SC

No. of Printed Pages: 02

[A-82]

SARDAR PATEL UNIVERSITY
External Examination
B. Sc. – Information Technology (IT) – Sixth Semester
US06CINT05: Information Security
6th April, Wednesday, 2016

Time: 02:30pm to 05:30pm Total Marks: 70

Q-1 Select an appropriate option. 10

1 A process that is designed to detect, prevent or recover from a security attack is known as _____.
(a) Security Service (b) Security Mechanism
(c) Security Attack (d) None of these

2 The _____ attack attempts to alter system resources or affect their operation.
(a) Passive (b) Active (c) Security (d) None of these

3 A _____ cipher replaces one symbol with another.
(a) Monographic (b) Substitution (c) Transposition (d) None of these

4 AES stands for _____.
(a) Asymmetric Encryption System (b) Advanced Encryption Standard
(c) Asymmetric Encryption Standard (d) None of these

5 DES is an example of a _____.
(a) complex block cipher (b) complex round cipher
(c) complex plaintext (d) None of these

6 A backdoor, is also known as a _____.
(a) Hidden door (b) Logic Bomb (c) Trapdoor (d) None of these

7 To provide confidentiality with symmetric-key cryptography, a sender and a receiver need to share a _____.
(a) secret key (b) private key (c) session key (d) none of these

8 To preserve the integrity of a message, the message is passed through an algorithm called a _____.
(a) hash function (b) hash document (c) hash digest (d)none of these

9 A _____ firewall filters at the application layer.
(a) packet filter (b) proxy (c) system (d) none of these

10 TLS stands for _____.
(a) Transport Level Service (b) Transport Layer Security
(c) Transport Level System (d) None of these

Q-2 Answer the following questions. (Any **TEN**) 20

1 Define terms: (i) Security Mechanism (ii) Security Attack
2 List the fundamental principles of cryptography.
3 Define active attack with its types.
4 List classes of intruders.
5 Explain the function of DES.
6 Define Malicious Software.
7 Differentiate between: Message authentication – Entity authentication.
8 List the criteria for hash function.
9 Explain session key.
10 Draw the diagram for transport mode.
11 Explain IPSec protocol.
12 Explain Secure Sockets Layer protocol.

Q-3
(a) Explain in detail Security Services. 5
(b) Explain transposition cipher in detail. 5

OR

Q-3
(a) Write a detail note on Network Security Model. 5
(b) What is cryptography? Specify the components of cryptography. Also define its categories. 5

Q-4
(a) Write a detail note on Data Encryption Standard. 5
(b) Explain application for public key cryptosystem. 5

OR

Q-4
(a) Explain the types of attacks performed on encrypted message. 5
(b) Explain Virus Structure in detail. 5

Q-5 Explain Message confidentiality in detail. 10

OR

Q-5 Explain Entity Authentication methods in detail. 10

Q-6
(a) Explain Authentication Header protocol in detail. 5
(b) Explain the characteristics of firewall. 5

OR

Q-6
(a) What is firewall? List the types of firewall and explain any one of them. 5
(b) Explain various services performed by SSL. 5

X=X=X