Total No. of Questions : 8] [Total No. of Printed Pages : 2

Roll No. .....

MCSE/MCTA–302(F)

M. E./M. Tech. (Third Semester)
EXAMINATION, Feb./March, 2009

NETWORK SECURITY

(Elective – V)

Time : Three Hours

Maximum Marks : 100

Minimum Pass Marks : 40

Note : Attempt any *five* questions. All questions carry equal marks. Make suitable assumptions wherever necessary.

1. (a) How physical security of computer and information system is achieved ? Explain the principles of information security.

   (b) What are the block cipher modes of operation and discuss the techniques and applicability of differential and linear cryptanalysis in DES ?

2. (a) How does Asymmetric key encryption ensure 'Non-Repudiation' ?

   (b) In RSA encryption method, if the prime no. p and q are 3 and 7 respectively, the encryption exponent e is 11, find the following :

   (i) The least positive decryption exponent d

   (ii) Public and Private key

   (iii) Cipher text when the plain next P is encrypted using the public key.

P. T. O.

3. (a) What are the public key encryption approaches for confidentiality and authentication ? Describe the public key approaches to one way authentication.

   (b) What is the purpose of Diffie-Hellman public key technique ? Also describe the algorithm.

4. (a) On the elliptic curve over the real numbers $y^2 = x^3 - 36x$, let P = $(-3 \cdot 5, 9 \cdot 5)$ and Q = $(-2 \cdot 5, 8 \cdot 5)$. Find P + Q and 2P.

   (b) What requirements must a public key crypto system fulfil to be a secure algorithm ? Briefly explain each of them with examples.

5. (a) Differentiate between the MD5 and SHA-1 algorithm.

   (b) How IPSec can be used to create VPN ?

6. (a) Explain the RSA algorithm using public key cryptography with $z = 1, y = 2, x = 3$ ...., $a = 26$ and $p = 5, q = 7$ and $d = 5$. Find e and encrypt 'fedcba'.

   (b) Explain the different types of firewall configuration. What are the differences between the three configurations ?

7. (a) Describe how digital signatures can be used for ensuring messages integrity in distributed system ?

   (b) How does digital signature prevent e-mail spoofing ? Explain.

8. Write short notes on any *three* of the following :
   (i) Stenography
   (ii) IDEA encryption algorithm
   (iii) IP security
   (iv) Trojan Horse