CNS-S (2019)

1. a**. Distinguish between plane text and cipher text.**

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

2. a. Name various types of attack in computer system

Ans; The various types of attacks in computer system are Interruption, Interception, Modification, Fabrication.

3. a. Define smart card.

Ans: It is a plastic card with a built in microprocessor, used typically to perform financial; transaction.

4. a. Define 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.

5. a. Define time stamp protocol.

Ans: The timestamp protocol is a cryptographic protocol for certifying timestamps using X.509.the timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time.

6. a. Distinguished 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.

7. a. Define password. What is plain text password?

Ans: It is a secret word or phrase that is used for authentication purposes. Plain text password means the password text is stored exactly in text format as one writes.

1. b. Comparison 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

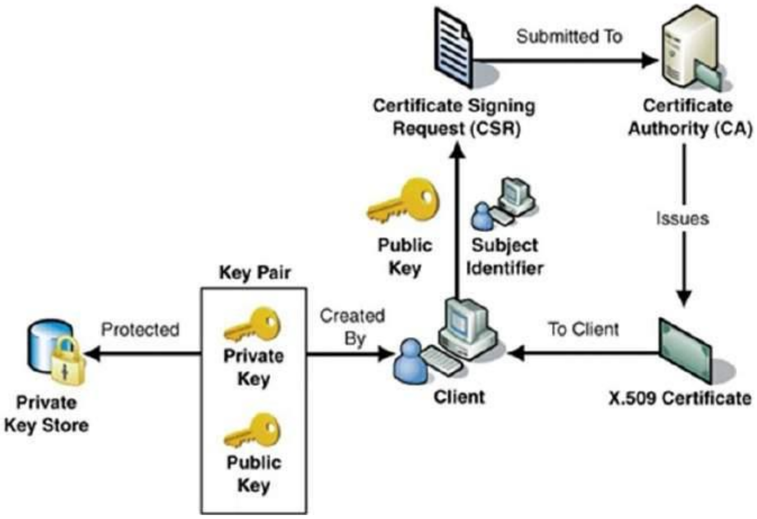
Asymmetric Cryptography:

- 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

2. b. Explain digital certificate. What are certificate creation procedures?

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.

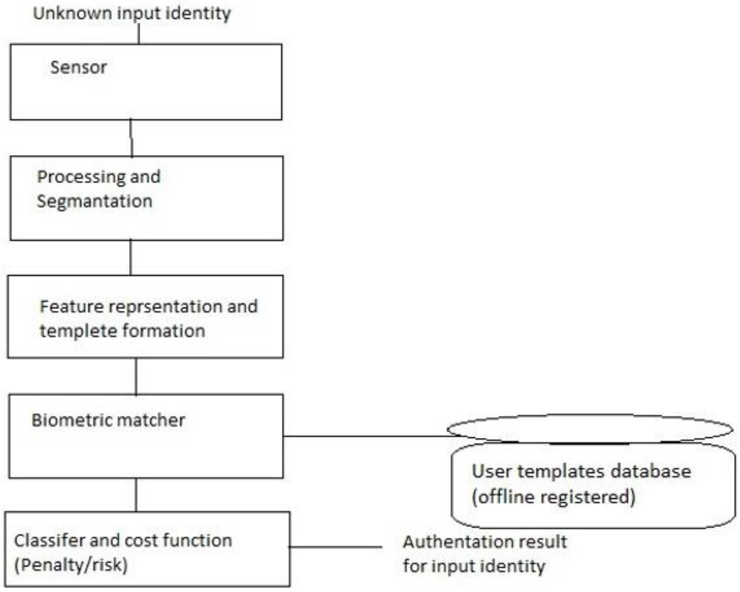
- CA digitally signs this entire information and includes digital signature in the certificate.
- Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public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

3. b. Describe biometric authentication.

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.


Unknown input identity
Sensor
Processing and Segmantation
Feature reprsentation and templete formation
Biometric matcher
User templates database (offline registered)
Classifer and cost function (Penalty/risk)
Authentation result for input identity

- 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.

4. b. Comparison 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

5. b. Explain private key management.

Ans: Since private or symmetric-key cryptography can be used for privacy and user authentication, various key management techniques used for the distribution of keys. Symmetric-key distribution involves the following problem:

- For n people to communicate with each other requires n(n-1)/2 keys. The problem is aggravated as n becomes very large.
- Each person needs to remember (n-1) keys to communicate with the the remaining (n-1) persons.
- How the two parties will acquire the shared key in a secured manner?
- To address this problem, the concept of session key has emerged. A session key is created for each session and destroyed when the session is over.

The Diffie-Hellman protocol is one of the most popular approach for providing one-time session key for both the parties.

- Used to establish a shared secret key Prerequisite: N is a large prime number such that (N-1)/2 is also a prime number. G is also a prime number. Both N and G are known to Sender and receiver • Sender chooses a large random number X and calculates $R1 = G^X \bmod N$ and sends it to receiver

- Receiver chooses another large random number Y and calculates $R2 = G^{Y} \bmod N$ and sends it to Sender
- The receiver calculates key $(K) = (R1)^{Y} \bmod N$
- The sender calculates key $(K) = (R2)^{X} \bmod N$

6. b. what are different principles of security? Explain with example.

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.

Example: Let there are two people communicating via an encrypted email they know the decryption keys of each other and they read the email by entering these keys into the email program. If someone else can read these decryption keys when they are entered into the program, then the confidentiality of that email is compromised.

- Data integrity refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

Example: Let's say you are doing an online payment of Rs.500, but your information is tampered without your knowledge in a way by sending to the seller Rs.5000, this would cost you too much.

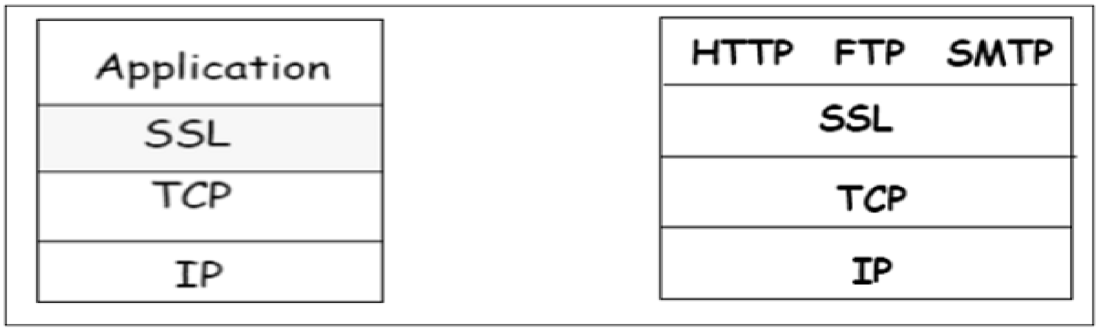
- Authentication is the process of making sure that the piece of data being claimed by the user belongs to it.
- Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.
- Example: Let's say a hacker has compromised a webserver of a bank and put it down. You as an authenticated user want to do an e-banking transfer but it is impossible to access it, the undone transfer is money lost for the bank.
- 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.

7. b. Describe position of SSL in TCP/IP protocol suite with diagram.

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.

The position of SSL protocol in TCP/IP protocol is between application and transport layer.



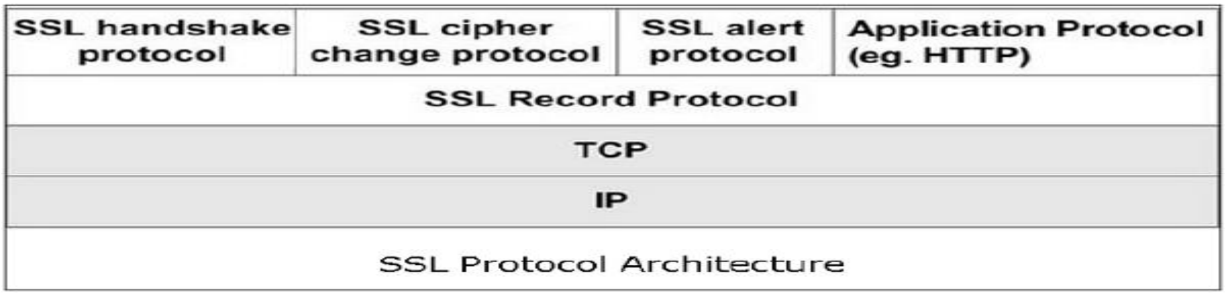
SSL itself is not a single layer protocol rather it is composed of two sub-layers.

- 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.



SSL Protocol Architecture

1. c. what do you mean by SET? Explain the SET process.

Ans: Secure Electronic Transaction (SET) is a standard protocol that is used for securing credit card transactions over insecure networks. SET itself is not a payment system. It is a a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion!

SET has following features:

- Maintains confidentiality of information: Information is provided only to the concerned recipient.
- SET takes care of Integrity of data.
- SET employs a particular subset of protocol for carrying out cardholder account authentication.
- SET employs a particular subset of protocol for carrying out Merchant authentication.

SET process: A SET system includes the following participants:

- Cardholder
- Merchant
- Issuer
- Acquirer
- Payment gateway
- Certification authority

Both cardholders and merchants must register with the CA (certificate authority) first, before they can buy or sell on the Internet. Once registration is done, cardholder and merchant can start to do transactions, which involve nine basic steps in this protocol, which is simplified.

- Customer browses the website and decides on what to purchase
- Customer sends order and payment information, which includes two parts in one message:

a. Purchase order – this part is for merchant

b. Card information – this part is for merchant’s bank only.

- Merchant forwards card information (part b) to their bank
- Merchant’s bank checks with the issuer for payment authorization
- Issuer sends authorization to the merchant’s bank
- Merchant’s bank sends authorization to the merchant
- Merchant completes the order and sends confirmation to the customer
- Merchant captures the transaction from their bank
- Issuer prints credit card bill (invoice) to the customer

2. c. Explain the RSA algorithm. Describe the example of RSA.

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 mod (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 $C = P^e$ mod n
- plaintext P , we get cipher text $C = 10^5$ mod 91=82

RSA Decryption :

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

3. c. Define Authentication token. How does this works? Explain its types.

Ans: A security 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.
Working:
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.

Token-based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, using a security token provided by the server.

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.

Types of tokens:
Static password token
The device contains a password which is physically hidden (not visible to the possessor), but which is transmitted for each authentication. This type is vulnerable to replay attacks.
Synchronous dynamic password token
A timer is used to rotate through various combinations produced by a cryptographic algorithm. The token and the authentication server must have synchronized clocks.
Asynchronous password token
A one-time password is generated without the use of a clock, either from a one-time pad or cryptographic algorithm.
Challenge response token
Using public key cryptography, it is possible to prove possession of a private key without revealing that key. The authentication server encrypts a challenge (typically a random number, or at least data with some random parts) with a public key; the device proves it possesses a copy of the matching private key by providing the decrypted challenge.

4. c. Describe substitution technique and transposition 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.

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

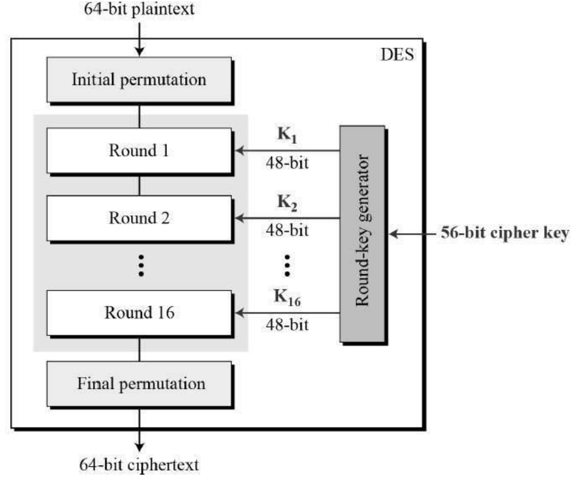
Feistel cipher structure

- 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 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. 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.

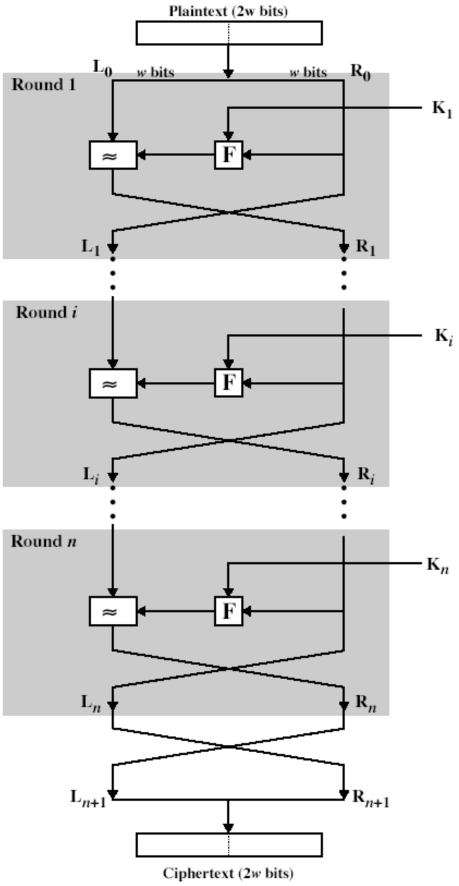
5. c. What do you mean by DES? Explain how it works?

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 8th 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.

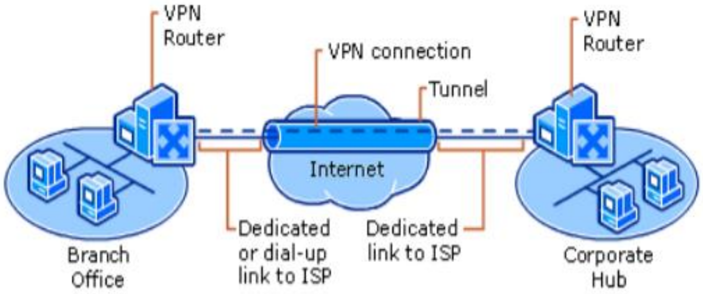
6. c. Explain VPN. Describe its architecture.

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.

7. c. Short notes

I.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.

I. **Certificate 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.

II. **Firewall**

Ans: 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. So 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. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. only authorized traffic, as defined by the local security policy, will be allowed to pass.

III. **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.