University Djilali Bounaâma of Khemis-Miliana
Department of Mathematics and Computer Science
L3 – Computer Systems (S6)
Retake Examination – Computer Security & Cryptography / Correction
May 2025

Exercise 1 (12 pts): Consider the following block cipher mode encryption formulas. For each, we have an encrypted bitstream **S**.

a. $\boldsymbol{C_i = E_k(P_i \oplus P_{i-1} \oplus C_{i-1})}$ **- S = 111100111110**

b. $\boldsymbol{C_i = E_k(P_i \oplus C_{i-1})}$ **- S = 111010011111**

c. $\boldsymbol{C_i = E_k(C_{i-1}) \oplus P_i}$ **- S = 100001011111**

1) Identify the block cipher mode corresponding to each formula. (1.5 pt)

   a- PCBC

   b- CBC

   c- CFB

2) Provide the decryption formula for each case. (03 pts)

   a- $\boldsymbol{P_i = D_k(C_i) \oplus (P_{i-1} \oplus C_{i-1})}$

   b- $\boldsymbol{P_i = D_k(C_i) \oplus C_{i-1}}$

   c- $\boldsymbol{P_i = E_k(C_{i-1}) \oplus C_i}$

3) Using the following cipher table and the initialization vector (IV), decrypt the encrypted bitstreams (Use decryption diagrams to illustrate your decryption process): (7.5 pts)

   Cipher table **IV = 101**

   000 ⇒ 111

   001 ⇒ 110

   010 ⇒ 101

   011 ⇒ 100

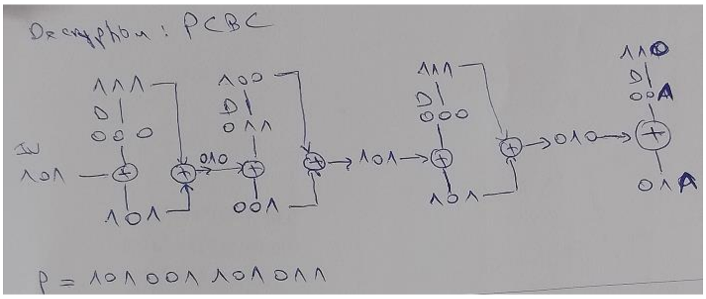
   100 ⇒ 000

   101 ⇒ 001

   110 ⇒ 010

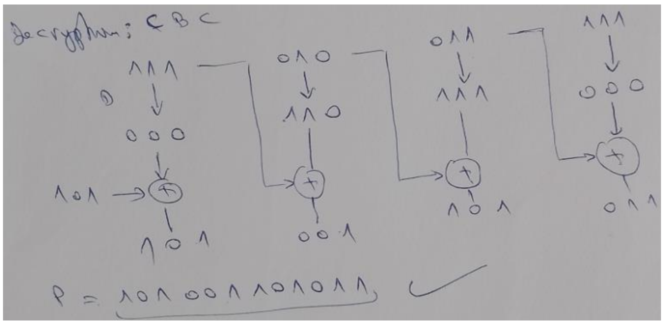
   111 ⇒ 011

a. PCBC (S = 111100111110)



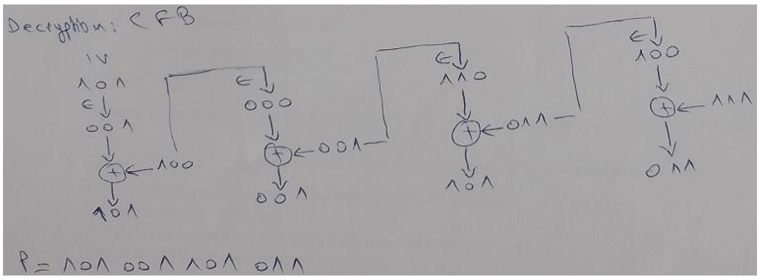
Plaintext = 101001101011

b. CBC (S = 111010011111)



Plaintext = 101001101011

c. CFB (S = 100001011111)



Plaintext = 101001101011

Exercise 2 (08 pts):

1) Arrange the following Block Chain transaction operations in the correct sequence and briefly describe each operation: (3.75 pts)

- A. Adding / B. Transaction / C. Validation / D. Reception / E. Grouping

Right order:

B. Transaction: **A** makes a transaction to **B**

E. Grouping: Several transactions are grouped into a block

C. Validation: The block is validated by the network nodes using cryptographic techniques

A. Adding: The block is dated and added to the blockchain to which all users have access

D. Reception: **B** receives the transaction from **A**

2) Order the following AES encryption steps correctly and provide a short explanation for each: (4.25 pts)

- A. Row shift / B. Column scrambling / C. Nonlinear byte transformation / D. Addition of the secret key / E. Addition of the round key

Right order:

D. Addition of the secret key: The secret key is added by a XOR to the plaintext block

C. Nonlinear byte transformation: The 128 bits are divided into 16 blocks of 8 bits, themselves distributed in a 4×4 table. Each byte is transformed by a nonlinear function S

A. Row shift: The last 3 rows are shifted cyclically to the left: the 2nd row is shifted by one column, the 3rd row by 2 columns, and the 4th row by 3 columns

B. Column scrambling: Each column is transformed by linear combinations of the different elements of the column (i.e: multiplying the 4×4 matrix by another 4×4 matrix)

E. Addition of the round key: At each round, a round key is generated from the secret key by a sub-algorithm. This round key is added by a XOR to the last block obtained