Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.TECH (ECE)/SEM-2/MCE-204-A/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 Question No. 1 and any *four* from the rest.

1. a) What is the difference between security attack and security threat ? 2

   b) What are the principle elements of a public – key cryptosystem ? 2

   c) What are the requirements of Hash functions ? 3

   d) Define Galois field and extended Galois field. 2

   e) What are the three protocols used in IPSec ? What are their functions ? 3

   f) Distinguish between passive attack and active attack. 2

2. a) Explain the generation of S-box as well as S-box substitution in case of AES algorithm.

   b) Explain the shift row and mix column steps of AES algorithm. 6 + 8

3 a) Distinguish between strong collision resistant and weak collision resistant property of Hash function.

   b) Given a Hash Function H with n possible outputs and a specific value h. How many random inputs must we test before our chance of finding some x such that h = H(x) is greater than $\frac{1}{2}$?

   c) How MAC can be exploited to generate fraudulent message with proper authentication ? Explain. 2 + 6 + 6

4. a) Explain Diffie – Hellman key exchange protocol.

   b) In a RSA system, you intercept the ciphertext C = 11 sent to user whose public key Pu = 7, N = 187. What is the plaintext ?

   c) What are the ECC domain parameters ? Explain them.

   5 + 5 + 4

5. a) Explain SHA – 1 algorithm.

   b) Describe different connection states in SSL. 8 + 6

6. a) Explain the whole process of SET transactions.

   b) Discuss the functions and limitations of Firewall packet filters.

   c) Compare SET and e-cash. 7 + 5 + 2

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

   a) IPSec security associations

   b) DSA

   c) Elliptic curve cryptography.

   d) Biometric Authentication.