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 2024**
Time Allowed	**90 minutes**
Total Mark	**20**
No. of Pages	**3 (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.

Answer all of the following questions:

Question (1): **[10 Marks]**

A) What is the output of the first round of the DES algorithm when the plaintext and the key are both all ones? **LO2** **[6pt]**

Answer :

Assume the input string X to be ones (64 bits) and K = ones (56 bits).

Having L0 = ones (32), and R0 = ones (32) after the initial permutation of X. Since, there is no effect of the initial permutation.

And after the fixed permutation of X, having round key K1 as ones (48).

The formula for obtaining the value of R1 through round 1 is as follows:

R1 = L0 XOR f (R0, K1)

In the above formula, the function *f* refers to Feistel function.

- As per the fixed permutation expansion rule, expand R0 to 48-bit string.
- Since, all the bits in the string R0 are 1, therefore, after expansion also the string R0 will contain all ones.
- This expanded R0 string will be XORed with K1.
- Since, both the key K1, and the string R0 are all 1's therefore, the XOR operation results in a string of zeroes of 48 bits.
- After this, the resultant string of 48 bits is divided into the 6 bits chunks. The *ith* bit will be transformed as per the rule of Si box. 000000 is being mapped 8 times with the Si box where $i = 1, \ldots, 8$.
- And this will produce the sequence of 14, 15, 10, 7, 2, 12, 4, 13.

Hence, the binary representation of the above sequence is as follows:

1110 1111 1010 0111 0010 1100 0100 1101

At last these bits is being permutated as per the P table:

1101 1000 1101 1000 1101 1011 1011 1100

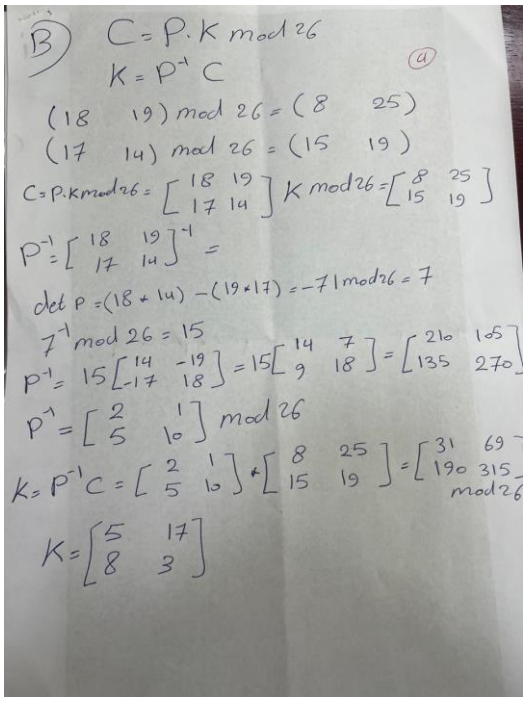
The result of the function f ((R0), K1) will be:
1101 1000 1101 1000 1101 1011 1011 1100
Now, R1 = L0 XOR f (R0, K1)
L0 = 1111 1111 1111 1111 1111 1111 1111 1111
f ((R0), K1) = 1101 1000 1101 1000 1101 1011 1011 1100
Hence, R1 = 0010 0111 0010 0111 0010 0100 0100 0011

The final result of the Round 1 = L1 + R1
L1 = R0 = (11 ... 1) (These are 32 ones).
After combining both the bits, the resultant bits are 64 in number and this is the result of round 1.
1111 1111 1111 1111 1111 1111 1111 1111 0010 0111 0010 0111 0010 0100 0100 0011

B) We are assuming that we have a ciphertext message was that encrypted using a 2 × 2 Hill cipher. Suppose that ciphertext "izkuizptjfhxrxwmvfexre" corresponds to plaintext "staystrongforyourself". Get Key **LO1&LO3** **[4pt]**

Answer :

5 17
8 3



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

A) Consider the Affine cipher encryption function: y = (a.x + b) mod 26 , x= a^{-1} (y - b) mod 26
Where, y is the ciphertext and x is the plaintext. **LO2 & LO3**

1. What are the limitations on the values of a, and b? **[1pt]**
2. Is the Affine cipher secure? Explain why or why not. **[1pt]**
3. Given a= 5, b =8, Decrypt the following ciphertext: **MaaxQapvwvm** **[2pt]**

Answer :

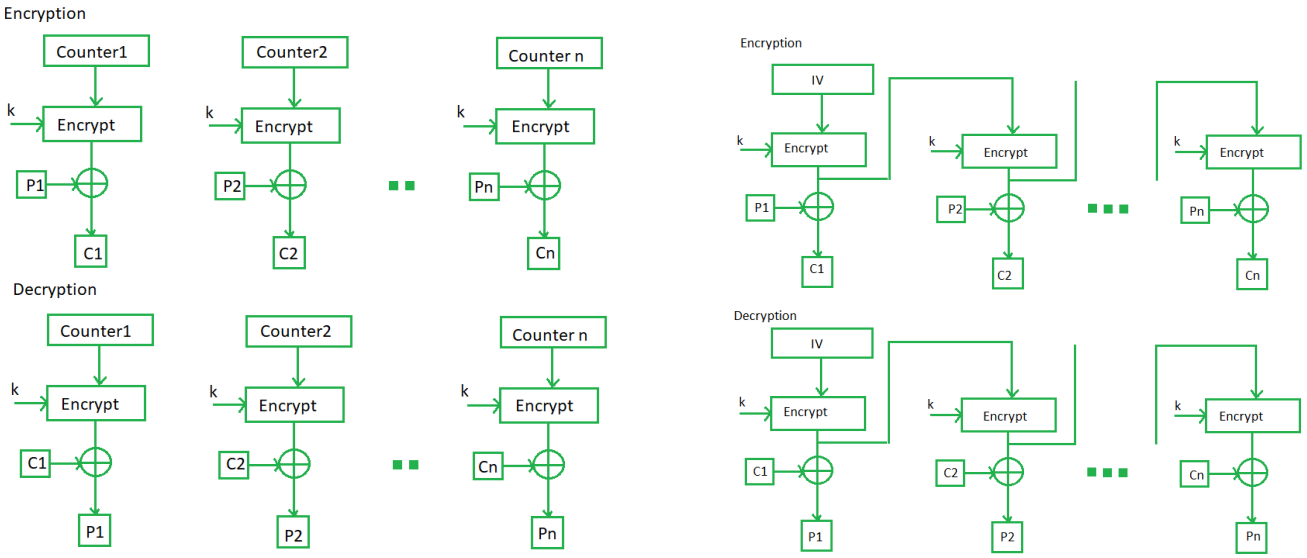
1. Since the alphabet is 26 characters, the value of b can only be 26. Thus, there are only 312 (12 * 26) keys possible. Additionally, if only 2 characters of the original text are known, the cipher can be cracked using a system of equations.
   An affine cipher has two parts to its key – an additive part b (the shift) and a multiplicative part m (the decimation interval). There are 26 Caesar ciphers; so, there are 26 choices for b. For each of those 26 choices for the additive key, there are 12 possible choices for the multiplicative key m.
2. No! The key space is only a bit larger than in the case of the shift cipher:
   key space = (#values for a)×(#values for b)
   = 12×26 = 312
   Again, several attacks are possible, including: Exhaustive key search and letter frequency analysis, similar to the attack against the substitution cipher.
3. GoodMorning

B) Compare between CTR and OFB modes of operation of block ciphers. Your comparison must satisfy the following: **LO2**

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

Answer :

CTR **OFB**



2. The capability for parallel processing and random access in each mode. **[2pt]**

Answer :

CTR : parallel processing **Yes** in Encryption and decryption

random access **Yes**

OFB: parallel processing **NO**

random access **NO**

Best Wishes

Dr. Farah Raad