Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA Integrated - SEMESTER–VIII-EXAMINATION – WINTER 2018

Subject Code: 4480603 Date: 22-11-2018

Subject Name: Network Security

Time: 02.30 pm to 5.00 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)** Do as directed (any 7): **07**

1. What is Information Security, Computer Security, Intranet Security & Internet Security?
2. Two types of attack are _____ and _____.
3. Nonce is _____.
4. Three classes of intruders are _____, _____ & _____.
5. Firewalls are classified into _____.
6. X/MIME stands for _____
7. The number of key(s) used in Asymmetric Cryptography is/are ____.
8. Phil Zimmermann is the founder of _____.
9. KDC is responsible for _____.
10. What is clear signed data in S/MIME?
11. IP address spoofing means _____.
12. Use of subject field in X.509 certificate.

(b) Differentiate between (any 2): **07**

1. Active attack & Passive attack
2. Security service & Security mechanism
3. SSL and TLS

Q.2 **(a)** Discuss RC4 algorithm in detail. **07**

(b) Discuss RSA Public-Key Encryption with a suitable example. **07**

OR

(b) (i) What is Elliptic Curve Cryptography (ECC)? **02**

(ii) What is a Digital Signature? **02**

(iii) Explain benefits of IPSec. **03**

Q.3 **(a)** Discuss Kerberos in detail. Write any 3 differences between version 4 and 5. **07**

(b) Discuss Diffie-Hellman key exchange algorithm in detail with suitable example. **07**

OR

Q.3 **(a)** Discuss SSL architecture. Also draw and explain the SSL Record Protocol. **07**

(b) Discuss in detail Public Key Infrastructure architecture (PKIX) with diagram. **07**

Q.4 **(a)** Discuss IEEE 802.11i Services. **07**

(b) What is Pretty Good Privacy (PGP)? Discuss its services in detail. **07**

OR

Q.4 **(a)** What is ESP (Encapsulating Security Payload)? Discuss ESP packet format in detail with diagram. **07**

(b) Explain the X.509 certificate in detail with suitable diagram. **07**

Q.5 **(a)** Discuss WAP infrastructure. **07**

(b) What do you mean by a Firewall? How it protects a machine/network? Discuss any one type of firewall and explain its configuration. **07**

OR

Q.5 **(a)** Short notes on: **07**

1. Statistical Anomaly Detection
2. Honeypots
3. CIA Triad
4. Design & parameters of HMAC
5. Block & Stream Ciphers
6. Anti-replay window in IPSec
7. Heuristic rules for intrusion detection.

(b) Discuss IPsec Association Database and IPsec Policy database in detail with suitable diagram. **07**

****