CS DEPT
MILITARY COLLEGE OF SIGNALS, NUST
CPS-425 NETWORK SECURITY
BESE-14

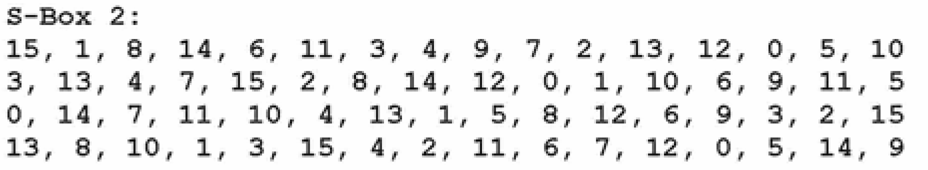
Exam:	Midterm	**Instructor:**	Dr. Faisal Bashir
Type of Paper:	Regular	**Total Marks:**	30
Semester:	Spring	**Time Allowed:**	90 mins

Instructions:

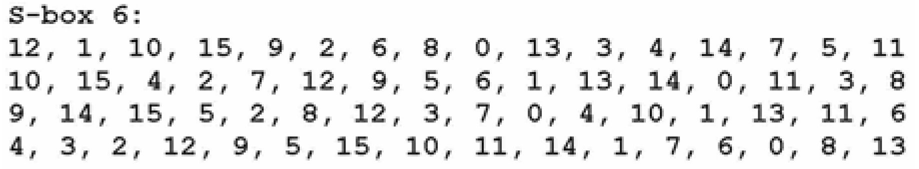
1. Attempt all questions
2. Write your Index # on question paper and answer book.
3. Please write neatly and number questions and subparts carefully.
4. If a question is unclear, state your assumptions and answer the problem based on your assumptions.
5. Understanding the question is also a part of the examination.

Q1. During the enciphering of a message using DES algorithm, the following 48 bit data is input to the S-boxes. For this input find the binary output of S-box 2 and 6.

11010101 01010111 11110101 11010000 00010101 11011111 **[2+2]**



S-Box 2:
15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10
3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5
0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15
13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9



S-box 6:
12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11
10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8
9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6
4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13

Q2. During the enciphering process the following matrix is obtained using AES algorithm after substitution is performed on the input message. **[2+5]**

Message after substitution:

53	CA	70	0C
B7	D6	DC	D0
F8	32	51	04
79	63	BA	68

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

You are required to perform the following operations on the above data.

a. Shifting of Rows

b. The first two bytes (in hexadecimal) obtained after applying Mix Column Transformation.

Q3. Suppose an adversary listen to an encrypted communication and some how finds that cipher text 58 corresponds to a plain text 16. Moreover, he learns that RSA algorithm was used for the encryption of the message and the public key used was (7, 77). Find the private key based on the known information. **[6]**

Q4. The following cipher is obtained using PlayFair Cipher algorithm. **[6]**

SHBWHRMXXEWPMCICRDSHIC

Find the plaintext if the key is: MIDTERM EXAM

Q5. With the help of a small network diagram, explain how ICMP based route spoofing attack can be launched. What measures should be taken to avoid such attacks. **[5]**

Q6. Suppose a 456723 bits message is given/input to the SHA-512 algorithm. For this message find the following **[2]**

a. Number of padding bits to be appended

b. Number of blocks in which the message will be broken