Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER– VII (NEW) EXAMINATION – WINTER 2021

Subject Code:2170709 Date:25/11/2021

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.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Differentiate symmetric and asymmetric key cryptography. Draw the design model of symmetric key cryptography.	**03**
	(b)	Use Playfair cipher to Decrypt the following message: "Must see you over Cadogan West. Coming at once" Key: EXAMPLE	**04**
	(c)	Enlist block cipher modes of operation. Justify the use of Electronic Codebook (ECB) mode in Cipher Block Chaining (CBC) mode.	**07**
Q.2	**(a)**	Differentiate the following: 1. Stream cipher and block cipher 2. Diffusion and confusion	**03**
	(b)	Apply Railfence cipher approach and columnar(Advanced) Railfence cipher approach to Encrypt the following message: "Give me the top ten possible plaintexts" Key for Railfence cipher: 3 Key for Columnar(Advanced) Railfence cipher: [1 4 2 5 3]	**04**
	(c)	Draw the design process of DES encryption and explain the round function of DES.	**07**
		OR	
	(c)	Discuss the design principles of block cipher.	**07**
Q.3	**(a)**	Discuss attack on double DES?	**03**
	(b)	Encrypt the message M = 9 using RSA with the following parameters: e = 3 and n = 5*11. Then regenerate the plaintext value back based on cipher text value.	**04**
	(c)	Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2. (i) Show that 2 is a primitive root of 11. (ii) If user A has public key Y_A=9, what is A's private key X_A? (iii) If user B has public key Y_B=3, what is the shared secret key K, shared with A?	**07**
		OR	
Q.3	**(a)**	Define the following terms: Masquerade attack, Source repudiation and Destination repudiation	**03**
	(b)	Discuss man-in-the middle attack on Diffie-Hellman key exchange.	**04**
	(c)	Draw the design process of AES round function and explain the sub-nibble transformation and shift row mechanism in detail with example.	**07**

Q.4	**(a)**	Why HASH function is required in cryptography?	**03**
	(b)	Describe Birthday attack.	**04**
	(c)	Define Digital signature. Explain digital signature algorithm.	**07**
		OR	
Q.4	**(a)**	Design RSA approach for digital signature standard.	**03**
	(b)	Define Message authentication code (MAC) and explain it in detail.	**04**
	(c)	Discuss SHA-512.	**07**
Q.5	**(a)**	Differentiate confidentiality and authentication.	**03**
	(b)	Discuss the advantages to use public key certificate over the public key authority in key distribution scenario.	**04**
	(c)	Enlist the various security protocols used at different layers of TCP/IP protocol stack and explain SSL protocol in brief.	**07**
		OR	
Q.5	**(a)**	Discuss transport layer security.	**03**
	(b)	Use confidentiality and authentication approach to explain secret key distribution.	**04**
	(c)	Describe Kerberos.	**07**

****