Reg. No. | | | | | | | | | | | | |

Question Paper Code : 60824

M.E./M.Tech. DEGREE EXAMINATION, MAY/JUNE 2017.

Second Semester

Computer Science and Engineering

NE 7202 — NETWORK AND INFORMATION SECURITY

(Common to M.E. Computer Science and Engineering (With Specialization in Net works) and M.Tech. Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What determines the integrity of a file or process?

2. What is a replay attack?

3. When is AES chosen instead of stream Cipher (e.g., RC4) during an SSL connection?

4. Why modular arithmetic has been used in cryptography?

5. Do you really need to use the same private/public key pair in RSA?

6. What are the security services provided by Digital Signature?

7. Enlist the purpose of access control challenges.

8. What do you mean by "Cross-Site Scripting"? What is the potential impact to servers and clients?

9. List out the requirements of Kerberos.

10. Sketch the general form for PGP message.

PART B — (5 × 13 = 65 marks)

11. (a) Who can attack cryptosystems? Discuss different categories of attack on cryptosystem. Also, distinguish between active and passive attacks. (13)

Or

(b) (i) Discuss the system specific security policy. How managerial guidance and technical specification can be used in SysSP? (8)

(ii) Who is responsible for policy management? How a policy is managed? Explain. (5)

12. (a) Brief out the encryption and decryption process of DES and depict the general — structure. List out the strengths and weaknesses of the same. (13)

Or

(b) Explain the process of deriving eight 64- bit words from the 1024-bits for processing of a single block and also discuss single round function in SHA-521 algorithm. Show the values of Wl6, W17, W18 and W19. (13)

13. (a) Describe the mathematical foundation of RSA algorithm. Perform encryption and decryption for the following.

P = 17, q = 7, e = 5, n = 119, message = 6

Use extended Euclid's algorithm to find the private key. (13)

Or

(b) John chooses Q = 101 and P = 7879. Assume (q, p, g and y): John's public key. John select h = 3 and calculate g. John choose x = 75 as the private key and calculate y. Now, John can send a message to Bob, Assume that H (M) = 22 and John choose secret no K = 50. Verify the signature. (13)

14. (a) (i) "Isn't Cross – site scripting the user's problem"? Explain in details. (5)

(ii) How to Test For Cross-site scripting Vulnerabilities? (8)

Or

(b) Describe the Canonical Data Model with an example. (13)

15. (a) For what purpose Zimmerman developed PGP? Brief the various services provided by PGP. Discuss the threats faced by an e-mail and explain its security requirements to provide a secure e-mail service. (13)

Or

(b) What are the services provided by SSL record protocol? Describe the operation of this protocol with suitable illustration. (13)

PART C — (1 × 15 = 15 marks)

16. (a) When security meets software engineering: Perform a case study of modeling secure information system. (15)

Or

(b) Design the architecture of distributed intrusion detection system with the necessary diagram. Illustrate the three common types of firewalls with diagrams. (15)