Reg. RA1911003033034

**SRM Institute of Science & Technology**
**Delhi NCR Campus, Modinagar, Ghaziabad**

# CYCLE TEST – 2 (SET A)

**Course/Branch: B.Tech/CSE** **Session: 2021-22**
**Subject: Network Security** **Code: 18CSE354T**
**Duration: 2 hours** **Max. Marks: 60**

## Part A

**Attempt all questions** *(10*1=10 Marks)*

1. UMTS stands for
   a. Uninterrupted Mobile Technical Services
   b. Universal Mobile Telecommunication Services
   c. Undirected Mobile Telecommunication System
   d. Universal Mobile Telecommunication System

2. In the SSL Protocol, each upper layer message if fragmented into a maximum of _____ bytes.
   a. $2^{12}$ b. $2^{14}$ c. $2^{16}$ d. $2^{32}$

3. SSL Stands for
   a. Secure Source Layer b. Secure Socket Layer
   c. Secure Series Locked d. Secure Semantic Layer

4. TLS used at
   a. Transport Layer System b. Transmission Layer Security
   c. Transport Layer Security d. Transaction layer Security

5. Which protocol is used to convey SSL related alerts to the peer entity?
   a) Alert Protocol b) Handshake Protocol
   c) Upper-Layer Protocol d) Change Cipher Spec Protocol

6. Which of the following are possible sizes of MACs?
   a. 12 Bytes b. 16 Bytes. c. 20 Bytes. d. 24 Bytes

7. MAC stands for
   a. Message Authentication Center b. Msg And Cipher
   c. Medium Access Control d. Media and Crime

8. In the alert protocol the first byte takes the value 1 or 2 which corresponds to _____ and _____ respectively.
   a. Select, Alarm b. Alert, Alarm
   c. Warning, Alarm d. Warning, Fatal

9. When a hash function is used to provide message authentication, the hash function value is referred to as
   a) Message Field b) Message Digest
   c) Message Score d) Message Leap

10. Which one of the following is not an application hash functions?
    a) One-way password file b) Key wrapping
    c) Virus Detection d) Intrusion detection

## Part B

**Attempt any Five Questions** **(5*4=20 Marks)**

11. Explain the layer that we used in SSL.
12. List out the security goals for UMTS
13. Define ALERT protocol in SSL
14. Define SQL injection.
15. Explain in short Public Key Infrastructure.
16. Explain the diagrammatically representation of SSL.
17. Difference in between Infrastructure and AdHoc Infrastructure.

## Part C

**Attempt any Three Questions** **(3*10=30 Marks)**

18. What kind of Encryption we use in Secure Socket layer? Explain in details with suitable diagram.
19. Define the Handshake protocol for Transport Layer Security.
20. Define GSM with associated securities with suitable diagram.
21. Explain the Record Protocol for SSL.
22. Define Cross Site Scripting (XSS) in details.

Reg. RA1911003030134

SET- B

SRM Institute of Science & Technology
Delhi NCR Campus, Modinagar, Ghaziabad
CYCLE TEST – 2

**Course/Branch: B. Tech/CSE** **Session:**
**Subject: Network Security** **Code: 18CSE354T**
**Duration: 2 hours** **Max. Marks: 60**

**Attempt all questions (10*1=10 Marks)**

**Part A**

1. Which component is included in IP security?
   a) Authentication Header (AH) b) Encapsulating Security Payload
   c) Internet key Exchange (IKE) d) All of the mentioned
2. Which two types of IPsec can be used to secure communications between two LANs?
   a) AH tunnel mode. d) ESP transport mode
   c) Both AH tunnel mode and ESP tunnel mode b) ESP tunnel mode
3. Public key cryptosystem is used for the encryption of
   a) Messages b) Session c) Session key & Message d) Public Key
4. In tunnel mode, IPSec protects the _____
   a) Entire IP packet b) IP header c) IP payload d) IP trailer
5. In which phase of IKE protocol is peer authentication performed?
   a) Phase 1 b) Pre initialization Phase c) Phase 2
   d) No peer authentication is performed.
6. Q1 S/MIME is abbreviated as _____
   a) Secure/Multimedia Internet Mailing Extensions
   b) Secure/Multipurpose Internet Mailing Extensions
   c) Secure/Multimedia Internet Mail Extensions
   d) Secure/Multipurpose Internet Mail Extensions
7. which of the following encryption algorithm are supported by SMIME
   a. RSA. b. DESc. 3DESd. SHA
8. From the options below, which of them is not a threat to information security?
   a) Disaster b) Eavesdropping c) Information leakage
   d) Unchanged default password
9. Which of the following is not a secured mail transferring methodology?
   a) POP3 b) SSMTP c) Mail using PGP d) S/MIME
10. Which mode of IPsec should you use to assure the security and confidentiality of data within the same LAN?
    a. AH transport mode b. ESP transport mode
    c. ESP tunnel mode d. AH tunnel mode

**Part B**

**Attempt any Five Questions** **(5*4=20 Marks)**

11. Explain the role of private key and public key in email security.
12. How is ISAKMP distinct from key exchange protocols?
13. Define IPSec in short.
14. Write down the five applications of IP Security.
15. Discuss the source authentication based on public key technology.
16. Differentiate between IPv4 and IPv6 in context to security.
17. Write a short note on Security services for e-mail.

C A C A D D D , A B

## Part C

**Attempt any Three Questions** **(3*10=30 Marks)**

18.Explain security policy database in brief. Write each entry information only contain in security policy database

19. What is IKE (Internet Key Exchange)? Define the phases of IKE in details with suitable diagram.

20. Explain PGP in details. Also explain the digital signature with suitable diagram.

21. What are the advantages of MIME over the SMTP.

22. Explain the Transport and Tunnel mode for AH and ESP with suitable diagram.