CNS-S-2016

1. Define digital signature

Ans: Digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. It is based on public key cryptography.

a. Explain PKIA model.

Ans: Public Key Infrastructure X.509 provides assurance of public key. It provides the identification of public keys and their distribution. PKIX has following components.

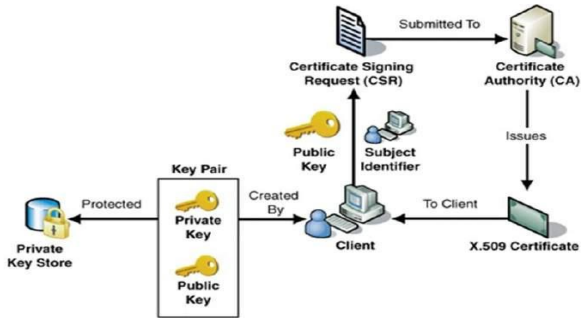
- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

o Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

o Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

o CA digitally signs this entire information and includes digital signature in the certificate.

o Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.



Certifying Authority (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

Registration Authority (RA)

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

Private Key Tokens

While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

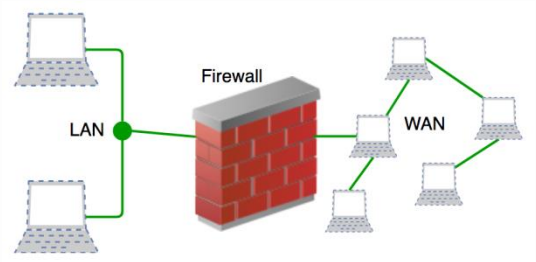
The procedure is given below

- A client whose authenticity is being verified supplies his certificate, generally along with the chain of certificates up to Root CA.
- Verifier takes the certificate and validates by using public key of issuer. The issuer's public key is found in the issuer's certificate which is in the chain next to client's certificate.
- Now if the higher CA who has signed the issuer's certificate, is trusted by the verifier, verification is successful and stops here.
- Else, the issuer's certificate is verified in a similar manner as done for client in above steps. This process continues till either trusted CA is found in between or else it continues till Root CA.

b. Define firewall. Explain different types of firewall.

Ans: Firewall is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and based on defined set of security rules it accept, reject or drop that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply
Firewall establishes a barrier between secured internal networks and outside untrusted network, such as Internet.



Types of firewall:

Packet Filtering Firewall : Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).
Packet firewalls treats each packet in Isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

Stateful Inspection Firewall : Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

Application Layer Firewall : Application layer firewall can inspect and filter the packets on any OSI layer, up to application layer. It has ability to block specific content, also recognize when certain

application and protocols (like HTTP, FTP) are being misused.
In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents direct connection between either side of firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

Host- based Firewalls : Host-based firewall are installed on each network node which controls each incoming and outgoing packet. It is a software application or suit of applications, comes as a part of operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
Network-based Firewalls : Network firewall function on network level. In other words, these firewalls filters all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on firewall. A Network firewall might have two or more network interface cards (NICs). Network-based firewall is usually a dedicated system with proprietary software installed.

2. Distinguish between plaintext and cipher text.

Ans: The original intelligible messages are plane text and the transformed messages are called cipher text.

a. Explain key principles of security.

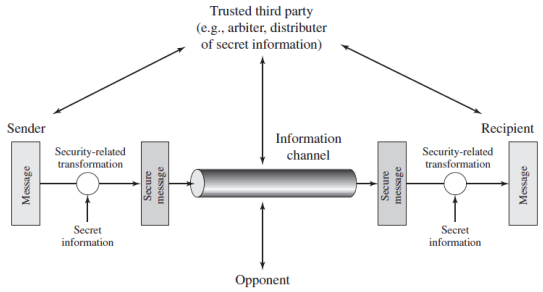
Ans: Data Confidentiality, Data Integrity, Authentication, Availability and Non-repudiation are core principles of modern-day cryptography.

- Confidentiality refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
- Data integrity refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
- Authentication is the process of making sure that the piece of data being claimed by the user belongs to it.
- Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.
- Non-repudiation refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

b. **Describe symmetric and asymmetric key cryptography**.

Ans: : In symmetric key cryptography the same key (secret key) is used for encryption and decryption. here key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.

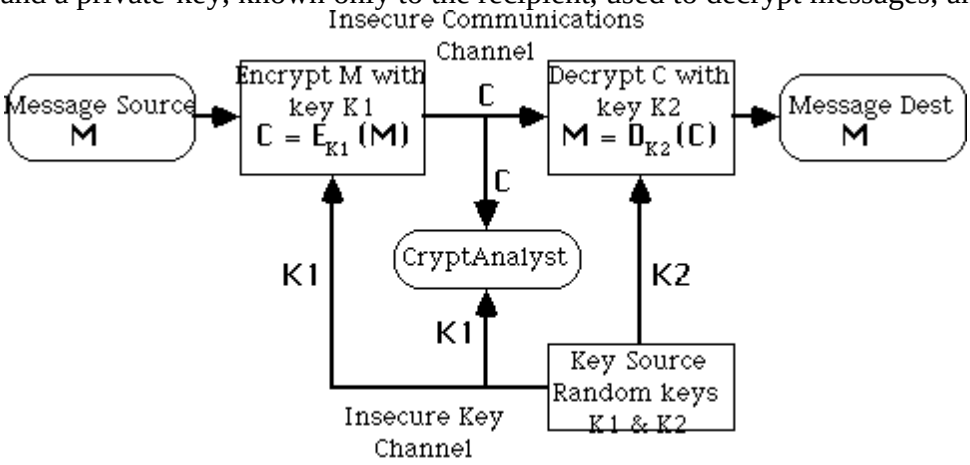
In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.
In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.



- traditional secret key cryptography uses a single key shared by both sender and receiver
- if this key is disclosed communications are compromised
- also does not protect sender from receiver forging a message & claiming is sent by sender, parties are equal

In asymmetric key cryptography two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message

Asymmetric Key Cryptography involves the use of two keys:
a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
and a private-key, known only to the recipient, used to decrypt messages, and sign signatures



Asymmetric (Public-Key) Encryption System

however, knowing the public-key and public description of the cipher, it is still computationally infeasible to compute the private key thus the public-key may be distributed to anyone wishing to communicate securly with its Owner.

SL. No.	symmetric key cryptography	asymmetric key cryptography
1	Symetric key is faster than public key.	It is slower than symmetric key cryptography.
2	In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	In asymmetric key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
3	In Symmetric key cryptography, the key is kept as a secret.	In asymmetric key cryptography, one of the two keys is kept as a

		secret.
4	Private key is Symmetrical because there is only one key that is called secret key.	Public key is Asymmetrical because there are two types of key: private and public key.
5	In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver does not need to share the same key.
6	In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.

3. What is IP security.

Ans: The Internet Protocol (IP) security is the security at the IP level which is design to authenticate and encrypts the packets of data to provide secured encrypted communication between two computers over network.

a. Define SSL and explain how it works.

Ans: The SSL protocol provides

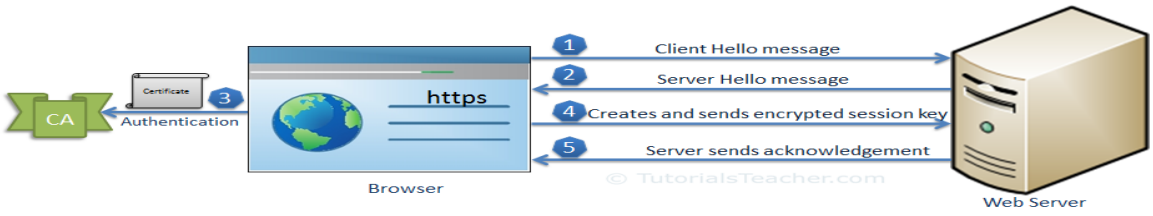
- Confidentiality − Information is exchanged in an encrypted form.
- Authentication − Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.
- Reliability − Maintains message integrity checks.

SSL communication between the browser and the web server is mainly divided into two steps: the SSL handshake and the actual data transfer.

SSL Handshake

The communication over SSL always begins with the SSL handshake. The SSL handshake is an asymmetric cryptography which allows the browser to verify the web server, get the public key and establish a secure connection before the beginning of the actual data transfer.

The following figure illustrates the steps involved in the SSL handshake:



SSL Handshake

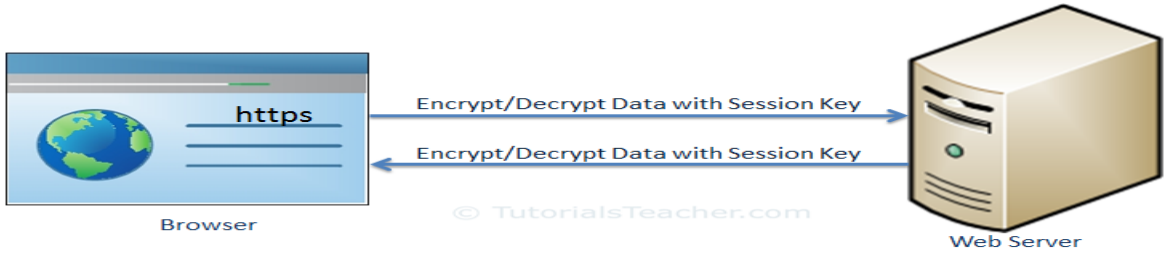
1. The client sends a "client hello" message. This includes the client's SSL version number, cipher settings, session-specific data and other information that the server needs to communicate with the client using SSL.
2. The server responds with a "server hello" message. This includes the server's SSL version number, cipher settings, session-specific data, an SSL certificate with a public key and other information that the client needs to communicate with the server over SSL.
3. The client verifies the server's SSL certificate from CA (Certificate Authority) and authenticates the server. If the authentication fails, then the client refuses the SSL connection and throws an exception. If the authentication succeeds, then proceed to step 4.

4. The client creates a session key, encrypts it with the server's public key and sends it to the server. If the server has requested client authentication (mostly in server to server communication), then the client sends his own certificate to the server.
5. The server decrypts the session key with its private key and sends the acknowledgement to the client encrypted with the session key.

Thus, at the end of the SSL handshake, both the client and the server have a valid session key which they will use to encrypt or decrypt actual data

Actual Data Transfer

The client and the server now use a shared session key to encrypt and decrypt actual data and transfer it. This is done using the same session key at both ends and so, it is a symmetric cryptography. The actual SSL data transfer uses symmetric cryptography because it is easy and takes less CPU consumption compared with the asymmetric cryptography.



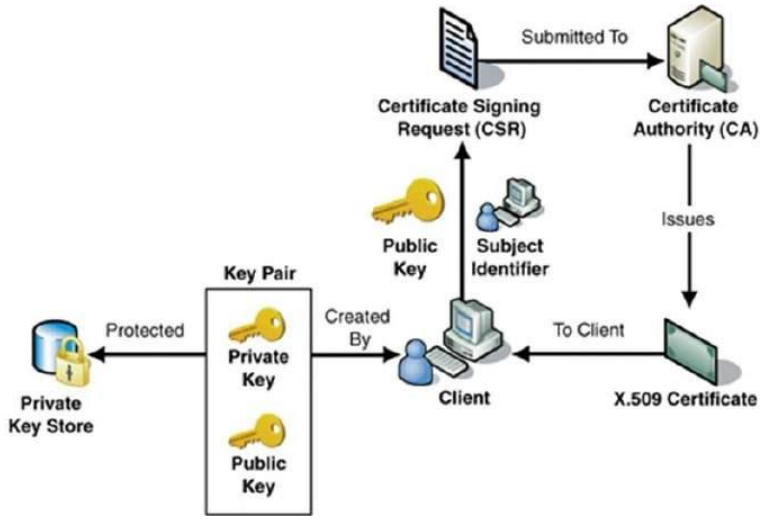
SSL Data Transfer

Thus, SSL fundamentally works using asymmetric cryptography and symmetric cryptography.

b. What is digital certificate? Describe it's procedure.

Ans: A Digital Certificate is an electronic document which provides information to prove the identity of an entity. It binds the identity of an entity to its public key. Digital certificates contain some standard information such as the name of the certificate holder, public key, validity period, and also the digital signature of the certification authority. It is issued by a certification authority (CA). These are used with self-signatures and message encryption. Digital certificates are also known as public key certificates or identity certificates.

Digital certificate creation procedure: The CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.



- Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

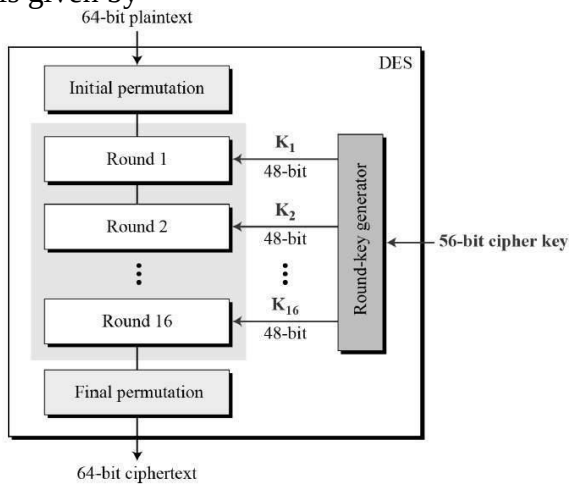
- CA digitally signs this entire information and includes digital signature in the certificate.
- Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

4. Define virus.name two virus.

Ans: It is a malicious software program loaded into the computer without user's knowledge and performs malicious action. Examples are ILOVEYOU, Code Red

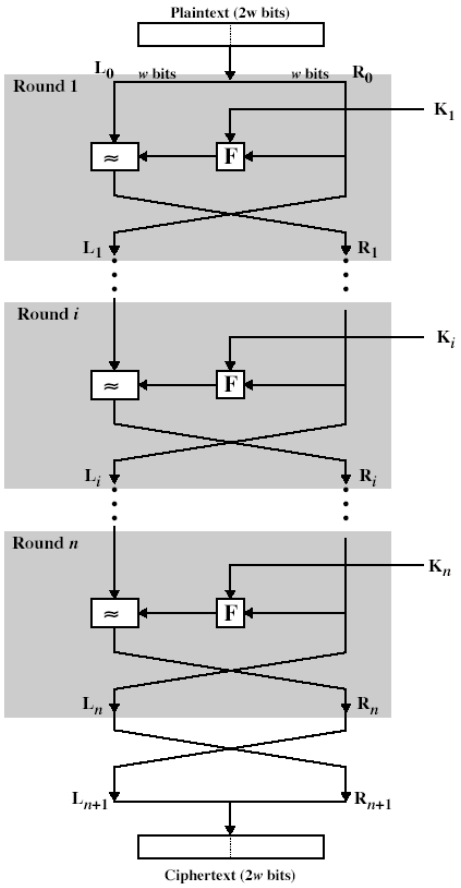
a. What is DES? Explain how does it work?

Ans: The Data Encryption Standard (DES) is a symmetric-key block cipher. DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. General Structure of DES is given by



DES has three main phases − Round function, Key schedule, Initial and final permutation.

The input to the encryption algorithm are a plaintext block of length 64bits and a key K. the plaintext block is divided into two halves L_0 and R_0 of 32 bits each. The key K of 56 bits is compressed into 48 bits by discarding the 8^{th} bit of each byte. The two halves of the data pass through 16 rounds of processing and then combine to produce the cipher text block. Each round "i" has inputs L_{i-1} and R_{i-1}, derived from the previous round, as well as the subkey K_i, derived from the overall key K. in general, the subkeys K_i are different from K and from each other. All rounds have the same structure. A substitution is performed on the left half of the data (as similar to S-DES). This is done by applying a round function F to the right half of the data and then taking the XOR of the output of that function and the left half of the data. The round function has the same general structure for each round but is parameterized by the round sub key K_i. Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data. This structure is a particular form of the substitution-permutation network.



The process of decryption is essentially the same as the encryption process. The decryption algorithm will take the cipher text as input along with the subkey K_i in reverse order. At each round, the intermediate value of the decryption process is same (equal) to the corresponding value of the encryption process with two halves of the value swapped.

After the last iteration of the encryption process, the two halves of the output are swapped, so that the cipher text is $R_{16} \| L_{16}$. The output of that round is the cipher text.

b. Describe different types of attack.

Ans: Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality.

Unauthorized party could be a person, a program or a computer.e.g., wire tapping to capture data in the network, illicit copying of files.

Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.

Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.

Cryptographic Attacks

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive

attacks are of two types:
Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.
Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.
Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.
Active attacks
These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:
Masquerade – One entity pretends to be a different entity.
Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.
It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

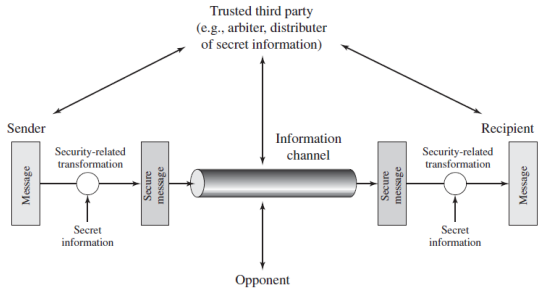
5. Define password.

Ans: it is a secret word or string of characters that allows access to a computer system or service.

a. What are different key aspect of algorithm? Explain different algorithm modes.

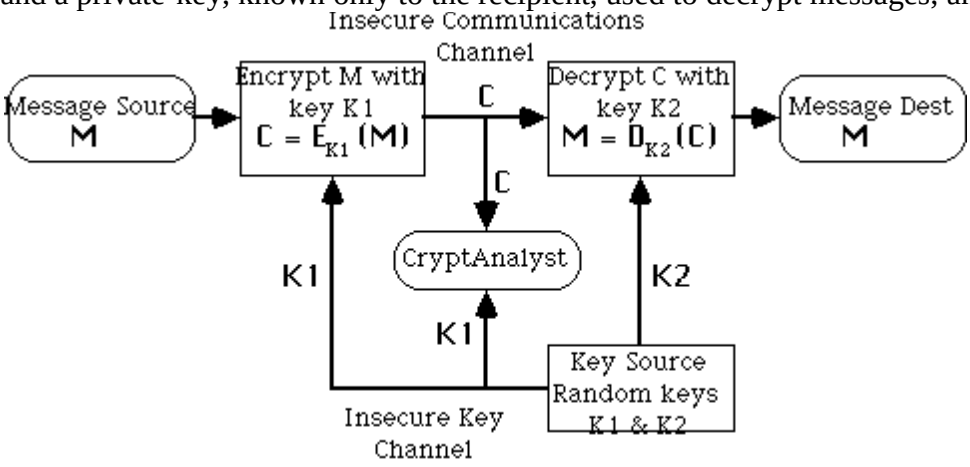
Ans: In computer network two types of cryptographic algorithms are used. Symmetric key cryptography and asymmetric key cryptography.

symmetric Key Cryptography:
In symmetric key cryptography the same key (secret key) is used for encryption and decryption. here key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography. Here the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it.In many cases, the encryption and decryption keys are the same.



Asymmetric Key Cryptography:
In asymmetric key cryptography two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message

Asymmetric Key Cryptography involves the use of two keys:
a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
and a private-key, known only to the recipient, used to decrypt messages, and sign signatures



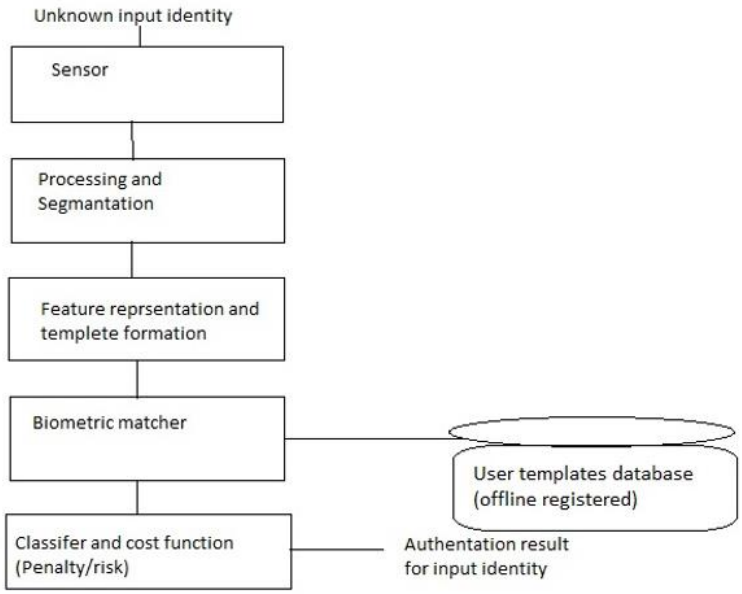
Asymmetric (Public-Key) Encryption System

however, knowing the public-key and public description of the cipher, it is still computationally infeasible to compute the private key thus the public-key may be distributed to anyone wishing to communicate securely with its Owner.

b. Define biometric Authentication? Explain it's working principle.

Ans: Biometric authentication is considered the automatic identification or identity verification of an individual using either a biological feature possesses physiological characteristics like a signature.
Biometric can be separated into two main categories:

- Physiological Characteristics: They are related to the shape of the body. The trait that has been used the longest, for over one hundred years, are fingerprints, other examples are face recognition, hand geometry and iris recognition.



- Behavioural Characteristics: They are related to the behaviour of a person. The first characteristics to be used that is still widely used today is the signature.

- Biometric samples are collected using an appropriate sensor. The samples are then processed to correct the deterministic variations like translational and rotational shifts due to interaction of a sensor with the external world. This leads to set of "discriminatory" attributes that are invariant to irrelevant transformation of the input at the sensor.
- Following this segmentation/identification is performed to extract/recognize the desired attributes from the biometric samples.
- Measurements performed on these attributes give features depending upon the representation method.
- The features so obtained are used to form a biometric template. The biometric template is stored in one of the many encrypted forms so as to avoid spoofing.
- Once the database is ready, a query template needs to be authenticated using a matcher so as to determine its similarity with templates in the database.
- The output of the matcher is a matching score which gives the degree of similarity of the query template with various templates. This is used to arrive at a decision using a classifier.

6. Distinguish between encryption and decryption.

Ans: The process of converting plaintext to cipher text using a cipher and a key is called encryption and the process of converting cipher text back into plaintext using a cipher and a key is called decryption

a. Explain the difference between substitution and transposition.

Ans**:** Substitution Cipher Technique

Substitution Cipher Technique is a traditional cipher text technique that is used to encrypt a plain text into ciphertext. In this technique, each character is substituted with other character/number or other symbol. These techniques change the identity of a character but not the position of it.

Transposition Cipher Technique

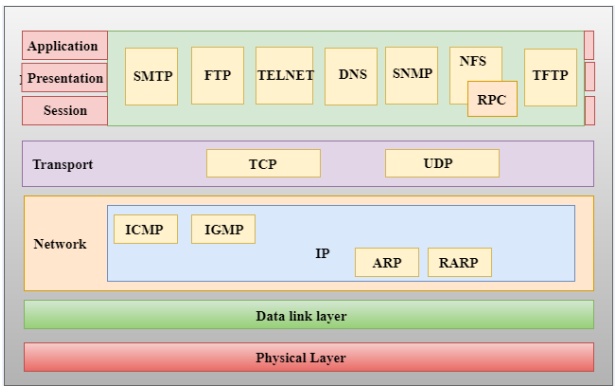
Transposition Cipher Technique is also a traditional cipher text technique that is used to encrypt a plain text into ciphertext. In this technique, each character's position is changed to a different position.

Key	Substitution	transposition
Algorithm	Each character is replaced with another character/number/symbol.	Each character is positioned differently from its original position.
Forms	Mono Alphabetic Substitution Cipher and Poly Alphabetic Substitution Cipher are its two forms.	Key-less Transposition Cipher and Keyed Transposition cipher are its two forms.
Change	Character identity is changed but the position remains the same.	Character position is changed but the identity remains the same.
Detection	A letter less frequently used can be easily traced.	A letter near to the original position gets traced easily.
Example	Caesar Cipher is an example of a Substitution Cipher.	Rail Fence Cipher is an example of Transposition Cipher.

b. What are different types of header fields inside TCP header? Explain.

Ans: The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.

- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- UDP consists of the following fields:

Source port address: The source port address is the address of the application program that has created the message.
Destination port address: The destination port address is the address of the application program that receives the message.
Total length: It defines the total number of bytes of the user datagram in bytes.
Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

7. Write short notes.

a. Smart card

Ans: A smart card is a special type of card like device which contains an integrated circuit chip embedded on it. The IC chip can be a microprocessor with memory or just simple memory circuit. In simple layman's words, a smart card is the card with which we can exchange the data, store it and manipulate data.

Smart-Card Features

- Authentication: Smart cards provide ways to authenticate others who want to gain access to the card.
- Secure data storage: Smart cards provide a way to securely store data on the card.
- Encryption: Smart cards provide a robust set of encryption capabilities, including key generation, secure key storage, hashing, and digital signing.
- Strong device security: Smart-card technology is extremely difficult to duplicate or forge, and has built-in tamper resistance.
- Secure communications: Smart cards provide secure communication between the card and reader.
- Biometrics: Smart cards provide ways to securely store biometric templates and perform biometric matching functions so improves privacy.

b. VPN

Ans: VPN allows private communication through public internet. It is essentially a logical (virtual) network within a conventional network. It makes use of cryptography (IPSec in tunnel mode) to perform private communication through insecure and public internet.

There are two common types of VPNs.

- Remote-Access—Also called a Virtual Private Dial-up Network (VPDN), this is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.
- Site-to-Site—Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Each site needs only a local connection to the same public network, thereby saving money on long private leased-lines.

c. Digital Signature

Ans: Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures. Digital signature provides following securities:

Authentication: Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.

Integrity: if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions

Non-repudiation :By this non-repudiation property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

d. TCP/IP

Ans: TCP/IP stands for Transmission Control Protocol/Internet Protocol, which is a set of networking protocols that allows two or more computers to communicate.

- It is Connection-Oriented that is a virtual connection is established before any user data is transferred.
- It is Reliable that is every transmission of data is acknowledged by the receiver.
- It is Byte Stream that is the connection is treated as a stream of bytes
- It offers Buffering of data and determining when it is time to send a datagram.
- It is Full Duplex that means transfer of data in both directions.

e. SHTTP

Ans: S-HTTP is a secure HTTP connections. S-HTTP provides a wide variety of mechanisms to provide for confidentiality, authentication, and integrity. S-HTTP is a superset of HTTP, which allows messages to be encapsulated in various ways. Encapsulations can include encryption, signing, or MAC based authentication. This encapsulation can be recursive, and a message can have several security transformations applied to it. S-HTTP also includes header definitions to provide key transfer, certificate transfer, and similar administrative functions. S-HTTP appears to be extremely flexible in what it will allow the programmer to do. S- HTTP also offers the potential for substantial user involvement in, and oversight of, the authentication & encryption activities

f. Authentication token

Ans: A authentication token is a peripheral device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password. It acts like an electronic key to access something. Examples include a wireless keycard opening a locked door, or in the case of a customer trying to access their bank account online, the use of a bank-provided token can prove that the customer is who they claim to be.

A token is a piece of data created by server, and contains information to identify a particular user and token validity. The token will contain the user's information, as well as a special token code that user can pass to the server with every method that supports authentication, instead of passing a username and password directly. An authentication is successful if a user can prove to a server that he or she is a valid user by passing a security token. The service validates the security token and processes the user request.

After the token is validated by the service, it is used to establish security context for the client, so the service can make authorization decisions or audit activity for successive user requests