Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – SUMMER • 2015

Subject Code: 2650002 Date: 04-05-2015

Subject Name: 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.**

Q.1	(a)	Explain Security Services (X.800).	7
	(b)	Discuss Active and Passive attacks in detail.	7
Q.2	(a)	Explain RC4 Algorithm in details.	7
	(b)	What is Symmetric Block Ciphers? Discuss Advanced Encryption Standard (AES).	7
		OR	
	(b)	What are the properties of Hash Function? Explain Secure Hash Algorithm (SHA) Function.	7
Q.3	(a)	Explain RSA Public-Key Encryption with a suitable example.	7
	(b)	(i) What is Elliptic Curve Cryptography (ECC).	2
		(ii) Write what a Digital Signature is.	2
		(iii) Explain Benefits of IPSec.	3
		OR	
	(a)	Explain Diffie-Hellman Key Exchange Algorithm with a suitable example.	7
	(b)	Discuss Kerberos Version 5 in details.	7
Q.4	(a)	Explain Secure Socket Layer (SSL) Architecture and SSL Record Protocol.	7
	(b)	(i) Draw and explain X.509 Certificate.	4
		(ii) Explain Encapsulation Security Payload (ESP) Packet Format.	3
		OR	
	(a)	Draw and discuss Public-Key Infrastructure (PKIX) Architecture Model.	5
	(b)	(i) Explain IEEE 802.11i Services.	5
		(ii) Explain WAP Infrastructure.	4
Q.5	(a)	What is Pretty Good Privacy (PGP) ? Explain PGP Services in details.	7
	(b)	(i) Explain IPsec Association Database and IPsec Policy database in details.	6
		(ii) What is Honeypots intrusion detection.	1
		OR	
	(a)	Write short note on following	
		(i) Statistical Anomaly Detection.	4
		(ii) Types of Firewall.	3
	(b)	Discuss firewall configuration.	7

****