

(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:

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

10

2. Attempt any two of the following:

- List different types of cryptography algorithms. Explain with example.
- Explain the steps in various rounds of AES.
- Explain subkey generation process of blowfish algorithm.
- Explain double DES algorithm.

10

3. Attempt any two of the following:

- How is RSA is used in digital signatures? Explain.
- Explain the working of secure hash algorithm-512.
- Explain the working of HMAC.
- Explain Elipitic Curve Cryptography and ElGamal.

10

4. Attempt any two of the following:

- Describe of the various fields of X.509v3 digital certificate.
- How is digital certificate is verified? Explain.
- Why do we trust digital certificate?
- List and explain public key cryptography standards.

10

5. Attempt any two of the following:

- Explain the handshake protocol.
- Explain the Secure Electronic Transaction process.
- With neat diagram write the internal operations of 3-D secure protocol.
- List the different firewall configurations. Explain any two.

10

6. Attempt any two of the following:

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

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

SRINIVASA RAU TECHNICAL COLLEGE OF ENGINEERING  
MURUGESWARANAGAR 11/10/2016 9:51:24 AM MUPD16502 SHF