MANIPAL ACADEMY OF HIGHER EDUCATION
MANIPAL SCHOOL OF INFORMATION SCIENCES

THIRD SEMESTER MASTER OF SCIENCE – M.Sc. (INFORMATION SCIENCE) DEGREE
EXAMINATION – DECEMBER 2020

SUBJECT: MIS 607 – COMPUTER INFORMATION SECURITY

Monday, 7ᵗʰ December 2020

Time: 10.00 – 13.00 Hrs.   Max. Marks: 100

✎ **Answer ALL the questions**

All questions carry 10 marks.

1. Define the following terminologies:
   a. Data confidentiality
   b. Data integrity
   c. Availability
   d. Non- Repudiation

   (4x2.5=10 Marks)

2. Decrypt the cipher text message LPDPH LVDZL FRQTX HUHG, which has been encrypted using Caesar Cipher.

   Explain the working principle of One-time Pad with appropriate example.

   (3+7=10 Marks)

3. a. Compare Stream cipher with Block cipher

   b. Explain the modes of operation of Block Cipher and explain the functioning of any one block in detail

   (3+7=10 Marks)

4. a. Use the following S-Table for DES to compute the values.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

The input for S box is given below find the output 011010 and 110010

b. Explain how the Integrity are achieved through Symmetric crypto (MAC)

(3+7 =10 Marks)

5. Explain the working principle of Knapsack crypto system with an example.

(10 Marks)

6. Explain the usage of hash function in the online bidding and Spam reduction

(3+7 =10 Marks)

7. Briefly explain the terms
    a. Man-in-the-Middle attack
    b. Worm
    c. Logic Bomb
    d. Race Condition   (4x2.5=10 Marks)

8. a. Explain the significance and working of password with salt.

    b. Explain confused deputy scenario and way to overcome the issue

(5x2=10 Marks)

9.   List out the importance of securing a database. Explain the techniques to overcome inference from database with an example.

10. Explain Kerberos in detail.

******