CNS-S-2017

1. Differentiate between plain text and cipher text

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

a. **Working of RSA with an example**.

Ans: RSA cryptosystem is a public key cryptosystem which has two aspects. Firstly generation of key pair and secondly encryption-decryption algorithms.

1. Generation of RSA Key Pair

The process of generation of keys pair is described below −

a) Generate the RSA modulus (n)

- Select two large primes, p and q.
- Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

b) Find Derived Number (e)

- Number e must be greater than 1 and less than (p − 1)(q − 1).
- There must be no common factor for e and (p − 1)(q − 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.

c) Form the public key

- The pair of numbers (n, e) form the RSA public key and is made public.

d) Generate the private key

- Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
- Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).
- This can be written as : $ed = 1 \bmod (p-1)(q-1)$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example

- Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p − 1)(q − 1) = 6 × 12 = 72, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Hence, public key is (91, 5) and private keys is (91, 29).

2. Encryption and Decryption

RSA Encryption :

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P=10 which is a number modulo n, the encryption process is $C = P^e \bmod n$
- plaintext P , we get cipher text $C = 10^5 \bmod 91 = 82$

RSA Decryption :

- Receiver after getting C, the plaintext $P = C^d \bmod n$
- Plaintext = $82^{29} \bmod 91 = 10$

b. Explain different types of attacks.

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.

2. What is digital envelop?

Ans: A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.

a. Explain different types of encryption standards.

Ans: Advanced Encryption Standard is a symmetric encryption algorithm that encrypts fixed blocks of data (of 128 bits) at a time. The keys used to decipher the text can be 128-, 192-, or 256-bit long. The 256-bit key encrypts the data in 14 rounds, the 192-bit key in 12 rounds, and the 128-bit key in 10 rounds. Each round consists of several steps of substitution, transposition, mixing of plaintext, and more. AES encryption standards are the most commonly used encryption methods today, both for data at rest and data in transit.

Rivest-Shamir-Adleman is an asymmetric encryption algorithm that is based on the factorization of the product of two large prime numbers. Only someone with the knowledge of these numbers will be able to decode the message successfully. RSA is often used in digital signatures but works slower when large volumes of data need to be encrypted.

Triple Data Encryption Standard is a symmetric encryption and an advanced form of the DES method that encrypts blocks of data using a 56-bit key. TripleDES applies the DES cipher algorithm three times to each data block. TripleDES is commonly used to encrypt ATM PINs and UNIX passwords.

Twofish is a license-free encryption method that ciphers data blocks of 128 bits. It's considered the successor to the Blowfish encryption method that ciphered message blocks of 64 bits. Twofish always encrypts data in 16 rounds regardless of the key size. Though it works slower than AES, the Twofish encryption method continues to be used by many file and folder encryption software solutions.

b. **Explain different symmetric key algorithm**.

Ans: AES: AES is an iterative symmetric key algorithm. It is based on substitution–permutation network. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix .The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

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 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.

Triple DES uses three different keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.

- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

IDEA: It is the International Data Encryption Algorithm. IDEA was originally meant to be a replacement for the DES standard. IDEA uses a 128-bit encryption key. There are two main reasons IDEA is not as widely used as planned. The first is the fact that IDEA is subject to a range of weak keys. The second reason is that there are currently faster algorithms that produce the same level of security.
RC4: It is the fourth version of the Rivest Cipher. RC4 uses a variable length encryption key. This key can vary from 40 to 256 bits. It's most commonly used with a 128-bit key. The RC4 algorithm is very simple and easy to implement. The problem is that if implemented improperly, it can lead to weak cryptographic systems. This is one of the main reasons why RC4 is slowly being phased out. RC4 has been one of the mostly widely used encryption algorithms. It is used in WEP and WPA on wireless networks. It has also been used in Secure Sockets Layer (SSL) and Transport Layer Security (TLS) with the Hypertext Transfer Protocol over SSL (HTTPS) protocol. RC4 has also been used with secure shell, Kerberos, and the Remote Desktop Protocol.

3. Explain following terms.

i. Authentication

Ans: Authentication Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

ii. Integrity

Ans: It ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

iii. Confidentiality

Ans: It ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

iv. Non-repudiation

Ans: It requires that neither the sender nor the receiver of a message be able to deny the transmission.

b. **Differentiate between symmetric and asymmetric key cryptography**.

Ans: Symmetric Cryptography:

- It is easy to use but less secure.
- It also requires a safe method to transfer the key from one party to another.
- It only requires a single key for both encryption and decryption.
- The size of cipher text is same or smaller than the original plain text.
- The encryption process is very fast.
- It is used when a large amount of data is required to transfer.
- It only provides confidentiality.
- Examples: 3DES, AES, DES and RC4

Asymmetric Cryptography:

- It is more secure than symmetric key encryption technique.
- It requires two key one to encrypt and the other one to decrypt.
- The size of cipher text is same or larger than the original plain text.
- The encryption process is slow.
- It is used to transfer small amount of data.
- It provides confidentiality, authenticity and non-repudiation.
- Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

c. **Explain various types of transposition technique**.

Ans: Transposition technique:
In this technique some permutation is performed on the plaintext letters. Examples are Rail fence, row transposition, feistel cipher etc.
Rail fence:
Here the plaintext is written as a sequence of diagonals and then read off as a sequence of rows.
Plaintext = meet at the school house
To encipher this message with a rail fence of depth 2, we write the message as follows:
m e a t e c o l o s
e t t h s h o h u e
The encrypted message is MEATECOLOSETTHSHOHUE
Row Transposition Ciphers-
A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.
e.g., plaintext = meet at the school house
Key = 3 4 2 1 5 6 7

R/C	1	2	3	4	5	6	7
1	M	E	E	T	A	T	T
2	H	E	S	C	H	O	O
3	L	H	O	U	S	E	

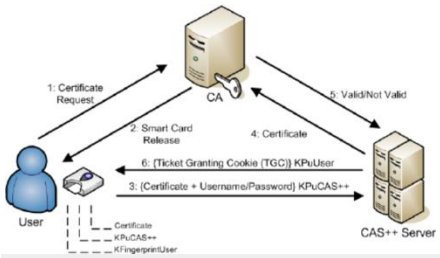
CT = ESOTCUEEHMHLAHSTOETO
Feistel cipher structure

- The input to the encryption algorithm are a plaintext block of length 2w bits and a key K.
- The plaintext block is divided into two halves L0 and R0.
- The two halves of the data pass through „n" rounds of processing and then combine to produce the ciphertext 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. The subkeys Ki 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. 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.
- 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.

4. What is data encryption?
Ans: Encryption is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information.

a. Explain certificate based authentication and biometric based authentication

Ans:

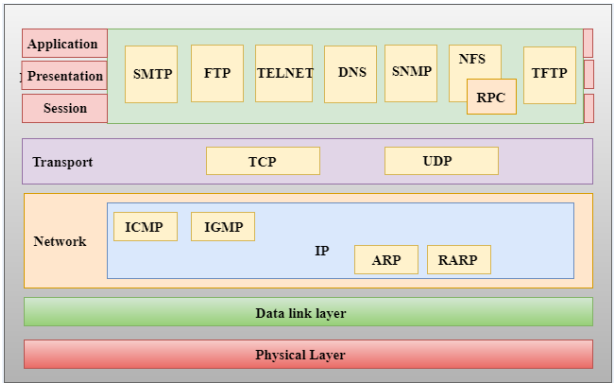


A certificate-based authentication scheme is a scheme that uses a public key cryptography and digital certificate to authenticate a user. A digital certificate is an electronic form that contains identification data, public key, and the digital signature of a certification authority derived from that certification authority's private key. When a user signs on to the server, he provides his digital certificate that has the public key and signature of the certification authority. The server then confirms the validity of the digital signature and if the certificate has been issued by a trusted certificate authority or not. The server then authenticates the user with public key cryptography to confirm the user is in possession of the private key associated with the certificate

b. What is TCP/IP. Explain the function of each layer in TCP/IP protocol suite.

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.

5. What is the role of SHTTP in cryptography?

Ans: Secure Hypertext Transfer Protocol is an obsolete alternative to the HTTPS protocol for encrypting web communications carried over HTTP.

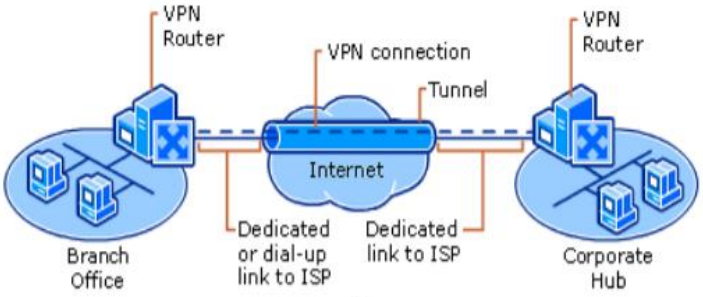
a. What is VPN? Explain it's working.

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.

VPN Architecture:



VPN Architecture

Tunneling is the process of encapsulating an entire packet within another packet and sending it over a network. Data tunneling is helpful in cases where it is desirable to hide the identity of the device originating the traffic. For example, a single device that uses IPsec encapsulates traffic that belongs to a number of hosts behind it and adds its own header on top of the existing packets. By encrypting the original packet and header (and routing the packet based on the additional layer 3 header added on top), the tunneling device effectively hides the actual source of the packet. Only the trusted peer is able to determine the true source, after it strips away the additional header and decrypts the original header. All the encryption protocols listed here also use tunneling as a means to transfer the encrypted data across the public network. It is important to realize that tunneling, by itself, does not provide data security. The original packet is merely encapsulated inside another protocol and might still be visible with a packet-capture device if not encrypted. It is mentioned here, however, since it is an integral part of how VPNs function.

A VPN offers following features.

- Data Confidentiality— Since your private data travels over a public network, data confidentiality can be attained by encrypting the data using IPsec protocol. This 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.
- IPsec— IPsec has two encryption modes: tunnel and transport. Tunnel mode encrypts the header and the payload of each packet while transport mode only encrypts the payload. Only systems that are IPsec-compliant can take advantage of this protocol. Also, all devices must use a common key or certificate and must have very similar security policies set up.
- Data Integrity— IPsec has a mechanism to ensure that the encrypted portion of the packet, or the entire header and data portion of the packet, has not been tampered with. If tampering is detected, the packet is dropped. Data integrity can also involve authenticating the remote peer.

- Data Origin Authentication—The identity of the source of the data that is sent can also verified.

b. Explain PKIX 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.

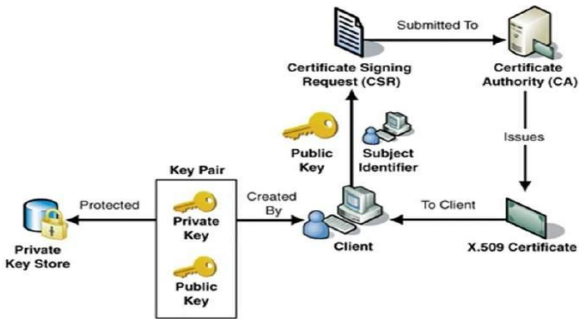
- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

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.

6. What is firewall?

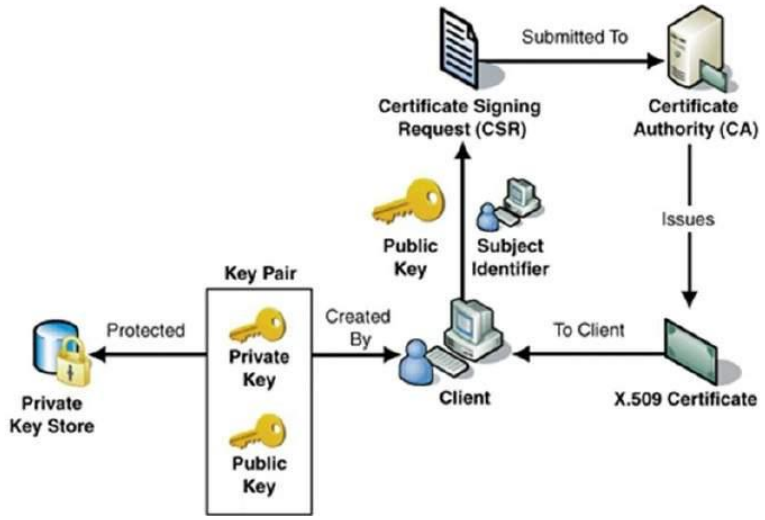
Ans: A firewall works as a barrier, or a shield, between your computer network and internet

- Its purpose is to control what traffic is allowed to be transferred from one side to the other.

a. What is digital certificate and write how to get it?

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.

b. **Explain various types of substitution technique**.

Ans: substitution technique: A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. Caesar cipher, Playfair cipher, One Time Pad Cipher is the examples of substitution technique.

Caesar cipher (or) shift cipher

The Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet.

A shift may be any amount, so that general Caesar algorithm is

$C = E(p) = (p+k) \bmod 26$

Where k takes on a value in the range 1 to 25.

The decryption algorithm is simply $P = D(C) = (C-k) \bmod 26$

Playfair cipher

The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy". The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letter „i" and „j" count as one letter.

Rules:

- Plaintext is divided into group of two letters.
- Repeating plaintext letters that would fall in the same pair are separated with a filler letter such as "x".
- Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last.
- Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.
- Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

One Time Pad Cipher

It is an unbreakable cryptosystem.

- Convert each the message into its corresponding format.
- The key is a random sequence of 0"s and 1"s of same length as the message.
- Once a key is used, it is discarded and never used again.
- The Cipher text of the plain text P is given by : $C_i = P_i \oplus K_i$ where C_i - ith binary digit of cipher text, P_i - ith binary digit of plaintext and K_i - ith binary digit of key. $\oplus$ is the exclusive OR operation.

7. Write short notes.

a. 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. That is In computing, Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection

b. Authentication basics.

Ans: Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. Authentication is used by a server when the server needs to know exactly who is accessing their information or site. Authentication is used by a client when the client needs to know that the server is system it claims to be. In authentication, the user or computer has to prove its identity to the server or client.

c. SSL

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 itself is not a single layer protocol rather it is composed of two sub-layers.

- Lower sub-layer comprises of the one component of SSL protocol called as SSL Record Protocol. This component provides integrity and confidentiality services.
- Upper sub-layer comprises of three SSL-related protocol components and an application protocol. Application component provides the information transfer service between client/server interactions.

Technically, it can operate on top of SSL layer as well. Three SSL related protocol components are −

- SSL Handshake Protocol
- Change Cipher Spec Protocol
- Alert Protocol

d. Principle of security.

- Ans: 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.

e. Digital signature

Ans: Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. That is a 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.

f. Authentication token.

Ans: 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.