1) What is cryptography
2) what is difference between symmetric and asymmetric encryption
3)what is firewall
4) what is IDS
5) what is SSL/TSL
6)what is hashing
7) what is RSA
8)what is AES
9)what is digital signature
10)what is VPN
11)what is Ddos attack,dos
12)what is honeypot
13)what is ransomware
14)what is Cipher
15)what is symmetric encryption and asymmetric encryption

Edited 20:37

1. **What is cryptography?**
    - Cryptography is the practice of securing information by converting it into unreadable code to prevent unauthorized access.
2. **What is the difference between symmetric and asymmetric encryption?**
    - **Symmetric encryption** uses the same key for both encryption and decryption, while **asymmetric encryption** uses a pair of keys—public for encryption and private for decryption.

3. **What is a firewall?**
    - A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on security rules.
4. **What is an intrusion detection system (IDS)?**
    - IDS is a device or software that monitors network traffic for suspicious activity and potential threats.
5. **What is SSL/TLS?**
    - Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are protocols used to secure communications over a computer network.

7. **What is hashing?**
    - Hashing is the process of converting input data of any size into a fixed-size string of characters, which is typically a digest that uniquely represents the data.

What is RSA in 1 line

RSA is an asymmetric cryptographic algorithm used for secure data transmission, relying on a pair of public and private keys.

- ***AES (Advanced Encryption Standard)*** is a symmetric encryption algorithm that encrypts data in ***fixed block sizes*** (128, 192, or 256 bits).

4. **What is a digital signature?**
    - An electronic signature used to verify the authenticity of a message or document.

11. **What is a VPN?**
    - A Virtual Private Network allows secure access to a private network over the internet.

20. **What is a denial-of-service (DoS) attack?**
    - An attack designed to shut down a machine or network by overwhelming it with traffic.
21. **What is a distributed denial-of-service (DDoS) attack?**
    - A DoS attack performed from multiple systems targeting one system or network.

42. **What is a honeypot?**

- A decoy system designed to lure attackers and gather information on their techniques.

16. **What is a worm?**
    - Malware that replicates itself and spreads to other computers without needing to attach to programs.
17. **What is a trojan horse?**
    - Malicious software disguised as legitimate software.
18. **What is ransomware?**
    - Malware that encrypts a victim's data and demands payment for decryption.
19. **What is phishing?**
    - Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.

5. **What is a cipher?**
    - An algorithm used to perform encryption or decryption.

2. **What is the difference between symmetric and asymmetric encryption?**
    - **Symmetric encryption** uses the same key for both encryption and decryption, while **asymmetric encryption** uses a pair of keys—public for encryption and private for decryption.

Module I: Introduction to Network Security & Cryptography

1. ***What is the CIA triad in network security?***

- CIA stands for ***Confidentiality***, ***Integrity***, and ***Availability***, which are the three key principles of information security.

2. ***How does a Vigenère cipher work?***

- It uses a ***keyword*** to shift the letters in the plaintext, repeating the keyword across the message to create a polyalphabetic cipher.

3. ***What is the difference between mono-alphabetic and poly-alphabetic substitution?***

- ***Mono-alphabetic*** uses a single fixed substitution for the entire text, while ***poly-alphabetic*** changes the substitution based on multiple alphabets (like in Vigenère).

4. ***Explain the concept of steganography.***

- It is the practice of ***hiding information*** within another medium, such as embedding a message inside an image or audio file.

information* within another medium, such as embedding a message inside an image or audio file.

5. ***What are the roles of the OSI security architecture?***
   - The OSI architecture defines security services like ***confidentiality, integrity, authentication***, and ***access control*** at different layers of communication.

Module II: Key Management, Distribution, and User Authentication

1. ***What is the purpose of public key cryptography?***
   - It enables ***secure communication*** by using a public-private key pair where the public key encrypts the data, and the private key decrypts it.

2. ***Explain the AES encryption algorithm briefly.***
   - ***AES (Advanced Encryption Standard)*** is a symmetric encryption algorithm that encrypts

- It enables ***secure communication*** by using a public-private key pair where the public key encrypts the data, and the private key decrypts it.

2. ***Explain the AES encryption algorithm briefly.***
- ***AES (Advanced Encryption Standard)*** is a symmetric encryption algorithm that encrypts data in ***fixed block sizes*** (128, 192, or 256 bits).

3. ***What is a digital signature? How is it used?***
- A digital signature ensures the ***authenticity and integrity*** of a message, proving it was not tampered with and came from the claimed sender.

4. ***How does Kerberos authentication work?***
- Kerberos uses ***tickets*** issued by a trusted authority to authenticate users securely over a network without transmitting passwords.

5. ***What is the difference betwee RSA and DSS digital signatures

5. ***What is the difference between RSA and DSS digital signatures?***

- ***RSA*** can be used for both encryption and signing, while ***DSS*** (Digital Signature Standard) is optimized for signatures only, often using ***SHA*** for hashing.

Module III: Malicious Software

1. ***Define a Trojan horse and how it differs from a virus.***

- A ***Trojan*** disguises itself as legitimate software to harm the system, while a ***virus*** replicates by attaching to files.

2. ***What is a rootkit, and how does it compromise a system?***

- A ***rootkit*** hides malicious processes or files, giving attackers ***privileged access*** to the system without detection.

3. ***Explain the concept of a denial-of-service (DoS) attack.***

- A DoS attack ***overwhelms*** a

processes or files, giving attackers *privileged access* to the system without detection.

3. *Explain the concept of a denial-of-service (DoS) attack.*
- A DoS attack *overwhelms* a target system or network with traffic to make it unavailable to legitimate users.

4. *What is phishing? Give an example.*
- *Phishing* is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity, e.g., *fake emails* asking for bank credentials.

5. *How do keyloggers work?*
- A *keylogger* captures and records the keystrokes made by a user to steal sensitive information like passwords or messages.

Module IV: IP Security, Transport Layer Security, and Email Security

1. *What is IPsec, and why is it

Module IV: IP Security, Transport Layer Security, and Email Security

1. ***What is IPsec, and why is it used?***

- ***IPsec*** is a protocol suite for securing Internet Protocol (IP) communications by encrypting and authenticating each IP packet.

2. ***Differentiate between AH and ESP protocols in IPsec.***

- ***AH (Authentication Header)*** ensures integrity and authentication, while ***ESP (Encapsulating Security Payload)*** provides both encryption and integrity.

3. ***What is the purpose of a VPN?***

- A ***VPN (Virtual Private Network)*** provides a ***secure, encrypted connection*** over the internet, protecting data from interception.

4. ***How does TLS ensure secure communication?***

- ***TLS (Transport Layer Security)***

4. ***How does TLS ensure secure communication?***
   - ***TLS (Transport Layer Security)*** encrypts data exchanged between a client and server, ensuring ***confidentiality and integrity***.

5. ***What is the difference between HTTPS and HTTP?***
   - ***HTTPS*** is the secure version of ***HTTP***, using TLS or SSL to encrypt the communication between a client and server.

Module V: Network Management Security and Network Access Control

1. ***What is SNMP, and how is it used for network management?***
   - ***SNMP (Simple Network Management Protocol)*** allows administrators to monitor and manage devices on a network, such as routers and switches.

2. ***Define NAC and its role in network security.***

2. ***Define NAC and its role in network security.***
- ***NAC (Network Access Control)*** ensures that only authorized and compliant devices can connect to a network.

3. ***What is the significance of enforcement methods in NAC solutions?***
- Enforcement methods ensure that ***non-compliant devices*** are restricted or given limited access to the network.

4. ***How does access control protect a network?***
- ***Access control*** ensures that only authorized users or devices can access network resources, preventing unauthorized access.

5. ***Name some common network management security tools.***
- Tools include ***firewalls, intrusion detection systems (IDS), and SNMP-based monitoring tools***.

Module VI: System Security

1. ***What is an IDS, and how does it work?***
   - An ***Intrusion Detection System (IDS)*** monitors network traffic for suspicious activities and raises alerts when such activities are detected.

2. ***What are the different types of firewalls?***
   - Firewalls can be ***packet-filtering, stateful, application-level, or next-generation firewalls***.

3. ***Explain the basic design principle of a firewall.***
   - A firewall acts as a ***barrier*** between a trusted and untrusted network, filtering traffic based on defined security rules.

4. ***What is the purpose of a firewall rules table?***
   - The ***rules table*** defines which traffic is allowed or blocked based on parameters like IP address, port number, and protocol.

5. ***What is the difference betwee***

5. ***What is the difference between stateful and stateless firewalls?***
*

- ***Stateful firewalls*** track the state of connections, while ***stateless firewalls*** filter packets individually without context.
