Network Security 2014-15

QP Code :04544

(2½ hours)

Total Marks: 75

N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. **Attempt *any two* of the following:** 10
a. What is the principle behind One Time pads? Why is it highly secure?
b. Explain the various ways of attack. (such as known plain-text attack etc.).
c. What are the two basic ways of transforming plain-text into cipher-text?
d. Explain the following principles of security:
i) Non-Repudiation ii) Integrity

2. **Attempt *any two* of the following:** 10
a. Explain CFB (Cipher Feedback) mode of algorithms.
b. What are the features of blowfish algorithm? Explain the steps in encryption process using blowfish algorithm.
c. Explain the principles/working of IDEA algorithm.
d. Explain in detail the steps in each round of DES.

3. **Attempt *any two* of the following:** 10
a. Compare symmetric and asymmetric key cryptography using their various characteristics.
b. What are the key requirements of message digest?
c. What is the difference between MAC and message digest?
d. Explain the concept of Digital Envelope?

4. **Attempt *any two* of the following:** 10
a. Write short note on private key management.
b. What is cross-certification? Why is it needed?
c. Describe the role of CA in creation/revocation of Digital Certificate.
d. Explain the steps in creation of Digital Certificate.

5. **Attempt *any two* of the following:** 10
a. What is buffer overflow attack on SSL?
b. What are the objectives of SET? How are they achieved?
c. Write a detailed note on VPN (Virtual Private Network).
d. What are the attacks on packet filter firewall?

6. **Attempt *any two* of the following:** 10
a. What is authentication token? Explain its working in brief.
b. Explain the password based authentication and the problems associated with it.
c. Explain the usage of smart cards in authentication.
d. Explain shared secret method of mutual authentication.

7. **Attempt *any three* of the following:**

a. What are the different types of criminal attacks?

b. Discuss how encryption happens in RC5.

c. Explain the working of SHA (Secure Hash Algorithm).

d. Explain PKCS#5 PBE (Password Based Encryption) standard.

e. Explain the concept of NAT (Network Address Translation).

f. Write a detailed note on biometric authentication.