Seat No.: Enrolment No.:

C U SHAH UNIVERSITY

Faculty of Technology and Engineering

M.Tech Semester-II Examination -2015

Branch:-CE **Semester:**-2nd M.Tech

Subject Code: 5TE02ANS1 **Subject Name:** Advance Cryptography and Network Security

Instructions:

- Make suitable assumptions whenever necessary.
- Figures to the right indicate full marks.
- Question 1 and Question 4 are compulsory

Section –I

Q-1	Attempt following Questions.		
	a)	What are the Difference Between Tunnel Mode and Transport Mode?	2
	b)	What is the objective of Security?	2
	c)	Difference between Symmetric and Asymmetric Cryptography.	2
	d)	How many keys are used in 3-DES and Double DES?	1
Q-2	a)	Explain Single Round of DES.	5
	b)	Describe RSA Algorithm with examples.	5
	c)	Explain Characteristics of Cryptography.	4
		OR	
Q-2	a)	Describe Playfair Cipher with Suitable examples.	5
	b)	Explain Singular Columnar Transposition Techniques with example.	5
	c)	Write Short Note on “Authentication Requirement”.	4
Q-3	a)	Write Short note on “Digital Signature”	5
	b)	Describe Diffie Hellman Algorithm with examples.	5
	c)	What are the different types of modes of Block Cipher?	4
		OR	
Q-3	a)	Write a Short Note On “Steganography”.	5
	b)	Explain Security Attacks.	5
	c)	Explain Web Security Architecture.	4

Section –II

Q-4	Attempt following Questions.		
	a)	What is the Full Form of VIRUS? Define VIRUS.	2
	b)	Which Techniques is More Secure and Why?	2
	c)	Differentiate RC4 and RC5.	2
	d)	List Out Real time Application of Security.	1
Q-5	a)	Explain Hill Cipher Technique with example.	5
	b)	Find out GCD (1974, 1086) Using Euclid Algorithm.	5
	c)	Explain in brief Concept of Message Digest.	4
		OR	
Q-5	a)	Explain IDEA.	5
	b)	Difference between SSL and SET.	5

	c)	Explain Process of Handshake Protocol.	4
Q-6	a)	What is the use of RC4? Explain RC4 Operation.	5
	b)	Explain Dual Signature.	5
	c)	Explain Worms and Trojan Horse.	4
		OR	
Q-6	a)	Explain Pretty Good Privacy (PGP).	5
	b)	Write a Short Note on “Blowfish”	5
	c)	Explain Concept of Kerberos.	4