*Seat No.: _____* *Enrolment No._____*

# GUJARAT TECHNOLOGICAL UNIVERSITY

**M. E. - SEMESTER – II • EXAMINATION – SUMMER • 2014**

**Subject code: 1722302** **Date: 18-06-2014**

**Subject Name: Advance Cryptography and Information Security**

**Time: 02:30 pm - 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)** | What is the difference between direct and arbitrated digital signature? Write the Digital Signature Algorithm. | **07** |
| | **(b)** | What is the difference between weak and strong collision resistance? Illustrate various ways in which a hash code can be used to provide message authentication. | **07** |
| **Q.2** | **(a)** | (1) What is the difference between an unconditional secure cipher and a computationally secure cipher? | **04** |
| | | (2) Write a short note on Steganography. | **03** |
| | **(b)** | (1) Write MAC (Message Authentication code) property. | **04** |
| | | (2) Write the Euclidean algorithm to find greatest common divisor (a, b). | **03** |
| | | **OR** | |
| | **(b)** | (1) Write the algorithm for finding multiplicative inverse in GF (p). | **04** |
| | | (2) Write a properties of hash function | **03** |
| **Q.3** | **(a)** | Explain the Single Round of DES Algorithm with diagram. | **07** |
| | **(b)** | (1) Explain Cryptographically Secure pseudorandom bit generator (CSPRBG). | **04** |
| | | (2) Explain Meet-in-the-Middle attack | **03** |
| | | **OR** | |
| **Q.3** | **(a)** | Draw a figure of classical Feistel Network. Explain the parameters and design choices those determine the actual algorithm of a feistel cipher. | **07** |
| | **(b)** | Write and explain the Deffie-Hellman key exchange algorithm. | **07** |
| **Q.4** | **(a)** | In AES, how the encryption key is expanded to produce keys for the 10 rounds. | **07** |
| | **(b)** | What type of information might be derived from a traffic analysis attack? What is traffic padding and what is its purpose? | **07** |
| | | **OR** | |
| **Q.4** | **(a)** | Why it is not desirable to reuse a stream cipher key? Explain the RC4 algorithm. | **07** |
| | **(b)** | What is replay attack? Explain a suppress-replay attack. List and explain three general approaches to dealing with replay attacks. | **07** |
| **Q.5** | **(a)** | Explain server-level web threats like repudiation, information disclosure, evaluation of privileges, and denial of service. | **07** |
| | **(b)** | Explain the anomaly and pattern base intrusion detection system. | **07** |
| | | **OR** | |
| **Q.5** | **(a)** | Explain fundamentals of secure network design scenario like Dual-Homed Host, Screened Host, Screened Subnets and Split Screened Subnets in detail. | **07** |
| | **(b)** | When system administrator trusts the internal users, what type of fire wall is to be used? Distinguish between packet filtering firewalls and stateful packet filtering. | **07** |

**********