**1.List the principles of public key cryptosystems ?**

There are **two** basic principles of any cryptosystem i.e. **confidentiality** and **authenticity.** We have seen that the symmetric cryptosystem has a problem associated with these two principles.

In symmetric cryptography, the problem associated with confidentiality is that we all know in symmetric cryptography a secret key is used to encrypt as well as decrypt the message. So, this key must be shared by both the communicating parties by any means or they must rely on a third party for the distribution of the key i.e. key distribution centre. But relying on a third party again risks the secrecy of the secret key.Symmetric key also had an issue with authentication. To become widespread there was a need for digital signatures that assure all parties that a particular message has been sent from a particular person.

**2.Define Knapsack Problem with example.**

* Knapsack is an asymmetric-key cryptosystem which requires two keys for communication: public key and private key.
* In knapsack public key is used only for encryption and private key is used only for decryption.
* The underlying mathematical problem is the subset sum problem which can be stated as follows: ‘Given which elements from a predefined set of numbers are in knapsack, it is easy to calculate the sum of the numbers; if the sum is given (Known),it is difficult to find which elements are in the knapsack.

**3.what are authentication requirements?**

* Disclosure
* Traffic Analysis
* Masquerade
* Content modification
* Sequence modification
* Time modification
* Repudiation

**4.Mention the various types of authentications.**

* PAP - Password **Authentication** Protocol.
* CHAP - Challenge-handshake **authentication** protocol.
* EAP - Extensible **Authentication** Protocol.
* TACACS, XTACACS and TACACS+
* RADIUS.
* DIAMETER.
* Kerberos (protocol)

**5.what is the message authentication code?**

MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

**6.Define Hash functions**

A hash function is a function that takes a set of inputs of any arbitrary size and fits them into a table or other data structure that contains fixed-size elements.

A hash is a value in the table or data structure generated by the hash function used to generate that particular table or data structure. The table or data structure generated is usually called a hash table. It is also generally assumed that the time complexity of accessing data in a hash table is O(1), or constant.

**7.In the context of kerberos,what is a realm?**

Realm: A network that uses Kerberos composed of one or more servers called KDCs(Key Distribution Center).

**8.what are the five principal services provided by PGP?**

1.Authentication

2. Confidentiality

3. Compression

4. E-mail compatibility

5. Segmentation

**9.what is S/MIME?**

S/MIME is an acronym for Secure/Multipurpose Internet Mail Extensions. It references a type of public encryption and signing of MIME data (a.k.a. email messages) to verify a sender’s identity. With S/MIME, it is possible to send and receive encrypted emails.

**10.what is the difference between transport mode and tunnel mode?**

Tunnel mode:

* Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by another set of IP headers.
* It is widely implemented in site-to-site VPN scenarios.
* NAT traversal is supported with the tunnel mode.
* Additional headers are added to the packet; so the payload MSS is less.

Transport mode:

* The transport mode encrypts only the payload and ESP trailer; so the IP header of the original packet is not encrypted.
* The IPsec Transport mode is implemented for client-to-site VPN scenarios.
* NAT traversal is not supported with the transport mode.
* MSS is higher, when compared to Tunnel mode, as no additional headers are required.
* The transport mode is usually used when another tunneling protocol (such as GRE, L2TP) is used to first encapsulate the IP data packet, then IPsec is used to protect the GRE/L2TP tunnel packets.

**11.what does esp include in a padding field?**

Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length. The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word.

**12.Define ESP payload protocol.**

Encapsulating Security **Payload** (**ESP**) is a member of the Internet **Protocol** Security (IPsec) set of **protocols** that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which **ESP** operates makes it possible for VPNs to function securely.

**13.Define Authentication Header Protocol.**

An **Authentication Header** or AH is a security mechanism used in authenticating the origins of datagrams (packets of data transmitted under Internet **Protocol** or IP conditions), and in guaranteeing the integrity of the information that's being sent.

**14.what is the difference between an SSL connection and an SSL session?**

**Difference between connection** and **session** is that **connection** is a live communication channel, and **session** is a set of negotiated cryptography parameters. ... On other hand, you can renegotiate TLS parameters and create entirely new **session** without interrupting **connection**.

**15.what services are provided in the SSL record protocol?**

Provides two important services for SSL connections:

* Confidentiality – Handshake Protocol defines a secret key for conventional encryption of SSL payloads.
* Integrity – Handshake Protocol defines a shared secret key used to form a message authentication code (MAC)

**16.Give definition of intruder and list the classes of intruder.**

**Intruder** is a proactive **security** monitoring platform for internet-facing systems. ... **Intruder** provides a simple cloud based **security** solution which continually scans your digital assets, highlighting vulnerabilities and outlining remediation advice in the simplest terms.Three Classes of Intruders

* Masquerader – unauthorized user who penetrates a system exploiting a legitimate user’s account *(outside)*
* Misfeasor - legitimate user who makes unauthorized accesses or misuses his privileges *(inside)*
* Clandestine user - seizes supervisory control to evade auditing and access controls or suppress audit collection *(inside|outside)*

**17.what are the two common techniques to protect password file?**

• One-way function: The system stores only the value of a function based on the user's password.When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.

• Access control: Access to the password file is limited to one or a very few

**18.List three design goals for a firewall.**

A firewall is a network security system that is designed to monitor outgoing and incoming network traffic. It can be either hardware based or software based. The primary goals of a firewall are:

\*Any traffic going outside the system and moving into the system must pass through the firewall.

\*Only local security policy authorized traffic will be able to get into and out of the firewall.

\*Internal threats are often at bay as the firewall provides alert of a possible malware threat.

**19.what is an application -level gateway?**

The application gateway directs application web traffic to specific resources in a backend pool. You assign listeners to ports, create rules, and add resources to a backend pool.

**20.what is a circuit-level gateway?**

A circuit-level gateway is a type of firewall. Circuit-level gateways work at the session layer of the OSI model, or as a "shim-layer" between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate.

**21.Explain firewall design principles.**

Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates the threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. The alternative, increasingly accepted, is the firewall.

The firewall is inserted between the premise network and internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from internet based attacks and to provide a single choke point where security and audit can be imposed. The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

.