



MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL

Paper Code : PEC- CS801 B/PECIT801B Cryptography & Network Security
UPID : 008257

Time Allotted : 3 Hours

Full Marks : 70

The Figures in the margin indicate full marks.

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

Group-A (Very Short Answer Type Question)

1. Answer any ten of the following :

[1 x 10 = 10]

- (I) ----- measures can help reduce the risk of data leakage?
- (II) ----- creates an isolated passage across a public network that enables computing devices to communicate and receive data discreetly as though they were directly linked to the private network.
- (III) Types of firewall are -----.
- (IV) The ____ protocol is responsible for sending change Cipher Spec messages.
- (V) Asymmetric encryption offers a procedure that wraps the protected information in _____ package(s).
- (VI) AES algorithm uses _____ number of keys for encryption and decryption.
- (VII) SSL use _____ algorithm in order to provide a message integrity.
- (VIII) Which one of the following modes of operation in DES is used for operating short data?
- (IX) ----- is used to generate a message digest by the network security protocols?
- (X) In __ authentication, the claimant proves that he/she knows a secret without actually sending it
- (XI) Define firewall.
- (XII) A proxy gateway is a _____.

Group-B (Short Answer Type Question)

Answer any three of the following :

[5 x 3 = 15]

2. Define cryptography. Briefly discussed Diffusion & Confusion. [5]
3. Explain the technical details of firewall and describe any one types of firewall with neat diagram. [5]
4. Explain different types of cyber attacks to break network security. [5]
5. Compare stream cipher with block cipher with proper example. [5]
6. Define cryptanalysis? Explain different security aspect in cryptography. [5]

Group-C (Long Answer Type Question)

Answer any three of the following :

[15 x 3 = 45]

7. (a) What are the steps involved in SSL protocol. [9]
(b) Discuss the advantages of SSL protocol. [3]
(c) How it is different form TLS. [3]
8. (a) Name some viruses & explain working mechanism of those viruses. [7]
(b) Explain in detail about various types of attacks. [8]
9. (a) What do you mean by network security? [4]
(b) Discuss security mechanism for a network. [4]
(c) Describe steganography. [4]
(d) What is Zombie? [3]
10. (a) Explain the Playfair cipher with example. [8]
(b) Discuss Vernam cipher in detail. [7]
11. (a) What are Biometrics? [3]
(b) Discuss different examples of Biometrics. [7]
(c) Discuss problems with current security systems. [5]

*** END OF PAPER ***