Roll No.: _

Amrita Vishwa Vidyapeetham
Amrita School of Computing, Coimbatore
B.Tech Mid-Term Examinations – March 2024
Sixth Semester
Computer Science and Engineering

19CSE311 Computer Security

Duration: Two hours | Maximum: 50 Marks

CO	Course Outcomes
CO01	Understand the fundamental concepts of computer security and apply to different components of computing systems.
CO02	Understand basic cryptographic techniques.
CO03	Understand how malicious attacks, threats, security and protocol vulnerabilities impact a system's Infrastructure.
CO04	Demonstrate knowledge in terms of relevance and potential of computer security for a given application.

Answer all questions

1. a. Given that a cryptalyst has learned that system used was RSA with $N = 84773093$ and $\Phi(n)=84754668$ find out the two factors of N. [CO02][BTL4][4 Marks]

   b. Assume that you are working on the authentication scheme of fog node and cloud. How do you find the cost of the scheme, to prove its effectiveness? [CO04][BTL4][3 Marks]

   c. Make the following statement correct by changing one word. *"The strength of Elgamal Cipher system is dependent on difficulty in integer-factorization".* [CO02][BTL2][1 Mark]

2. a. Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Verify the correctness of the statement "Consider the RSA digital signature scheme. Here, Alice generates her public and private keys. Let's assume Alice's public key is *(e, n) = (17, 3233)*, and her private key is *(d, n) = (2753, 3233)*. Alice creates a message M that she wants to sign.Let's say M = "***Hello, Student!***". Alice computes a hash value of the message using a hash function (e.g., SHA-256).Let's say the hash of the message is *H(M) = 256*. The signature of Alice is *1331*." . Also, rationalize your answer. [CO02][BTL 3][3 Marks]

   b. Ramu handles highly confidential information and is concerned about the potential for a virus to infect his system, potentially granting an attacker access to his files, including sensitive data and passwords. He requires a method to securely sign electronic documents; however, storing the signing key on his computer poses a risk, as a virus could capture the key, allowing an attacker to forge signatures. Even employing a passphrase to decrypt the signing key wouldn't suffice, as a virus could log the keystrokes and misuse the key. Ramu considers using a smartcard, a device that connects to his system and performs the signing operation. The document is sent to the smartcard, signed there, and then the signed document is returned for transmission, ensuring the signing key remains secure on the smartcard, away from potential viruses. However, this method still leaves room for attackers to manipulate the system to sign arbitrary documents. How might an attacker achieve this,

considering the smartcard's security measures? **Note:** Just speculate a little on a possible approach don't get stuck for too long trying to design a great solutions.

[CO01][BTL 4][3 Marks]

3. a. Alice, a system administrator, has conducted an analysis of her network system and identified several measures. Assist her in determining the nature of the intrusion by completing the entries in the provided table. [CO01][BTL 4][4 Marks]

Measure	Typeof intrusion detected
Login frequency per day	
Quantity of output to location	
Time since last login	
Program resource utilization	

b. A firewall functions as a computer network security mechanism, regulating internet traffic into, out of, or within a private network. Enumerate one benefit and one drawback of each of four firewall types. [CO01][BTL2][4 Marks]

4. a. Alice and Bob work for the same company XYZ and need to communicate securely over the internet using symmetric encryption. However, they face the challenge of sharing the symmetric key securely without meeting in person. The company uses a simple web-based application, *SecureKeyShare*, designed to facilitate secure symmetric key distribution among its employees. Discuss one potential security risk associated with sharing a symmetric key over the internet, even with the use of *SecureKeyShare*. Also, describe the process Alice should follow to securely send the symmetric key to Bob using the *SecureKeyShare* application. [CO04][BTL3][3 Marks]

b. 1. What method would you use to convert " **PCDZWP**" back into its original text, assuming it was encrypted with a shift cipher, and what would the decrypted text be? [CO02][BTL4][2 Marks]

2. Explain the roles of public and private keys in Asymmetric Key Systems [CO02][BTL2][3 Marks]

5. a. NetSolutions is testing its new data transmission protocol in a network that is known for its high error rate. The development team has decided to implement CRC for frame error detection at the data link layer. Detail the steps to compute CRC for the original test frame "1101011011" using the given polynomial CRC-8 ($x^8 + x^2 + x + 1$). [CO01][BTL3][3 Marks]

b. As part of Secure Communications Inc.'s efforts to enhance their data security, the IT department has been tasked with implementing AES encryption for sensitive internal communications. You, as a cyber-security student, are given a scenario where you need to apply the AES encryption process and perform the following tasks

1. Represent the Plaintext “Anokha Workshops” as state matrix and give the output after *subbyte* and *shiftrow* operations. [CO02][BTL3][1+2+2 Marks]

2. With a block diagram and and example show the process of generating temporary word (T_i) during the key generation process. [CO02][BTL3][4 Marks]

		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 1: AES substitution Box

6. a. In an online treasure hunt game, players are given a clue that leads to the next location. The clue is a number theory puzzle: "Find the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 4, and a remainder of 4 when divided by 5." Help the players solve this puzzle. [CO02][BTL3][4 Marks]

b. Alice and Bob are developers working on a secure messaging application. They decide to use a cryptographic technique that involves primitive elements in a finite field for generating shared secret keys. Is their approach right?Why?. They have decided to use the prime number $p=29$ for their application. Help them to verify if *2* is a primitive element of GF(29). [CO02][BTL3][1+3 Marks]

****

Course Outcome /Bloom's Taxonomy Level (BTL) Mark Distribution Table

CO	Marks	BTL	Marks
CO01	**14**	2	**8**
CO02	**30**	3	**26**
CO03	**--**	4	**16**
CO04	**6**		