October University for Modern Sciences & Arts

Mid Term Exam Answer

Faculty	**Engineering**
Department	**Electrical Communication and Electronics Systems Eng.**
Module Code	**ECE5432/ECE5632**
Module Title	**Cryptography**
Semester	**Spring 2023**
Time Allowed	**90 minutes**
Total Mark	**20**
No. of Pages	**4 (including the cover page)**
Material provided	**None**
Equipment permitted	**No programmable calculator**
Additional Instructions	**None**

No books, paper or electronic devices are permitted to be brought into the examination room other than those specified above.

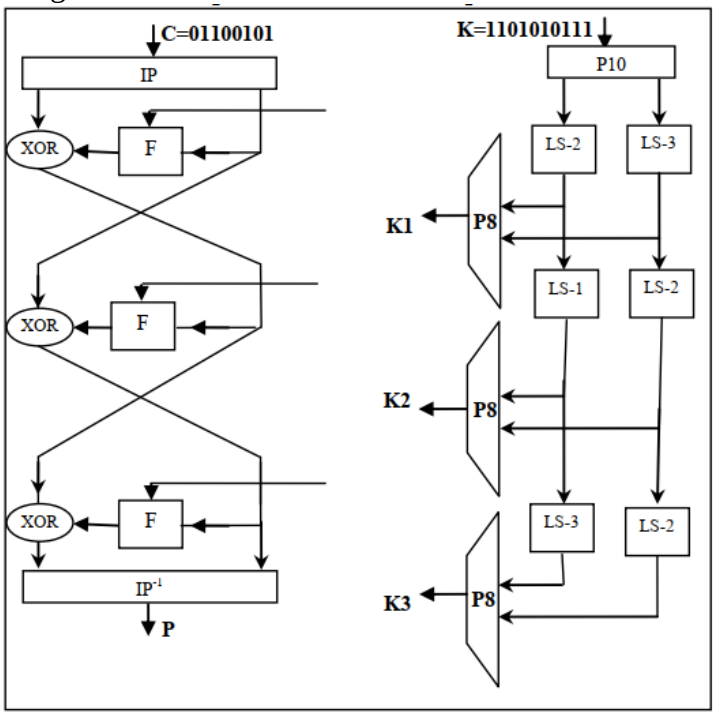
October University for Modern Sciences and Arts

Faculty of Engineering
Module Code: ECE5432/ECE5632
Module Title: Cryptography
Semester: Mid Term Exam – Spring 2023

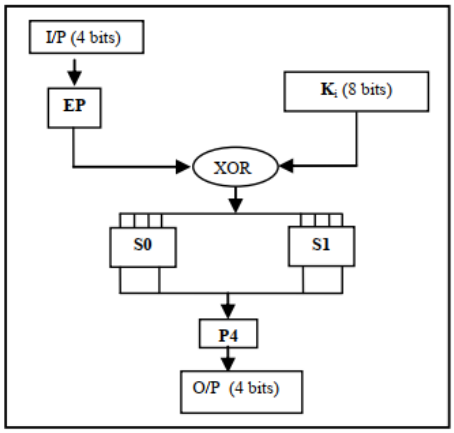
Answer all of the following questions:

Question (1): [10 Marks]

A) Consider the Simplified-DES block-cipher shown on the left with the F function shown on the right:



The function F:



The following information is also given:

IP = [7 8 6 4 5 3 1 2],
P8=[1 4 3 2 7 6 5 10],
EP =[4 1 2 3 2 3 4 1],
P4 = [2 1 4 3],
P10 = [10 9 8 7 6 5 3 4 1 2]

	S_0 Column Number			
Row No.	0	1	2	3
0	1	0	2	3
1	3	1	0	2
2	2	0	3	1
3	1	3	2	0

	S_1 Column Number			
Row No.	0	1	2	3
0	0	3	1	2
1	3	2	0	1
2	1	0	3	2
3	2	1	3	0

The block cipher is used to **decrypt the ciphertext C**. Satisfy the following:

1. Find the sub-keys K1, K2 and K3. **[2pt]**
2. Compute the output of F for decryption, in the first, second and in the third round. **[6pt]**
3. Find the inverse permutation IP^{-1} of IP. **[1pt]**
4. Compute the plaintext P. **[1pt]**

k1= 11101111

k2= 01110011

k3= 11011110

IP out= 01100101

EP Output= 10101010

S-Boxes Output(Before P4)= 1001

Output of F = 0110

1st round Out(Before switching)= 00000101

EP Output= 00000000

S-Boxes Output(Before P4)= 1010

Output of F = 0101

2nd round Out(Before switching)= 00000000

EP Output= 00000000

S-Boxes Output(Before P4)= 0100

Output of F = 1000

3rd round Out= 10000000

P = 00000010

Question (2): **[10 Marks]**

A) Consider the Affine cipher encryption function: $y = (a.x + b) \bmod 26$, $x = a^{-1} (y - b) \bmod 26$
Where, y is the ciphertext and x is the plaintext.

1. Given a= 3, b =8, Decrypt the following ciphertext: *UACBN* **[2pt]**
2. Is the Affine cipher secure? Explain why or why not. **[1pt]**

1. Plaintext: Egypt
2. No. Fixed mapping and small key space. Vulnerable to brute force, frequency analysis, and known-plaintext attacks.

B) A block cipher with block-length (n =64 bits) is used in the CFB mode of operation with block segment (s = 8 bits). Compute the error propagation in bits if the first ciphertext bit is in error. **[2pt]**

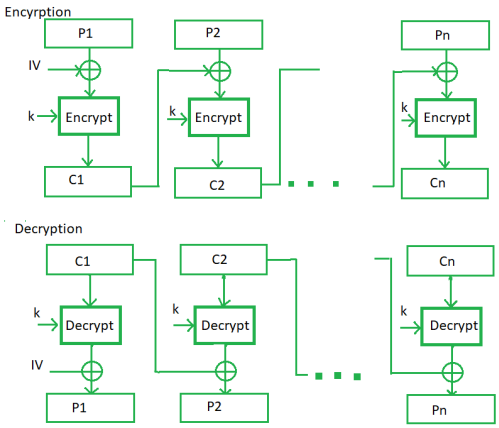
The error is in the first bit of ciphertext i.e. in C1
The error propagates as long as C1 still in the shift register.
No. of rounds that C1 stays inside the shift register = n/s = 8
But as the error was in the first bit (left-most bit of C1), it won't affect the 4th round. So, we have only 8

blocks with errors as well as one bit error in the first block (P1) resulting from the bitwise XOR with C1.
Finally, the total number of error bits = (8)(64) + 1 = 513 bits.

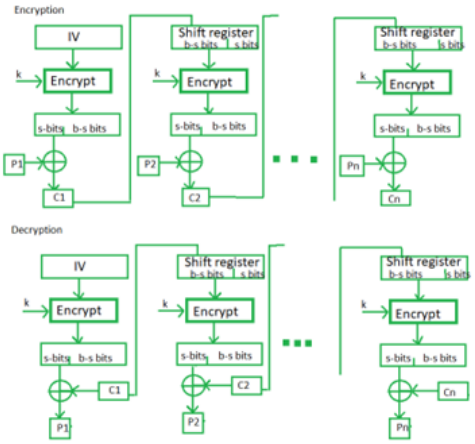
C) Compare between CBC and CFB modes of operation of block ciphers. Your comparison must satisfy the following:

1. Block diagrams of Encryption/Decryption for each mode. **[4pt]**

CBC



CFB



2. The possibility of preprocessing and random access in each mode. **[1pt]**

- CBC >> preprocessing: Not Allow. And allows random access to ciphertext
- CFB >> preprocessing: Not Allow. And Allows random access to ciphertext

Best Wishes
Dr. Farah Raad