BI/K/TX

Reg. No: [redacted]

Final Assessment Test – November 2024

VIT
Vellore Institute of Technology

Course: CSI3022 - Cyber Security and Application Security

Class NBR(s): 1961/1962 Slot: C1+TC1

Time: Three Hours Max. Marks: 100

- ➢ KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- ➢ DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions

(10 X 10 = 100 Marks)

1. a) State Euler's theorem to find the modulus of the positive number. Apply it to find a number *x* between 0 and 14 such that x is congruent to 7^{126}modulo 15. Show the results of every step and the final x value. [5]

   b) State the Fermat's theorem and its use in finding the Modulus of the positive number. Find 4^{227} mod 13 using Fermat's theorem. [5]

2. A collective of 13 artists uncovers a trove of paintings. When they attempt to divide the paintings, they find that 6 are left over. When 11 artists agree to divide the paintings, they find that 4 painting remain after their division. When 7 artists agree to divide the paintings, they find that 5 left over. What is the minimum number of paintings in the trove?

3. Describe the security services defined in OSI Security Architecture. How do these services support the overall security objectives of authentication, confidentiality and integrity?

4. Consider the plaintext = 11011100 and key = 1010001110. Implement SDES algorithm and perform the following

   i) Compute the keys K1 and K2 required for each round of computation [5]

   ii) Encrypt the plaintext and find the cipher text. Show all steps in the computation and the result of each round. [5]

S0

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S1

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

IP	2	6	3	1	4	8	5	7		
IP^{-1}	4	1	3	5	7	2	8	6		
P10	3	5	2	7	4	10	1	9	8	6
P8	6	3	7	4	8	5	10	9		
Expanded Permutation			4	1	2	3	2	3	4	1
P4	2	4	3	1						

5. The following four words corresponding to the input key in Advanced Encryption Standard (AES) that uses a 128 bit key are W0, W1, W2 and W3.

W0 – 40 C2 A2 33

W1 – 21 02 40 21

W2 – 63 03 B5 13

W3 – 12 61 22 34

Discuss the key expansion procedure and determine the next four words W4, W5, W6 and W7 that will be derived from W0, W1, W2 and W3 to be used in the encryption process. Show all the steps that led to the result in your answer.

j	1	2	3	4	5	6	7	8	9	10
RC(j)	01	02	04	08	10	20	40	80	1B	36

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

6. a) Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on q=17 and α=5. Party A chooses 4 and party B chooses 6 as their respective private keys. Find the secret session key utilized between these parties for further communications. [7]

b) Compare the trade-offs between using symmetric and asymmetric encryption. [3]

7.a) Assume your friend Mr. Ramana is working on his laptop when he suddenly sees a pop-up window that states "Warning! Virus detected, 10 viruses detected. Click here to fix the problem immediately!" The pop-up is brightly colored and includes a countdown timer. Feeling panicked, Ramana clicks the link, which takes him to a website that asks him to download a program to remove the threats. What type of attack is Ramana experiencing? What signs indicate this type of attack? What steps could Ramana take to prevent falling victim to scareware attacks in the future?

OR

7.b) Suppose Ms. Jenie is a graphic designer notices that an acquaintance from college has been repeatedly messaging her on social media. Initially, the messages seemed harmless, but they have become increasingly invasive, with the acquaintance commenting on her daily activities, posting about her on their own profile, and tracking her location through tagged photos. Jenie feels uncomfortable and anxious about the attention. What type of attack is Jenie experiencing? What indicators suggest this is a case of cyberstalking? What actions should Jenie take to address the situation, and what steps can she implement to protect her online privacy in the future?

8.a) Assume your cousin brother, Mr. John, is a businessman. He receives an email from someone claiming to be from TWNB Bank, stating that his account needs to be updated for safety purposes and asking him to click the link provided in the email. Shortly after, John receives a phone call from someone claiming to be a representative from TWNB Bank. The caller provides John with personal information to establish trust and states that they need to verify recent transactions. The caller then asks John to confirm his online banking login credentials to address a supposed security issue. What specific types of phishing attacks are being used against John, and what signs indicate these? What actions can TWNB Bank take to educate and protect its customers from attacks like the ones John encountered?

OR

8.b) One day, Ruhin, the IT manager at RBB Hotel, receives multiple complaints from customers regarding unauthorized access to their booking details. Confused by these reports, she begins to investigate the system. While reviewing the logs, Ruhin notices that several customers have received strange emails containing their personal information, including reservation dates and payment details, even though they had not requested such information. Alarm bells go off when she examines the server logs and finds suspicious SQL queries being executed. What type of attack occurred at RBB Hotel? How was this attack achieved? How can it be prevented in the future?

9. Email is the electronic equivalent of a postcard. From archiving to content guidelines, organizations have many factors to consider when creating email policies. Discuss the email security policies that should be incorporated into the organization.

10. Database security includes a variety of measures to secure database management systems from malicious cyber-attacks and illegitimate use. State the need for database security attacks and Elucidate types of attacks and methods to protect the database system.

⇔⇔⇔ **BI/K/TX** ⇔⇔⇔