Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.C.A.- SEMESTER – V • EXAMINATION – WINTER 2012

Subject code: 650002 Date: 26-12-2012

Subject Name: Network Security

Time: 10:30 am – 1:00 pm Total Marks: 70

Instructions:

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

Q.1	(a)	Define the following terms. i) Cryptography ii) Relative Prime Number iii) MAC iv) Digital Signature v) Non repudiation vi) Dual signature vii) Euler's totient function	07
	(b)	i) For a user workstation in a typical business environment, list potential locations for confidentiality attacks.	02
		ii) What is traffic padding and what is its purpose?	02
		iii) What is the difference between link and end-to-end encryption?	03
Q.2	(a)	How diffusion and confusion is achieved in DES (Data Encryption Standard)? Explain single round of DES algorithm.	07
	(b)	Why mode of operation is defined? Explain any two cipher block modes of operations.	07
		OR	
	(b)	i) What are three broad categories of applications of public-key cryptosystems? What requirements must a public key cryptosystems fulfill to be a secure algorithm?	03
		ii) List the steps of RSA algorithm.	04
Q.3	(a)	What is the difference between direct and arbitrated digital signature? Explain the Digital Signature algorithm.	07
	(b)	What is a message authentication code? Briefly explain the HMAC algorithm.	07
		OR	
Q.3	(a)	Briefly explain Diffie-Hellman key exchange. Justify that Diffie Hellman key exchange is vulnerable to man in the middle attack.	07
	(b)	i) What characteristics are needed in a secure hash function?	02
		ii) What is the difference between weak and strong collision resistance?	02
		ii) Explain the general structure of secure hash functions.	03
Q.4	(a)	Draw ESP format for IPSec and describe the need of various fields.	07
	(b)	What protocols comprise SSL? List and briefly define the parameters that define an SSL session state and SSL session connection.	07
		OR	
Q.4	(a)	What is SET? Explain purchase request and payment authorization processes of SET.	07
Q.4	(b)	What is IPSec? What are the applications of IPSec? Explain the modes of IPSec operations.	07
Q.5	(a)	Briefly explain how the authentication service is provided in distributed environment using Kerberos.	07
	(b)	How PGP constructs a secure mail? Write the steps involved in the process.	04
	(c)	How enveloped data is constructed in SMIME. Write all steps for the same	03
		OR	
Q.5	(a)	Explain how attacks like IP address spoofing, source routing and tiny fragments can be carried out on packet filtering routers? What are the counter measures?	07
	(b)	Explain general Format of PGP Message	04
	(c)	What are the five principal services provided by PGP? What is a key ring in PGP?	03

****