

**GUJARAT TECHNOLOGICAL UNIVERSITY****BE - SEMESTER-VII(NEW) EXAMINATION – SUMMER 2019****Subject Code:2170709****Date:14/05/2019****Subject Name:Information and Network Security****Time:02:30 PM TO 05:00 PM****Total Marks: 70****Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks

		MARKS
<b>Q.1</b>	(a) Which two methods are used to frustrate statistical cryptanalysis?	<b>03</b>
	(b) In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the ciphertext, if the plaintext is 2?	<b>04</b>
	(c) (i) Explain working of ECB. Why ECB (Electronic code book) is rarely used to encrypt message? (ii) Why CFB(Cipher feedback mode) encrypted messages are less subject to tampering than OFB(Output feedback mode)?	<b>07</b>
<b>Q.2</b>	(a) Is a message authentication code(MAC) function is similar to encryption. Does MAC provide authentication or confidentiality? Justify your answer	<b>03</b>
	(b) For Diffie-Hellman algorithm, two publically known numbers are prime number 353 and primitive root of it is 3. A selects the random integer 97 and B selects 233. Compute the public key of A and B. Also compute common secret key.	<b>04</b>
	(c) Explain four different stages of AES(Advance Encryption standard) structure.	<b>07</b>
OR		
	(c) Explain how DES(Data Encryption standard) algorithm observes Fiestel structure. Explain key generation and use of S-box in DES algorithm.	<b>07</b>
<b>Q.3</b>	(a) Explain the three approaches to attack RSA mathematically.	<b>03</b>
	(b) What is the difference between weak and strong collision resistance? Consider the hash functions based on cipher block chaining, What kind of attack can occur on this?	<b>04</b>
	(c) Given key $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ and plaintext = "ney". Find out the ciphertext applying Hill Cipher. Is Hill cipher strong against ciphertext only attack or known plaintext attack? Justify the answer.	<b>07</b>
OR		
<b>Q.3</b>	(a) For what purpose Secure Shell(SSH) is useful? Briefly define SSH protocol.	<b>03</b>
	(b) How meet in the middle attack is performed on double DES?	<b>04</b>

	(c)	How cryptanalyst can exploit the regularities of the language? How digrams can solve this problem? Use the key “hidden” and encrypt the message “Message” using playfair cipher.	07
Q.4	(a)	Explain the rail fence cipher. Why a pure transposition cipher is easily recognized?	03
	(b)	What is the difference between a session key and a master key? List four general categories of schemes for the distribution of public keys.	04
	(c)	Explain the logic of SHA(Secure Hash Algorithm).	07
OR			
Q.4	(a)	Why Transport Layer Security makes use of a pseudo random function?	03
	(b)	What is the purpose of X.509 standard? How is an X.509 certificate revoked?	04
	(c)	Write the algorithm for message authentication code(MACs) based on HASH functions.	07
Q.5	(a)	Define the parameters that define SSL session state and session connection.	03
	(b)	What problem was Kerberos designed to address? What are the three threats associated with user authentication over a network or Internet?	04
	(c)	Describe Elgamal digital signature.	07
OR			
Q.5	(a)	Which types of security threats are faced by user while using the web?	03
	(b)	List three approaches to secure user authentication in a distributed environment.	04
	(c)	What is the principle of digital signature algorithm(DSA). How a user can create a signature using DSA? Explain the signing and verifying function in DSA.	07

\*\*\*\*\*