VIT
Vellore Institute of Technology

School of Computer Science and Engineering

Fall Semester 2024-25

Continuous Assessment Test – I

SLOT A1

Programme Name & Branch: 5 Year Integrated M. Tech (MIC, MID)

Course Name & Code: Applied Cryptography and Network Security & CSI3002

Class Number (s): Applicable to all

Faculty Name (s): Dr. S M Farooq, Dr. Nivitha K, Dr. Thangaramya K and Dr. Sunil Kumar

Exam Duration: 90 Min. **Maximum Marks: 50**

General instruction(s):

1. Students are allowed to use a straightforward non-programmable scientific calculator in the examinations.
2. Exchange of calculators is strictly prohibited.

Answer All the Questions.

Q. No.	Question	Max Marks
1.	a) Suppose that everyone in a group of N people wants to communicate secretly with N-1 others using symmetric key cryptographic system. Communication between either of two people should not be decodable by others in the group. Explain about the number of keys required in the system to satisfy the confidentiality requirement.	3
	b) Denial of Service (DoS) attack compromises Availability (security requirement) by flooding dummy packets. In the same way can a replay attack also compromise Availability?	2
	c) Explain different types of security attacks and discuss about how they are threat to security goals.	5
2.	a) The extended Euclidean algorithm computes integers x and y such that, ax+by=gcd(a,b). If the given values of a=1398 and b=324, find x and y values.	5
	b) Find the remainder for $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ mod 7 using Fermat's Little Theorem.	5
3.	Suppose Alice and Bob use an Elgamal scheme with a common prime q = 157 and a primitive root $\alpha = 5$. i. If Bob has public key YB = 10 and Alice chose the random integer k = 3, what is the ciphertext of M = 9? ii. If Alice now chooses a different value of k so that the encoding of M = 9 is C = (25, C2), what is the integer C2?	10
4.	Draw an architecture of RC4 algorithm and discuss the process of initialization, initial state permutation, key stream generation and encryption in detail.	10
5.	Find the fourth round-key of AES-128 using the following third round key which is given in hexadecimal, S-Box table and round constant 08.	10

Third Round Key

2C	A5	F2	43
5C	73	22	8C
65	0E	A3	DD
F1	96	90	50

AES S-Box Table

		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	4D	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