SRI VIDYA COLLEGE OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
QUESTION BANK

Year / Dept / Sem:	**IV / CSE / 07**	**Subject code:**	**CS6551**
Staff Name :	**M.Mohana**	**SubjectName:**	**Cryptography and Network Security**

UNIT-IV
PART-A

1. Define Kerberos.

Kerberos is an authentication service developed as part of project Athena at MIT. The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

2. What is Kerberos? What are the uses?

Kerberos is an authentication service developed as a part of project Athena at MIT.Kerberos provide a centralized authentication server whose functions is to authenticate servers.

3. What 4 requirements were defined by Kerberos?

- Secure
- Reliable
- Transparent
- Scalable

4. In the content of Kerberos, what is realm?

- A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:

- The Kerberos server must have user ID and hashed password of all participating users in its database.

- The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".

5. What is the purpose of X.509 standard?

X.509 defines framework for authentication services by the X.500 directory to its users.X.509 defines authentication protocols based on public key certificates.

8. List the 3 classes of intruder?

Classes of Intruders

- Masquerader
- Misfeasor
- Clandestine user

9. Define virus. Specify the types of viruses?

- A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program.
  Types:
- Parasitic virus
- Memory-resident virus
- Boot sector virus
- Stealth virus
- Polymorphic virus

10. What is application level gateway?

An application level gateway also called a proxy server; act as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

11. List the design goals of firewalls?

- All traffic from inside to outside, and vise versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

12. What are the steps involved in SET Transaction?

- The customer opens an account
- The customer receives a certificate
- Merchants have their own certificate
- The customer places an order.
- The merchant is verified.
- The order and payment are sent.
- The merchant requests payment authorization.
- The merchant confirm the order.
- The merchant provides the goods or services.
- The merchant requests payment.

13. What is dual signature? What it is purpose?

The purpose of the dual signature is to link two messages that intended for two different recipients.To avoid misplacement of orders.

14. Give SSL record format?

<table>
<tr><td>Content type</td><td>Major version</td><td>Minor version</td><td>Compressed length</td></tr>
<tr><td colspan="4">Plain text(Optimality compressed)</td></tr>
<tr><td colspan="4">MAC 0,16,or 20bytes.</td></tr>
</table>

15. What is the need for authentication applications?

- Security for E-mail
- Internet protocol security
- IP address security.

16. Differentiate public key encryption and conventional encryption.

Conventional encryption	Public key encryption
Same algorithm with same key used for encryption and decryption.	Same algorithm Is used for encryption and decryption with a pair of keys.
Sender and receiver must share the algorithm and keys.	Sender and reciver have one of the matched pair keys.
Key must be kept secret.	Any one of the key must be kept secretly.

17. What is message authentication?

Message authentication is a process that verifies whether the recived message comes from assigned source has not been altered.

18. Specify the requirements for message authentication?

- Disclosure
- Traffic analysis
- Masquerade
- Content modification
- Sequence modification
- Timing modification
- Repudiation.

19. Specify the four categories of security threats?

- Interruption
- Interception
- Modification
- Fabrication

20. What do you mean by SET? What are the features of SET?

SET is an open encryption and security specification designed to protect credit card transaction on the Internet.

21. Write any 3 hash algorithm?

- MD5 algorithm
- SHA-I
- RIPEMD-160 algorithm.

22. Define the classes of message authentication function.

- Message encryption
- Meassage authentication code
- Hash function.

23. List out the four phases of virus.

- Dormant phase
- Propogation phase
- Triggering phase
- Execution phase

24. What is worm?

A worm is a program that can relicate itself and send copies from computer to computer across network connections.

25. What is Bastion host?

Bastion host is a system identified by firewall administrator as critical strong point in network security.

26. What is a trusted software?

Trusted software a system that enhance the ability of a system to defend against intruders and malicious programs by implementing trusted system technology.

27. Four general techniques of firewall.

- Security control
- Direction control
- User control
- Behaviour control

28. Three types of firewall.

- Packet filter
- Application level gateway
- Circuit level gateway.

29. List approaches for intrusion detection.

- Statistical anamoly detection
- Rule based detection

30. What is intruder?

An intruder is an attacker who tries tog an unauthorized access to a system.

31. What is mean by SET? What are the features of SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet.

Features are:

a). Confidentiality of information

b). Integrity of data

c). Cardholder account authentication

d). Merchant authentication

32. What is Zombie?

A Zombie is a program that securely takes over another internet-attached computer and then uses that computer to launch attacks are difficult to trace the Zombie's creator.

PART-B

1. Explain in detail about KDC.
2. Explain the different ways of public key distribution in detail.
3. What is Kerberos? Explain how it provides authenticated service.
4. Explain the format of the X.509 certificate.
5. Explain the technical details of firewall and describe any three types of firewall with neat diagram.
6. Write short notes on Intrusion Detection.
7. Define virus. Explain in detail.
8. Describe trusted system in detail.
9. Explain the technical details of firewall and describe any three types of firewall with neat diagram.
10. Write short notes on Intrusion Detection.
11. Explain any two approaches for intrusion detection.
12. Explain firewalls and how they prevent intrusions.
13. Define intrusion detection and the different types of detection mechanisms, in detail.
14. Explain the types of Host based intrusion detection. List any two IDS software available.
15. What are the positive and negative effects of firewall?
16. Describe the familiar types of firewall configurations.
17. Explain Intrusion detection.
18. Explain the firewall design principles.
19. Name some viruses & explain it.
20. Describe about trusted systems.