Nama : Andi Sri Mulyani
Nim : 212126
Kelas : 5 TKKO - F

1. Chipertext dalam mode EBC dan CBC (4 bit)
2. Deskripsikan chipertext kembali ke plaintext.

Jawaban :

1. Plaintext = 33C9E : 0011 0011 1100 1001 1110
   Kunci (K) : 6 = 0110
   - Mode EBC
     Enkripsi : 0011 0011 1100 1001 1110
     Kunci 0110 0110 0110 0110 0110 ⊕
     hasil XOR 0101 0101 1010 1111 1000
     geser 1 bit kekiri 1001 1010 1101 1111 0001
     dalam notasi hexa 9 A D F 1
     jadi, hasil enkripsi : 1001 1010 1101 1111 0001 (9ADF1 dalam notasi hexa)

   - Mode CBC
     * $C_1 = P_1 \oplus C_0 = 0011 \oplus 0000 = 0011$
     $= 0011 \oplus K = 0011 \oplus 0110 = 0101$ geser 1 bit kekiri : 1010
     jadi, C_1 : 1010 (A dalam notasi hexa)

     * $C_2 = P_2 \oplus C_1 = 0011 \oplus 1010 = 1001$
     $0011 \oplus K = 0011 \oplus 0110 = 0101$ geser 1 bit kekiri : 1010
     jadi, C_2 : 1010 (A dalam notasi hexa)

     * $C_3 = P_3 \oplus C_2 = 1100 \oplus 1010 = 0110$
     $1100 \oplus K = 1100 \oplus 0110 = 1010$ geser 1bit ke kiri : 0101
     jadi, C_3 : 0101 (5 dalam notasi hexa)

     * $C_4 = P_4 \oplus C_3 = 1001 \oplus 0101 = 1100$
     $= 1001 \oplus K = 1001 \oplus 0110 = 1111$ geser 1 bit kekiri : 1111
     jadi, C_4 : 1111 (F dalam hexa)

     * $C_5 = P_5 \oplus C_4 = 1110 \oplus 1111 = 0001$
     $= 1110 \oplus K = 1110 \oplus 0110 = 1000$ geser 1 bit ke kiri 0001
     jadi, C_5 : 0001 (1 dalam notasi hexa)

jadi hasil enkripsi : 1010 1010 0101 1111 0001 (AA5F1 dalam notasi hexa)

2. - Mode ECB

Dik : chiperteks : 9 A 9 F 1

: 1001 1010 1101 1111 0001

kunci : 0110

c : 1001 1010 1101 1111 0001

geser 1 bit ke kanan : 1100 0101 1110 1111 1000

c : 1100 0101 1110 1111 1000

0110 0110 0110 0110 0110 ⊕

1010 0011 1000 1001 1110

hexa : A 3 8 9 E

jadi hasil deskripsi : 1010 0011 1000 1001 1110 (A3 8 9E dalam notasi hexa)

* mode CBC

dik : chiperteks : AA5F1

: 1010 1010 0101 1111 0001

kunci (k) : 0110

c : 1010 1010 0101 1111 0001

k : 0110 0110 0110 0110 0110

- C_1 : 1010

geser ke kanan : 0101

: 0101 ⊕k : 0101 ⊕ 0110 : 0011

→ P_1 : 0011 ⊕ C_0 : 0011 ⊕ 0000 : 0011 (3 dalam notasi hexa)

- C_2 : 1010

geser ke kanan : 0101

: 0101 ⊕k : 0101 ⊕ 0110 : 0011

: 0011 ⊕ C_1 : 0011 ⊕ 0011 : 0000 (0 dalam notasi hexa)

- C_3 : 0101

geser ke kanan : 1010

: 1010 ⊕k : 1010 ⊕ 0110 : 1100

: 1100 ⊕ C_2 : 1100 ⊕ 0000 : 1100 (C dalam notasi hexa)

- C_4 : 1111

geser ke kanan : 1111

: 1111 ⊕k : 1111 ⊕ 0110 : 1001

: 1001 ⊕ C_3 : 1001 ⊕ 1100 : 0101 (5 dalam notasi hexa)

- C_5 : 0001

geser ke kanan : 0001 ⊕ k : 0001 ⊕ 0110 : 0111

: 0111 ⊕ C_4 : 0111 ⊕ 0101 : 0010 (2 dalam notasi hexa

jadi hasil deskripsi : 0011 0000 1100 0101 0010 (30C52 dalam notasi hexa)