Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA – SEMESTER – 5 • EXAMINATION – SUMMER 2018

Subject Code: 2650002 **Date: 02-May-2018**

Subject Name: Network Security (NS)

Time: 10.30 am to 1.00 pm **Total Marks: 70**

Instructions:

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

Q1.A. Answer the following: [07]

1. Write a short note on: Challenges in implementing Network Security. [05]
2. Briefly explain any one active attack on network security. [02]

Q1.B Answer the following: [07]

1. Explain the simplified model for symmetric encryption systems. [05]
2. Mention any two design parameters for designing a typical symmetric block cipher. [02]

Q2.A Answer the following: [07]

1. Mention and briefly explain any two requirements for designing a secure hash function. [05]
2. Instead of using HMAC with MD5, if only MD5 is used, does it affect network security? If yes, how? If no, why not? [02]

Q2.B Answer the following: [07]

1. Explain with a diagram how confidentiality is achieved when using public key cryptography. [05]
2. Mention any two applications of RSA algorithm other then encryption/decryption. [02]

OR

Q2.B Answer the following: [07]

1. Explain: Public Key Infrastructure. [05]
2. What does a digital signature certificate certify? Which is the standard for the format of a digital signature certificate? [02]

Q3.A Answer the following: [07]

1. Briefly explain: Connection and Session w.r.t SSL. [05]
2. Which two services are provided by SSL Record Protocol to SSL connections? [02]

Q3.B Answer the following: [07]

1. Write a short note on: IPSEC Applications. [05]
2. Which security services are available in ESP for IPSEC? [02]

OR

Q3.A Answer the following: [07]

1. Mention and briefly explain any five Non-Fatal Alerts in Alert Protocol of SSL. [05]
2. Which are the major two differences between TLS and SSL? [02]

Q3.B Answer the following: [07]

1. Write a short note on: Benefits of Padding in IPSEC. [05]
2. Differentiate briefly between tunnel mode and transport mode for IPSEC. [02]

Q4.A Answer the following: [07]

1. Mention and briefly explain the IEEE 802.11i RSN Services along with their Corresponding security mechanisms used to provide those services. [05]
2. Mention any two possible AKM Suites for IEEE 802.11i. [02]

Q4.B Answer the following: [07]

1. Mention any five reasons which made PGP popular. [05]
2. Briefly explain the need to use radix 64 algorithm in PGP. [02]

OR

Q4.A Answer the following: [07]

1. Mention and briefly explain the IEEE 802.11i phases of operation. [05]
2. What is the importance of Master Session Key in IEEE 802.11i? [02]

Q4.B Answer the following: [07]

1. Mention the security services provided and their corresponding mechanisms used in PGP. [05]
2. Briefly explain: Private Key Ring in PGP. [02]

Q5.A Answer the following: [07]

1. Mention and briefly explain the common fields in Security Audit Records. [05]
2. Briefly explain the difference between Rule based Penetration Identification and [02]

Rule based Anomaly Detection.

Q5.B Answer the following: [07]

1. Briefly explain different types/categories of firewalls. [05]
2. Briefly explain: Default Discard Policy in Firewalls. [02]

OR

Q5.A Answer the following: [07]

1. Write a short note on: Distributed IDS. [05]
2. Give an example of False Positive and False Negative in an IDS. [02]

Q5.B Answer the following: [07]

1. Briefly explain different types of firewall topologies. [05]
2. Mention any two differences between a Personal firewall and Enterprise Firewall. [02]

-x-x-x-x-x-