Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**ME – SEMESTER I (NEW) – • EXAMINATION – SUMMER 2016**

**Subject Code: 2715601** **Date:20/05/2016**

**Subject Name: Cryptography and Network Security**

**Time:02:30 pm to 05:00 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)** | (i) Explain the terms confusion and diffusion?<br>(ii) Explain mono-alphabetic substitution cipher? Also discuss letter frequency attack on mono-alphabetic substitution cipher? | **07** |
| | **(b)** | Explain how public key encryption is used to distribute secret keys. | **07** |
| **Q.2** | **(a)** | Explain RSA algorithm? Perform encryption and decryption using RSA algorithm for p=3, q= 11 and e=7, M=5. | **07** |
| | **(b)** | Explain algorithm for key exchange using Elliptic curve cryptography. | **07** |
| | | **OR** | |
| | **(b)** | Explain Deffie Helman Key Exchange algorithm. | **07** |
| **Q.3** | **(a)** | What is the need for message authentication? List various techniques used for message authentication. Explain any one. | **07** |
| | **(b)** | What is Digital Signature? Explain Digital signature standard. | **07** |
| | | **OR** | |
| **Q.3** | **(a)** | Explain the ticket granting server(TGS) scheme in Kerberos. | **07** |
| | **(b)** | Explain X.509 certificate in detail. | **07** |
| **Q.4** | **(a)** | What is dual signature? What is the use of dual signature. | **07** |
| | **(b)** | Explain modes of operation of IPSec and application of IPSec | **07** |
| | | **OR** | |
| **Q.4** | **(a)** | Explain general format of PGP message. | **07** |
| | **(b)** | Explain SSL protocol. | **07** |
| **Q.5** | **(a)** | State various types of firewall? Explain any one of them. | **07** |
| | **(b)** | Explain AES key expansion algorithm. | **07** |
| | | **OR** | |
| **Q.5** | **(a)** | Explain RFID security issues | **07** |
| | **(b)** | (i) Explain any one random number generation algorithm?<br>(ii) define Following terms<br>Intrusion detection system, DDOS attack, virus | **07** |

**********