CS/IT–7201

B. E. (Seventh Semester) EXAMINATION, June, 2007

Common for CS & IT Engg.)

NETWORK SECURITY

(Elective–II)

Time : Three Hours

Maximum Marks : 100

Minimum Pass Marks : 40

Note : Attempt any *five* questions. All questions carry equal marks.

1. (a) Define the following terms : 4 each
   (i) Authentication
   (ii) Data Confidentiality
   (iii) Data Integrity
   (iv) Non-repudiation
   (b) Give the advantages of HMACs over RSA to sign SHA-1 hashes. 4

2. (a) Explain the MD5 with block diagram. 10
   (b) A message that is 200 bits long is encrypted with a one-time pad. How many trial decrptions are necessary for a brute-force attack on this message ? 5
   (c) Why is Diffie-Hellman not resilient to a man-in-the-middle attack ? 5

P. T. O.

3. Explain the following : 10 each
   (i) Elliptic curve cryptography
   (ii) Message Authentication Code

4. Explain the following concepts precisely and completely : 4 each
   (i) Chosen plaintext attack
   (ii) Brute-force attack
   (iii) Confusion
   (iv) Error propagation rate
   (v) Security through obscurity

5. (a) Explain the RSA algorithm. Using the RSA public key Cryptography with $z = 1, y = 2, x = 3 \ldots\ldots, a = 26$ and $p = 5, q = 7$ and $d = 5$ find e and encrypt 'fedeba'. 10
   (b) Explain the different types of firewalls configuration. What are the differences between among the three configuration ? 10

6. (a) Differentiate between the following in brief : 12
   (i) Stenography and Cryptology
   (ii) Private and Public key
   (iii) E-mail viruses and Worms
   (iv) Crytanalysis and Cryptography
   (b) Assume you have a worm that can infect a known host in 5 rounds and that it cannot infect more than one host at a time. If a worm is released one a single host, how many rounds will it take to infect 1 million hosts ? 4
   (c) What property does a digital signature provide that an HMAC does not ? Discuss. 4

7. (a) Explain digital signature with the help of an example. Give its properties and requirement in brief. 10
   (b) Why do mutable fields present problems for IP sec and in which modes do these problems manifest ? 5
   (c) What is the difference between vulnerability and a threat ? 5

8. Write notes on any *three* of the following :
   (i) Transposition Cipher
   (ii) Authentication function
   (iii) HTTPS
   (iv) IP security