[48]

SARDAR PATEL UNIVERSITY

B. Sc. Information Technology, 6th Semester
Wednesday, 04th April, 2018
US06CINT05: Information Security

Time: 10:00 AM to 01:00 PM   Total Marks: 70

Note: Answer of all the questions (including Multiple Choice Questions) should be written in the provided answer book only

Q:1 Give answers of following multiple choice questions   [10]

[01] The _____ attack attempts to alter system resources or affect their operation.
- (A) Active
- (B) Security
- (C) Passive
- (D) None of these

[02] Which one is the category of the Active attack?
- (A) Release of Message
- (B) Traffic Analysis
- (C) Masquerade
- (D) None of these

[03] _____ is the protection of transmitted data from passive attacks.
- (A) Confidentiality
- (B) Authentication
- (C) Access control
- (D) Data Integrity

[04] A backdoor, is also known as a _____
- (A) Hidden door
- (B) Trapdoor
- (C) Logic Bomb
- (D) None of these

[05] _____ is a piece of software that can "infect" other programs by modifying them.
- (A) Trojan Horse
- (B) Logic bomb
- (C) Virus
- (D) None of these

[06] The full form of ECB is _____
- (A) Electronic Cipherbook
- (B) Elective Codebook
- (C) Electronic Codebook
- (D) Hyper link

[07] The full form of MDC is _____
- (A) modification detection code
- (B) message detection code
- (C) modification document code
- (D) None of these

[08] A _____ is one that is used only for the duration of one session.
- (A) private key
- (B) session key
- (C) secrete key
- (D) None of these

[09] SSL stands for_____
- (A) Security Service Level
- (B) Socket Service Level
- (C) Security Socket Layer
- (D) None of these

[10] The _____ is designed to provide security at the network layer.
- (A) Pretty Good Privacy
- (B) SSL / TLS
- (C) IPSec
- (D) None of these

Q:2 Answer the following short questions (any Ten)   **[20]**

   [01] What is Security attack? Also list out its categories.
   [02] Define Terms: Plaintext and Ciphertext
   [03] List the fundamental principles of cryptography.
   [04] List various types of attacks performed on encrypted message.
   [05] Define: Virus and Worm
   [06] Define Malicious Software. Also list out its categories.
   [07] List the various security services.
   [08] List the criteria for hash function.
   [09] Explain session key in brief.
   [10] Explain IPSec protocol in brief.
   [11] Draw the diagram for tunnel mode.
   [12] Define firewall. Also list its types.

Q:3 **[A]** Write a detail note on Network Security Model.   **[06]**

   [B] Explain fundamental crypto graphical principles in brief.   **[04]**

                                    OR

Q:3 **[C]** What is cryptography? Specify the basic terms of cryptography.   **[06]**
         Also define its categories.

   [D] Explain transposition cipher in detail.   **[04]**

Q:4 **[A]** Explain the types of attacks performed on encrypted message.   **[06]**

   [B] Explain in brief phases of virus.   **[04]**

                                    OR

Q:4 **[C]** Explain ECB and CBC cipher modes in detail.   **[06]**

   [D] Explain in brief phases of virus.   **[04]**

Q:5 **[A]** Write a detail note on Message integrity.   **[10]**

                                    OR

Q:5 **[B]** List the key management methods and explain any one of them in   **[10]**
         detail.

Q:6 **[A]** Explain Tunnel mode of IPSec in detail.   **[05]**

   [B] Explain Encapsulating Security Payload protocol in detail.   **[05]**

                                    OR

Q:6 **[C]** What is firewall? List the types of firewall and explain any one of **[06]**
         them.

   [D] Explain Proxy firewall in detail.   **[04]**