Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.E Sem-II Examination July 2010

Subject code: 720205

Subject Name: Cryptography & Network Security

Date: 08 /07 /2010 **Time: 11.00am – 1.30pm**

Total Marks: 60

Instructions:

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

Q.1	**(a)**	1) Explain the following terms: Confidentiality, Authentication, Authorization, Non-repudiation 2) Briefly define the monoalphabetic cipher. 3)What are the two general approaches to attacking a cipher?	**06**
	(b)	Explain all the steps of encryption process in DES.What is the purpose of of the S-boxes in DES?	**06**
Q.2	**(a)**	Encrypt the message "GTU" using the Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations and the result. Show the calculations for corresponding decryption of the ciphertext to recover the original plaintext.	**06**
	(b)	Explain the block cipher modes of operation in brief. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?	**06**
		OR	
	(b)	What are the security services(x.800) categories? Explain each in brief?	**06**
Q.3	**(a)**	Explain all the steps of encryption process in AES. Briefly describe SubBytes and ShiftRows.	**06**
	(b)	For a user workstation in a typical business environment ,list potential locations for confidentiality attacks. What is the difference between link and end to end encryption?	**06**
		OR	
Q.3	**(a)**	Explain a typical key distribution scenario. Write your comment on key life.	**06**
	(b)	Explain Pseudorandom number generators (PRNGs). What is the difference between statistical randomness and unpredictability ?	**06**
Q.4	**(a)**	Explain the principal of public-key cryptosystem. What are the principal elements of a public-key cryptosystem?	**06**
	(b)	What are the Secure Electronic Commerce components? Explain each in brief. Give the overview of SET (Secure Electronic Transaction).	**06**
		OR	
Q.4	**(a)**	What type of attacks are addressed by message authentication? What is message authentication code?	**06**
	(b)	Explain IP Security Architecture .Also give the examples of applications of IPSec.	**06**
Q.5	**(a)**	Explain the various web security threats ,its consequences and countermeasures for that.	**06**
	(b)	What are the reasons for the PGP (Pretty Good Privacy)'s growth? Explain PGP cryptographic functions.	**06**
		OR	
Q.5	**(a)**	Explain the SSL Architecture .What protocols comprise SSL?	**06**
	(b)	What problem was Kerberos designed to address? What are three threats associated with user authentication over a network or Internet?	**06**

****