JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS-MAY 2025

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARKS: 35

COURSE NAME: INFORMATION SECURITY

COURSE INSTRUCTORS: **Dr. Praveen Modi** MAX. TIME: 2:00 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	Mark
1.	a) Which type of active attack may be possible in the following scenarios? 1. Network address translation at IP layer 2. Stealing of session cookies at application layer 3. Multiple SYN packets at TCP	1	3
	b) Encrypt the following message using Hill ciphering method? Assign the index A=0....Z=25 Message: "JUIT" key = $\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$	2	4
2.	a) Write a brief note on following: 1. Cipher Block Chaining Mode 2. Double DES method with the encountered problem.	3	3
	b) Consider the DES encryption technique to perform the following operations at any round for the given plain text and key (Hexadecimal)? Note: No need to perform any initial permutation. Expand the 4 bits to 6 bits of input plaintext by repeating 1st bit at the extreme bit positions.	3	
	P: F E D C 1 2 3 4 K: C 1 B 6 2 A		
	1. Fiestel function as XNOR.		2
	2. S-Box for the output of step (i)		3
	3. Generate the intermediate cipher text for the output of step (ii)		2
	c) Consider the AES technique to generate the key $[w_4\ w_5 w_6 w_7]$ for first round using RC = 02 00 00 00? AB 7C BF 64 43 8D 7C 14 8F 69 FF 08 B9 34 0B 53	3	4
3.	Consider an Elgamal cryptosystem. Let Alice wants to send a message M = "JUIT" to Bob using Bob's public key [q=19, α = 10, Y_B = 3]. What will be encrypted message if Alice chooses random	4	5

	integer k = 6? Assign the index A=0, B=1....Z=25.		
4.	Draw the block diagram to achieve the security mechanism e.g. authentication using message authentication code? a) Authentication is tied to plaintext b) Authentication is tied to cipher text	4	4
5.	Write a brief note on following: a) Worms b) Trojans c) Ransom ware d) Adware e) Fileless malware	5	5

Table 1: AES S-Box

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 2: DES_ S-Box

0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011
0010	0011	0100	0101	1001	1010	1011	1100	1101	1110	1111	0000	1000	1001	1010	0001
0101	0110	0010	0011	0111	1000	1001	1010	0100	0101	1100	1101	1001	1010	0111	1000