Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.Tech(IT)/SEM-2/ITM-203/2012

2012

CRYPTOGRAPHY & NETWORK SECURITY

Time Allotted : 3 Hours *Full Marks* : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer any *five* of the following. 5 × 14 = 70

1. Discuss the types of attack that an occur on an encrypted text. What is transposition ? Discuss the types of transposition technique with suitable example. 5 + 1 + 8

2. State the requirements for an encryption algorithm to be computationally secure. Discuss an algorithm mode that can handle large blocks of data. Illustrate bucket brigade attack with suitable example. 2 + 5 + 7

3. Discuss single round operation of a symmetric algorithm that uses both diffusion and confusion for encryption, requires 2^{128} operations to break it and employs the technique of key shifting. State the encryption procedure of a symmetric algorithm that is suitable for smart card and the key can change frequently. 7 + 7

4. Discuss in detail, the encryption procedure of a symmetric algorithm that is suitable for smart card, secure in nature, based on Rijndael algorithm and uses the concept of "word" for key generation.

5. State the requirements of a hash function ? Discuss a protocol that serves the function of a KDC and also provides authentication. State the concept of collision in reference to hash function. 5 + 8 + 1

6. Discuss in detail a transport layer security protocol that uses MAC in one of its sub-protocols ? Illustrate an application layer security protocol that does not use the function of compression. 9 + 5

7. Write short notes on any *two* of the following : 2 × 7

   a) DES

   b) RSA

   c) MD5

   d) SHA1

   e) HMAC.