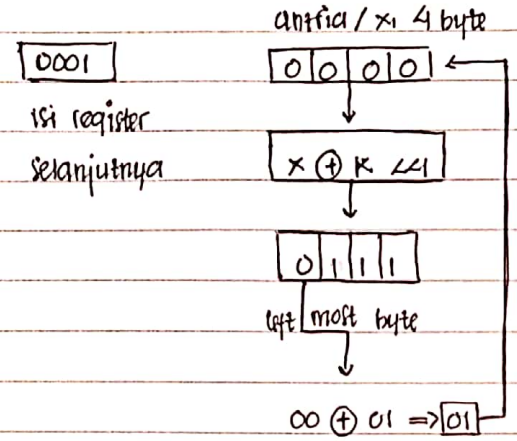
$C_1 = 0001$ $C_2 = 1111$ $C_3 = 1110$ $C_4 = 0110$
Hexa = 1 Hexa = F Hexa = E Hexa = 6

Hasil enskripsi plainteks = 0011 0101 0011 0110
= 3b3b (Hexa)

CBC = 0001111111100110

• 1FE6 (Hexa

3. Chiper feedback (CFB)



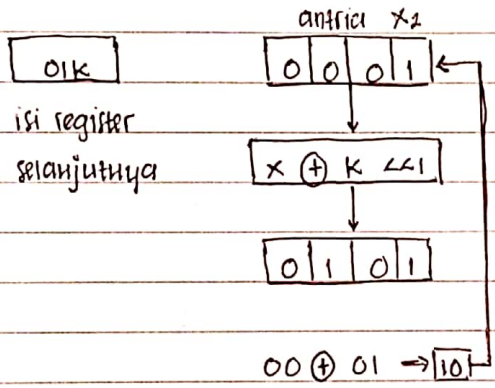
x1 = 0000 P1 = 00

K = 1011 ⊕ 01 ⊕

1011 01

wrapping = 0111 C1 = 01

LMB = 0111

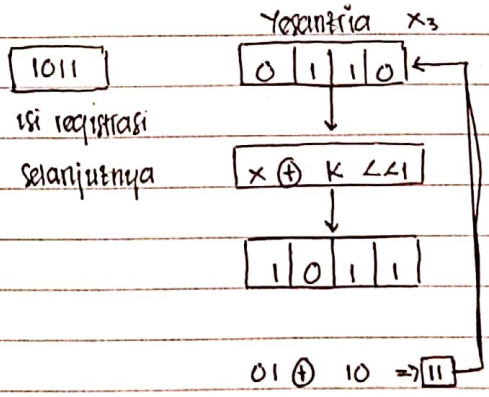


x2 = 0001 PP2 = 11

K = 1011 ⊕ 01 ⊕

1010 C2 10

= 0101

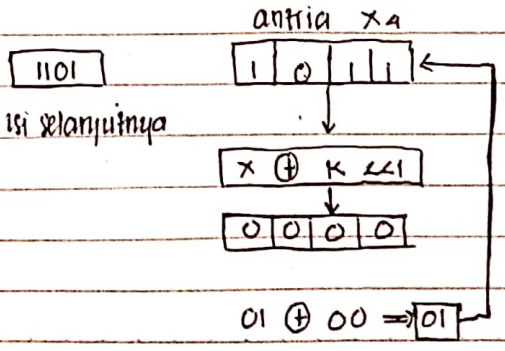


x3 = 0110 PP3 = 01

K = 1011 ⊕ 10 ⊕

1101 C3 11

= 1011

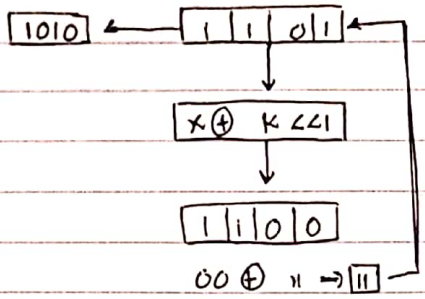


x4 = 1011 P4 = 01

K = 1011 ⊕ 00 ⊕

0000 C4 01

antrian x5



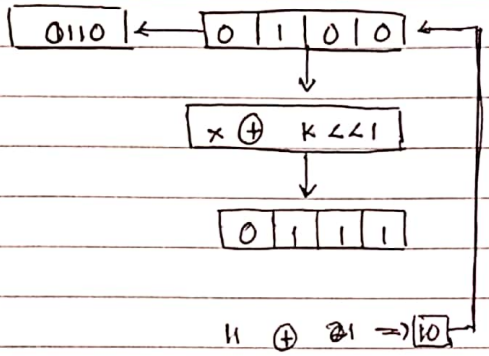
x5 = 1101 P5 = 00

K = 1011 ⊕ 11 ⊕

0110 C5 = 11

= 1100

antrian x6



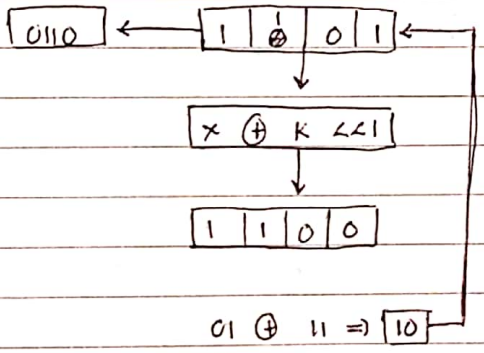
x6 = 0101 P6 = 11

K = 1011 ⊕ 01 ⊕

1110 C6 = 10

= 1101

antrian x7



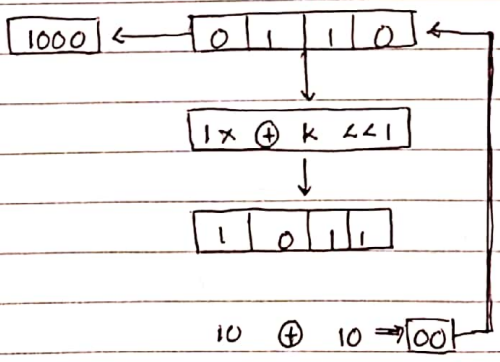
x7 = 1101 P7 = 10

K = 1011 ⊕ 11 ⊕

0110 C7 = 10

= 1100

antrian x8



x8 = 0110 P8 = 10

K = 1011 ⊕ 10 ⊕

1101 C8 00

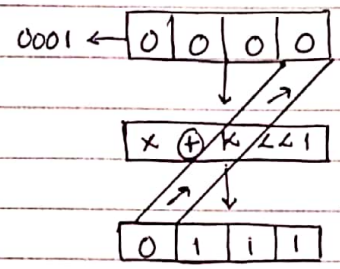
= 1011

Jadi, hasil enskripsi Plainteks

= 0011010100110110

= 0101101011010000

4. Output feedback (OFB)



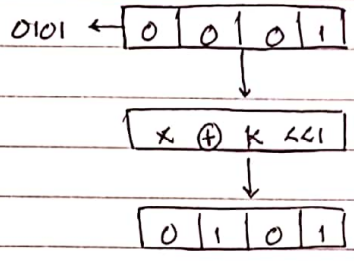
$x_1 = 0000$ $P_1 = 00$

$K = 1011 \oplus$ $01 +$

1011 $C_1 = 01$

$= 0111$

$00 \oplus 01 \Rightarrow 01$



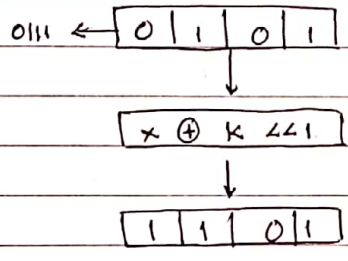
$x_2 = 0001$ $P_2 = 11$

$K = 1011 \oplus$ $01 \oplus$

1010 $C_2 = 10$

$= 0101$

$11 \oplus 01 \Rightarrow 10$



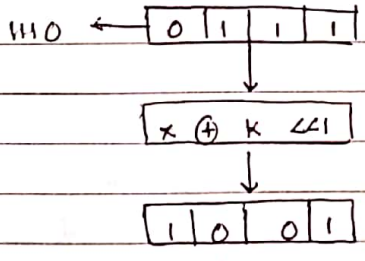
$x_3 = 0101$ $P_3 = 01$

$K = 1011 \oplus$ $11 \oplus$

1100 $C_3 = 10$

$= 1101$

$01 \oplus 11 \Rightarrow 10$



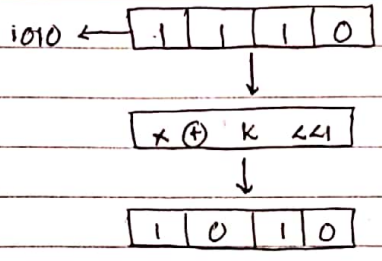
$x_4 = 0111$ $P_4 = 01$

$K = 1011 \oplus$ $10 \oplus$

1100 $C_4 = 11$

$= 1001$

$01 \oplus 10 \Rightarrow 11$



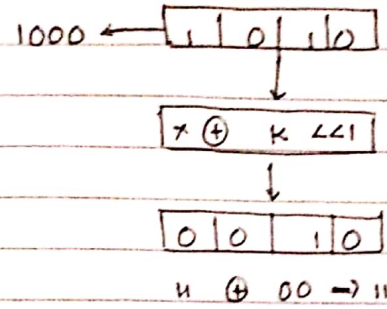
$x_5 = 1110$ $P_5 = 00$

$K = 1011 \oplus$ $10 \oplus$

0101 $C_5 = 10$

$= 1010$

$00 \oplus 10 \Rightarrow 10$



$x_6 = 1010$

$K = 1011 \oplus$

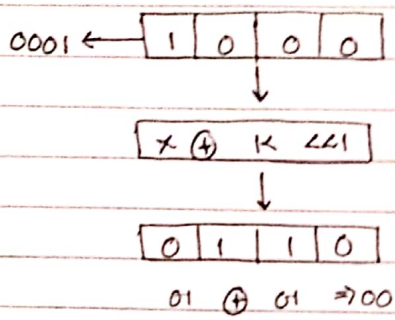
0001

$= 0010$

$P_6 = 11$

$00 \oplus$

$C_6 \quad 11$



$x_7 = 1000$

$K = 1011 \oplus$

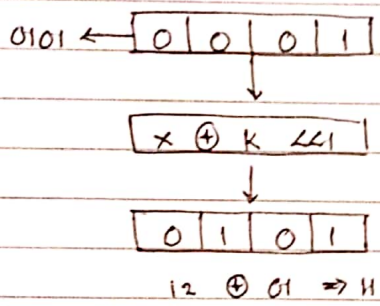
0011

$= 0110$

$P_7 = 01$

$01 \oplus$

$C_7 = 00$



$x_8 = 0001$

$K = 1011 \oplus$

1010

$= 0101$

$P_8 = 10$

$01 \oplus$

$C_8 = 11$