Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–IV • EXAMINATION – WINTER 2018

Subject Code: 3640004 Date: 27/11/2018

Subject Name: Network Security

Time:10.30 am to 01.00 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)** Answer the following questions. **07**

1. List out categories of active attack.
2. What is replay?
3. What is stream cipher?
4. What is brute-force attack?
5. What is the first step in AES round?
6. What is Public-Key Encryption?
7. What is Session key?

(b) Answer the following questions. **07**

1. An encrypted hash of a message is a type of _____
2. RC4 is an example of _____
3. The power of counter mode is _____
4. A random number in key exchange is popularly known as _____
5. SSH is a protocol for _____
6. Extended service set is _____
7. Secret key algorithms are also known as _____

Q.2 **(a)** 1. Explain Security Mechanism. **03**

2. Explain Network Security Model with supporting diagram. **04**

(b) What are the essential ingredients of a symmetric cipher? Explain Feistel Cipher Structure. **07**

OR

(b) What is symmetric encryption? Explain ECB and CBC mode. **07**

Q.3 **(a)** What is a message authentication code? List three approaches to message authentication. **07**

(b) Explain Diffie-Hellman Key Exchange algorithm. **07**

OR

(b) What are the principal ingredients of a public-key cryptosystem? List and briefly define three uses of a public-key cryptosystem. **07**

Q.4 **(a)** 1. What is the job of SSL Record Protocol? **04**

2. Write any three important differences between SSL and TLS **03**

(b) What is the basic building block of an 802.11 WLAN? List and briefly define IEEE 802.11 services. **07**

OR

Q.4	**(a)**	List out the security services provided by WTLS and describe with appropriate example.	**07**
	(b)	Explain Kerberos version 4 in detail.	**07**
Q.5	**(a)**	What are the five principal services provided by PGP? Why does PGP generate a signature before applying compression?	**07**
	(b)	1. Write and explain any three applications of IPsec. 2. How security associations are combined in IPsec? Give appropriate examples.	**03** **04**

OR

Q.5	**(a)**	What is Intrusion? Discuss intrusion detection techniques.	**07**
	(b)	Why firewall is needed in a secure network? Describe the various types of Firewall.	**07**

****