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

Question Paper Code : 50437

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2024.

Fifth/Sixth Semester

Computer Science and Engineering

CCS 354 – NETWORK SECURITY

(Common to : Computer Science and Engineering (Artificial Intelligence and Machine Learning)/Computer and Communication Engineering/Artificial Intelligence and Data Science/Information Technology)

(Regulations 2021)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate conventional encryption and public-key encryption.

2. Define message digest.

3. Write the main elements of X.509 certificate.

4. List the counter measures for replay attacks.

5. Define EAP over LAN.

6. Give examples for Denial of Service attacks.

7. List any two factors that contribute to the higher security risks of wireless networks compared to wired networks.

8. Mention any two functionalities of S/MIME.

9. What are the advantages of Application Proxy Firewall?

10. Suggest some of the counter measures for malicious intruders in cloud computing platforms.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Use Fermat's theorem to find a number between 0 and 72 with a congruent to 9794 modulo 73. (7)

(ii) Describe the basic arithmetical and logical functions used in SHA. (6)

Or

(b) (i) Discuss the types of attacks that are handled by message authentication. (6)

(ii) Discuss the steps involved in Digital Signature Algorithm (DSA) with examples. (7)

12. (a) (i) Describe the schemes that are widely used for the distribution of public keys with examples. (7)

(ii) Elaborate the key elements of PKIX architectural model with a neat diagram. (6)

Or

(b) (i) Explain the steps involved in Kerberos protocol for providing authentication service. (6)

(ii) Identify the protocol used for the following one-way authentication technique based on asymmetric encryption. And explain the protocol. (7)

$$A \rightarrow B : ID_A$$
$$B \rightarrow A : R_1$$
$$A \rightarrow B : E(PR_a, R_1)$$

13. (a) (i) Briefly describe various network access enforcement methods in detail. (6)

(ii) Describe the protocol layers that form the context of Extensible Authentication Protocol (EAP) with a neat diagram. Explain the authentication methods supported by EAP. (7)

Or

(b) Explain the SSH protocol stack in detail with a neat diagram. Explain the SSH user authentication protocol and connection protocol with the steps involved in message exchanges. (13)

14. (a) Describe the five phases of operation of IEEE 802.11i RSN in detail. (13)

Or

(b) (i) Describe the elements of MIME specification in detail. (6)

(ii) Describe the major security concerns related to mobile device security. (7)

15. (a) (i) Describe the characteristics of packet filtering firewall along with its advantages and limitations. (7)

(ii) Explain in detail the elements of a typical block in blockchain. (6)

Or

(b) (i) Describe various SecaaS categories of services offered by a service provider for cloud security with examples. (6)

(ii) With a neat diagram explain the various components of IoT security framework. (7)

PART C — (1 × 15 = 15 marks)

16. (a) (i) Perform encryption and decryption using RSA algorithm where $p = 3$; $q = 11$; $e = 7$ and $M = 5$. (6)

(ii) Consider a public-key system using RSA. Let the ciphertext C = 10 be sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M? (9)

Or

(b) The following authenticated key agreement protocol is given:

$1 : A \rightarrow B : g^x \bmod p$

$2 : B \rightarrow A : g^y \bmod p,\ E_k\left(S_B\left(g^y \bmod p,\ g^x \bmod p\right)\right)$

$3 : A \rightarrow B : E_k\left(S_A\left(g^x \bmod p,\ g^y \bmod p\right)\right)$

Assume that the parties have agreed on a (g, p) pair for Diffie-Hellman key exchange, that each user has RSA keys for digital signatures and that they have agreed on a block cipher E for use in subsequent encryption. Further, k is the agreed secret key and S_A and S_B denotes $A : s$ and $B : s$ signature operations respectively.

(i) Describe the details (as a list) $A : s$ and $B : s$ actions at receipt of messages 2 and 3 and what beliefs they have at that stage. (6)

(ii) Are A and B successfully authenticated to each other after protocol run? (9)