JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS-Apr 2025

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARKS: 25

COURSE NAME: INFORMATION SECURITY

COURSE INSTRUCTORS: **Dr. Praveen Modi** MAX. TIME: 1:30 Hr

Note: *All questions are compulsory. Marks are indicated against each question in Marks column. Write the answer of the question belonging to the same part in the same order. Needed tables are provided in the next page.*

Q. No	Question	CO	Marks
Q1.	Write a brief note on following? a) Triple DES b) Meet In the Middle attack c) Counter Mode of operation d) Avalanche Effect	3	2 2 2 2
Q2	Consider the AES technique to perform the following operation (at first round) for the given plaintext and key (Hexadecimal)? P: EA 83 5C F0 04 45 33 2D 65 5D 98 AD 85 96 B0 C5 Key FF 0B 84 4A 08 53 BF 7C 69 34 AB 43 64 14 8F B9 (i) Substitute Bytes (ii) Shift Rows for output of step (i) (iii) Mix Column for index position (2,1) using predefined matrix for output of step (ii) (iv) Generate the Round key w4 using RC = 01 00 00 00.	3	2 2 2 5
Q3	Consider the DES technique to perform the following operations at any round for the given intermediate text and key (Hexadecimal)? Note: No need to perform any initial permutation. Expand the 4 bit to 6 bit by repeating the second right bit at extreme bit positions. Plaintext: D E 7 F 0 3 A 6 Key 1 2 D E 5 2 (i) Feistel function as XOR. (ii) S-Box for the output of step (i) (iii) Generate the intermediate cipher text using step (ii)	3	2 2 2

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2																
3																
4																
5																
6																
7																
8																
9																
A																
B																
C																
D																
E																
F																

AES_S-Box

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

AES_ Pre-defined- Matrix

00	01	10	11	10	01	00	11	00	01	11	00	11	00	01	10
10	01	00	11	00	11	01	00	11	00	01	10	11	10	01	00
11	00	01	10	11	10	01	00	10	01	00	11	00	11	01	00
01	00	11	10	01	10	11	00	01	00	00	11	00	11	01	10

DES_ S-Box