14 IT
Network security sem-V
2016-17

Q. P. CODE : 363801

(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. Explain with example different approaches to implement security model.
b. Encrypt the message 'Come Home Tomorrow' using
   i. Ceaser Cipher
   ii. Simple Columnar Transposition Techniques with four columns. Order is 3,2,4,1
c. Explain how attackers misuse cookies to collect important information.
d. List possibilities of attacks when the sender of a message encrypts the plain text message into its corresponding cipher text.

2. **Attempt *any two* of the following:** **10**
a. List different types of cryptography algorithms. Explain with example.
b. Explain the steps in various rounds of AES.
c. Explain subkey generation process of blowfish algorithm.
d. Explain double DES algorithm.

3. **Attempt *any two* of the following:** **10**
a. How is RSA is used in digital signatures? Explain.
b. Explain the working of secure hash algorithm-512.
c. Explain the working of HMAC.
d. Explain Elipitic Curve Cryptography and EIGamal.

4. **Attempt *any two* of the following:** **10**
a. Describe of the various fields of X.509v3 digital certificate.
b. How is digital certificate is verified? Explain.
c. Why do we trust digital certificate?
d. List and explain public key cryptography standards.

5. **Attempt *any two* of the following:** **10**
a. Explain the handshake protocol.
b. Explain the Secure Electronic Transaction process.
c. With neat diagram write the internal operations of 3-D secure protocol.
d. List the different firewall configurations. Explain any two.

6. **Attempt *any two* of the following:** **10**
a. How does clear text password work? What are the problems with it?
b. Write a short note on key distribution center.
c. Explain the working of how challenge/response tokens.
d. What are the One-way authentication approaches? Explain any two.

[TURN OVER]

7. **Attempt *any three* of the following:** 15

a. Write a short note on phishing.

b. Explain subkey generation process of each round of international data encryption algorithm.

c. Explain with a neat diagram the man-in-middle attack.

d. Why is a self-signed certificate needed?

e. Explain the working of how pretty good privacy.

f. How does certificate-based authentication work? Explain.
