Total No. of Pages: 1

7278

Register Number:

Name of the Candidate:

M.C.A. DEGREE EXAMINATION, May 2015

(FIFTH SEMESTER)

521. NETWORK SECURITY

Time: Three hours Maximum: 100 marks

SECTION -A (8 × 5 = 40)

Answer any EIGHT questions

1. Explain Model for Network Security with neat sketch.
2. Which parameters and design choices determine the actual algorithm of Feistel Cipher? Explain it.
3. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=11 and primitive root α=5.
   a) If user A has private key X_A–2, what is A's public key Y_A?
   b) If user B has private key X_B=3, what is B's public key Y_B?
   c) What is the shared secret key K?
4. What are the requirements for Hash function?
5. Illustrate the benefits and applications of IP security.
6. Explain the parameters associated with SAD.
7. Write in short note SSL record protocol.
8. What are the steps involved in SET transaction?
9. Explain honey pots in detail.
10. Explain in detail about the generation of antivirus.

SECTION -B (3 × 20 = 60)

Answer any THREE questions

11. a) Explain symmetric key distribution scenario.

    b) Encrypt and Decrypt the text "MCA" using Hill Cipher algorithm with given key matrix.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \qquad K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

12. Briefly explain the SHA algorithm with neat sketch.
13. Explain the operational description of PGP.
14. Explain payment processing in detail.
15. Discuss about password selection strategies and their significance.
