M.Tech-Computer Science and Engineering Sem II

# MT-1009.4 - Elective-II : Network Security & Cryptography

| | | |
|---|---|---|
| P. Pages : 1 | | **GUG/W/16/3944** |
| Time : Three Hours | * 4 7 4 4 * | Max. Marks : 70 |

---

Notes : 1. Attempt **any five** questions.
2. All questions carry equal marks.
3. Due credit will be given to neatness and adequate dimensions.
4. Illustrate your answers wherever necessary with the help of neat sketches.

| | | | |
|---|---|---|---|
| **1.** | a) | Explain classical feistal network. | **7** |
| | b) | What is the difference between differential and linear cryptanalysis. | **7** |
| **2.** | | Explain AES encryption and decryption. | **14** |
| **3.** | a) | List important design considerations of a stream cipher key. | **7** |
| | b) | Explain steganography. | **7** |
| **4.** | a) | Explain authentication functions. | **7** |
| | b) | Explain HMAC algorithm. | **7** |
| **5.** | a) | Explain Kerberos. | **7** |
| | b) | Explain transport and tunnel modes. | **7** |
| **6.** | a) | Explain secure electronic transaction. | **7** |
| | b) | Explain distributed denial of services. | **7** |
| **7.** | a) | Explain transmission and reception of PGP messages. | **7** |
| | b) | Explain multipurpose internet mail extension. | **7** |
| **8.** | a) | Explain IPsec authentication header. | **7** |
| | b) | Explain elliptic curve arithmetic. | **7** |

*********