



UNIVERSITY OF THE PUNJAB

B.S. 4 Years Program / Eighth Semester – 2019

Paper: Network Security

Course Code: IT-406 Part – I (Compulsory)

Time: 15 Min. Marks: 10

Roll No. in Fig.

Roll No. in Words.

Signature of Supdt.:

ATTEMPT THIS PAPER ON THIS QUESTION SHEET ONLY.

Division of marks is given in front of each question.

This Paper will be collected back after expiry of time limit mentioned above.

Q.1. Encircle the correct option.

(10x1=10)

1. Message _____ means that the data must arrive at the receiver exactly as sent.
A. Confidentiality
B. Authentication
C. Integrity
D. None of Above
2. Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
A. Confidentiality
B. Integrity
C. Authentication
D. None of Above
3. If _____ is needed, a cryptosystem must be applied over the scheme.
A. Integrity
B. Confidentiality
C. Nonrepudiation
D. Authentication
4. A digital signature needs a
A. Private-key system
B. Shared-key system
C. Public-key system
D. All of them
5. One way to preserve integrity of a document is through use of a
A. Eye-Rays
B. Finger Print
C. Biometric
D. X-Rays
6. Which of the following is not a factor in securing the environment against an attack on security?
A. The education of the attacker
B. The system configuration
C. The network architecture
D. The business strategy of the company
E. The level of access provided to employees
7. Which of the following pieces of information can be found in the IP header?
A. Source address of the IP packet
B. Destination address for the IP packet
C. Sequence number of the IP packet
D. Both (A) and (B) only.
8. Why would a hacker use a proxy server?
A. To create a stronger connection with the target.
B. To create a ghost server on the network.
C. To obtain a remote access connection.
D. To hide malicious activity on the network.
9. Encryption and decryption provide secrecy, or confidentiality, but not
A. Authentication
B. Integrity
C. Privacy
D. All of above
10. Digital signature provides _____.
A. Authentication
B. Both (A) and (B)
C. Nonrepudiation
D. None of it



UNIVERSITY OF THE PUNJAB
B.S. 4 Years Program / Eighth Semester – 2019

Paper: Network Security

Course Code: IT-406 Part – II

Roll No.
Time: 2 Hrs. 45 Min. Marks: 50

ATTEMPT THIS (SUBJECTIVE) ON THE SEPARATE ANSWER SHEET PROVIDED

Question #2.

(4*5=20)

Write the short answers of the following question.

1. Describe the Block Cipher Principles and The Data Encryption Standard?
2. Discuss the role of Ticket Granting Server (TGS) in inter realm operations of Kerberos?
3. Explain the Advanced Encryption Standard, Evaluation Criteria For AES?
4. Explain the viruses, Trojan horse and Worms?
5. Discuss and explain The Strength of Des and Differential and Linear Cryptanalysis?

(Long Questions)

(3x10=30)

Question #03

Explain the Firewall Design Principles, Firewall Characteristics, Types of Firewalls and Firewall deployment with diagrams?

Question #04

- a) Describe the Key Management, Distribution of Public Keys and its following general schemes like Public announcement, Publicly available directory, Public-key authority, Public-key certificates?
- b) Briefly explain RSA?

Question #05

Describe the Intruders, Intrusion Techniques and Intrusion Detection in detail?