JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- 2024

M.Tech-I Semester

COURSE CODE (CREDITS): 161WCI122 (3) MAX. MARKS: 15

COURSE NAME: Cryptography and Information System Security

COURSE INSTRUCTORS: Er. NITIKA MAX. TIME: 1 Hour

Note: (a)*All questions are compulsory.*

(b)Marks are indicated against each question in square brackets.

(c) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

---

Q1. How does the OSI Security Architecture assist in developing a comprehensive security policy for a network? Provide examples of how specific layers address different security concerns. [5 Marks]

Q2. What is a Galois Field? Consider the finite field GF (3), where all arithmetic operations are performed modulo 3. [3 Marks]

Q3. Consider the numbers 103 and 55. Use the Extended Euclidean Algorithm to find:

1) The greatest common divisor (GCD) of 103 and 55.

2) The integers x and y such that 103x+55y=GCD (103, 55). [3 Marks]

Q4. Explain AES algorithm by using Plain text: "Two One Nine Two" and key: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

1) Perform the SubBytes transformation for the first round.
2) Perform the ShiftRows transformation for the first round.
3) Perform the MixColumns transformation for the first round.
4) Generate the first round key using the given 128-bit key.
5) Perform the AddRoundKey operation for the first round. [4 Marks]

JUIT TEST-1 EXAMINATION- Sep 2024

		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

JUIT TEST-1 EXAMINATION- Sep 24