Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– I (New course)• REMEDIAL EXAMINATION – SUMMER 2015

Subject Code: 2715601 **Date:18/05/2015**

Subject Name: Cryptography and Network Security

Time: 10:30 am to 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)	What is OSI security architecture? Briefly define X.800 security services.	07
	(b)	1) Explain the following terms: Confidentiality, Authentication, Authorization, Non-repudiation 2) Briefly define the monoalphabetic cipher.	07
Q.2	(a)	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?	07
	(b)	What are two building blocks of encryption techniques. List three encryption techniques of each. Explain any one of them with one relevant example.	07
		OR	
	(b)	What is triple DES? What are the proposed attacks on triple DES?	07
Q.3	(a)	Explain all the steps of encryption process in AES. Briefly describe Substitute Bytes transformation and MixColumn transformation.	07
	(b)	Discuss in detail the RSA algorithm, highlighting its computational aspects and security.	07
		OR	
Q.3	(a)	Explain different modes of operation applied in block cipher algorithm.	07
	(b)	Explain the RC4 stream cipher method used for encryption and decryption.	07
Q.4	(a)	Briefly explain the idea behind Elliptic Curve Cryptosystem.	07
	(b)	Explain Diffie Hellmann key Exchange in detail with an example.	07
		OR	
Q.4	(a)	Explain the architecture of IP Security.	07
	(b)	Describe Simple Hash function with one example.	07
Q.5	(a)	Which environmental and technical limitations of Kerberos version 4 have been addressed by version 5? Briefly mention the improvements in each area.	07
	(b)	Describe the general format of X.509 certificate and strong authentication procedures.	07
		OR	
Q.5	(a)	Explain the working of the firewalls to protect the network. Differentiate Intrusion Detection Sytem (IDS) and firewall.	07
	(b)	What are viruses? Explain the virus related threats and the counter measures applied.	07