BALASORE SCHOOL OF ENGINEERING, BALASORE

DEPARTMENT OF COMPUTER SC. & ENGINEERING

SYUDY MATERIAL FOR COMPUTER SCIENCE STUDENTS

SUBJECT:- CRYPTOGRAPHY & NETWORK SECURITY

SUB.CODE:- CST-603

SEM:- 6TH

PREPARED BY:- SUCHISMITA PRADHAN

2 marks

Q-1)Differentiate between plain text and cipher text? (2017/16)

Ans-Plaintext The original intelligible message

Cipher text The transformed message

Cipher An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Q-2)What is digital envelope? (2017)

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 digital envelope is also known as a digital wrapper.

Q-3) What is data encryption? (2017)

Ans-Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

Q-4) What is role of SHTTP in cryptography? (2017/16)

Ans-S-HTTP (Secure HTTP) is an extension to the Hypertext Transfer Protocol (HTTP) that allows the secure exchange of files on the World Wide Web. Each S-HTTP file is either encrypted, contains a digital certificate, or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL). A major difference is that S-HTTP allows the client to send a certificate to authenticate the user whereas, using SSL, only the server can be authenticated. S-HTTP is more likely to be used in situations where the server represents a bank and requires authentication from the user that is more secure than a userid and password.

Q-5) What is firewall? (2017)

Ans-A **firewall** is a system designed to prevent unauthorized access to or from a private network. You can implement a **firewall** in either hardware or software form, or a combination of both. **Firewalls**prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.

Q-6) Explain following terms used in cryptography n network security.Authentication,integrity,confidentiality,nonrepudiation (2017/16)

Ans-The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

E.g. Printing, displaying and other forms of disclosure.

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

Integrity: 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.

Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.

Availability: Requires that computer system assets be available to authorized parties when needed.

Q-6) Define virus. (2017)

Ans-A computer **virus** is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The **virus** requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

Q-6) What do you mean by digital signature? (2017)

Ans-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.

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. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Q-6) Define cryptography. (2017/16)

Ans-The art or science encompassing the principles and methods of transforming an

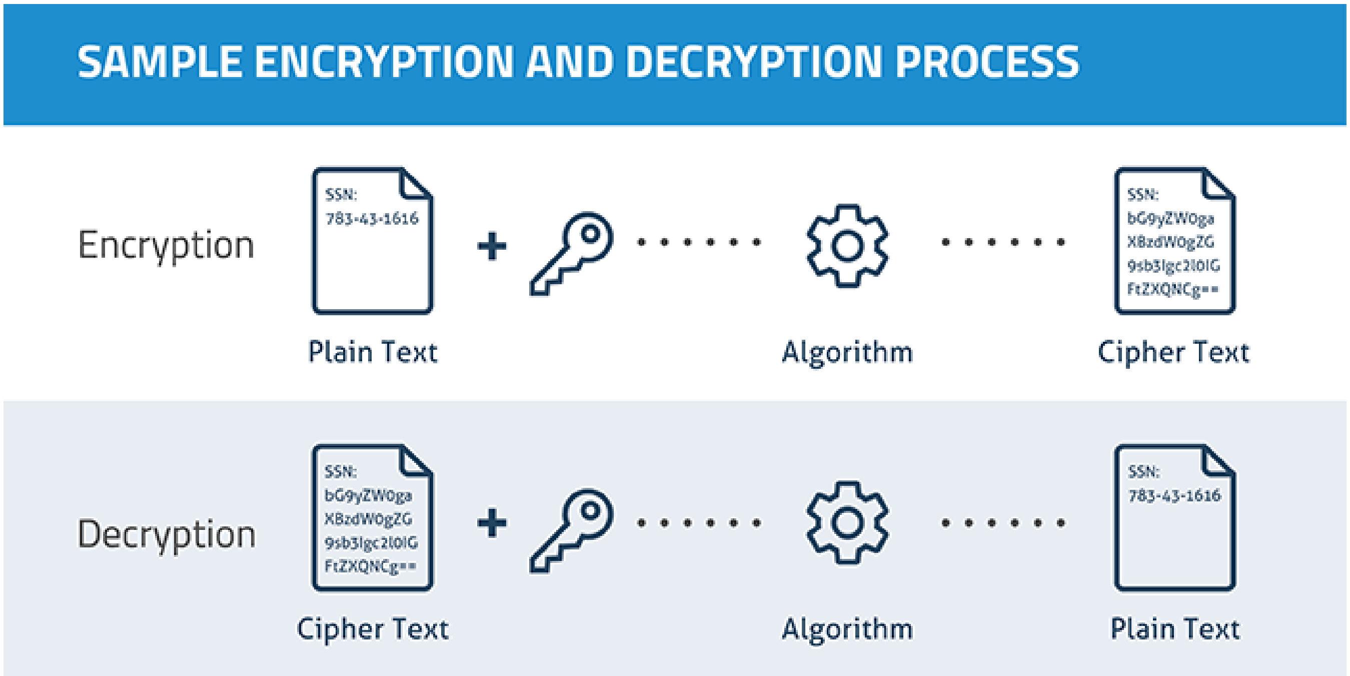
intelligible message into one that is unintelligible, and then retransforming that message back to its original form

Q-6) Define password. (2017)

Ans-A **password** is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of **password**), which is to be kept secret from those not allowed access. The use of **passwords** is known to be ancient.

Q-6) Distinguish between encryption ad decryption with example. (2017)

Ans-



Encryption is the process that transforms the original information into another form that cannot be identified. It occurs at the sender's side. This new form of the message is totally different from the initial message. Therefore, hackers cannot read this data. The sender uses an encryption algorithm and a key to transform the original message into an encrypted message. This encrypted message is also known as a **ciphertext**. Encryption is also called **enciphering**.

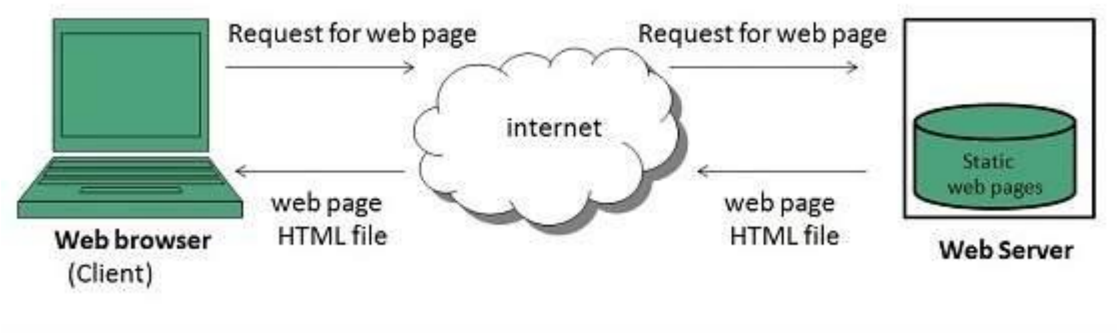
Decryption is the process of converting the received unrecognizable message back to the original message. It occurs at the receiver's end. It uses decryption algorithms and a key to transform the ciphertext back to original plaintext. The decryption is also called **deciphering**. Both sender and receiver use unique keys and they are not known to the outsiders. Decryption is the reverse process of encryption.

Q-6) What is static and dynamic page? (2016) (2017)

Ans-web page is a document available on world wide web. Web Pages are stored on web server and can be viewed using a web browser.

Static web pages are also known as flat or stationary web page. They are loaded on the client's browser as exactly they are stored on the web server. Such web pages contain only static information. User can only read the information but can't do any modification or interact with the information.

Static web pages are created using only HTML. Static web pages are only used when the information is no more required to be modified.



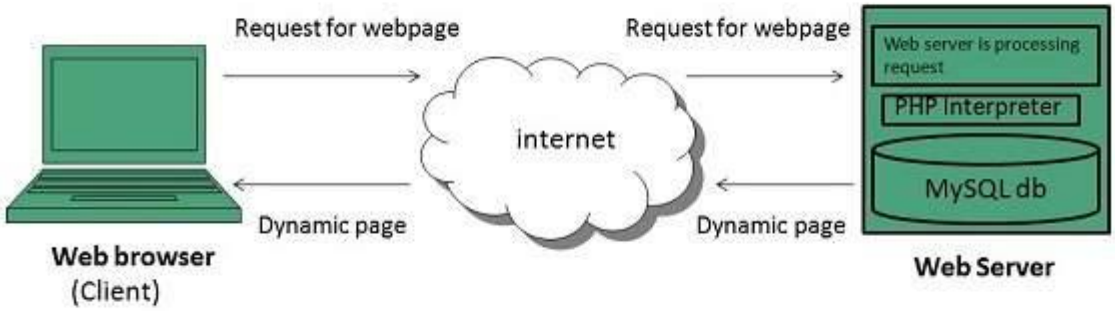
Dynamic web page shows different information at different point of time. It is possible to change a portaion of a web page without loading the entire web page. It has been made possible using **Ajax** technology.

SERVER-SIDE DYNAMIC WEB PAGE

It is created by using server-side scripting. There are server-side scripting parameters that determine how to assemble a new web page which also include setting up of more client-side processing.

CLIENT-SIDE DYNAMIC WEB PAGE

It is processed using client side scripting such as JavaScript. And then passed in to **Document Object Model (DOM).**



Q-6) What do you mean by IP security? (2017)

Ans-Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.

5 marks

Q-1)Explain the working principle of RSA algorithm through example,(2017/16)

Ans-Best known and widely regarded as most practical public-key scheme was proposed by Rivest, Shamir &Adleman in 1977:
R L Rivest, A Shamir, L Adleman, "On Digital Signatures and Public Key Cryptosystems", Communications of the ACM, vol 21 no 2, pp120-126, Feb 1978
· it is a public-key scheme which may be used for encrypting messages, exchanging keys, and creating digital signatures
· is based on exponentiation in a finite (Galois) field over integers modulo a prime o nb exponentiation takes O((log n)3) operations
· its security relies on the difficulty of calculating factors of large numbers
onb factorization takes O(e log n log log n) operations
o (same as for discrete logarithms)
· the algorithm is patented in North America (although algorithms cannot be patented elsewhere in the world)
o this is a source of legal difficulties in using the scheme

RSA is a public key encryption algorithm based on exponentiation using modular arithmetic

selecting two large primes at random (~100 digit), p, q
o calculating the system modulus R=p.q p, q primes

oselecting at random the encryption key e,

oe < R, gcd(e, F(R)) = 1

osolving the congruence to find the decryption key d,

oe.d [[equivalence]] 1 mod [[phi]](R) 0 <= d <= R

opublishing the public encryption key: K1={e,R}

osecuring the private decryption key: K2={d,p,q}

- Encryption of a message M to obtain ciphertext C is:
- C = $M_e$mod R 0 <= d <= R
- Decryption of a ciphertext C to recover the message M is:

○M = C_d = $M_{e.d}$= $M_{1+n.[[phi]](R)}$ = M mod R

- the RSA system is based on the following result:

if R = pq where p, q are distinct large primes then

X [[phi]](R) = 1 mod R

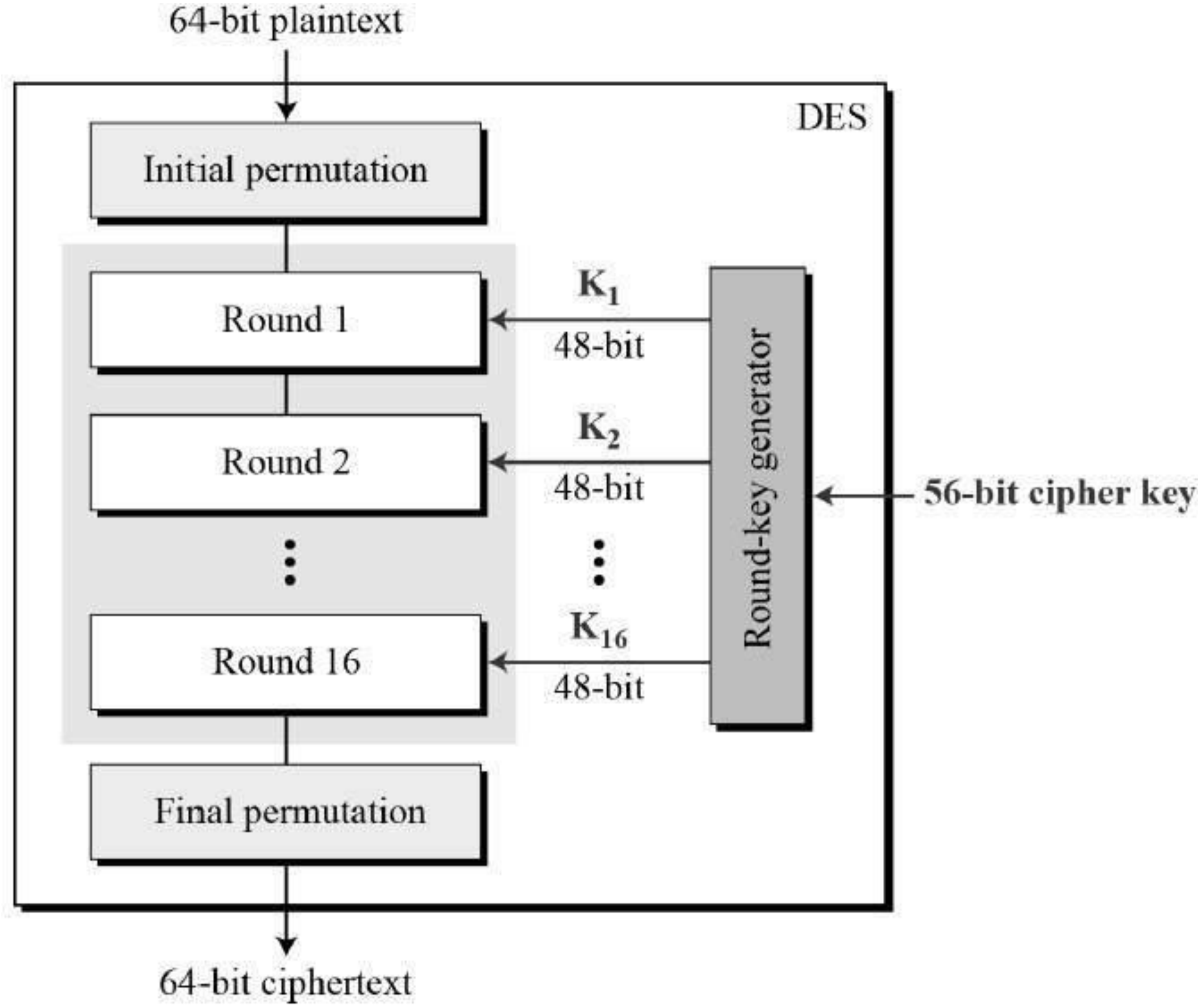
for all x not divisible by p or q

and [[Phi]](R) = (p-1)(q-1)

Q-2)Explain various types of data encryption standards.(2017)

Ans-The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −

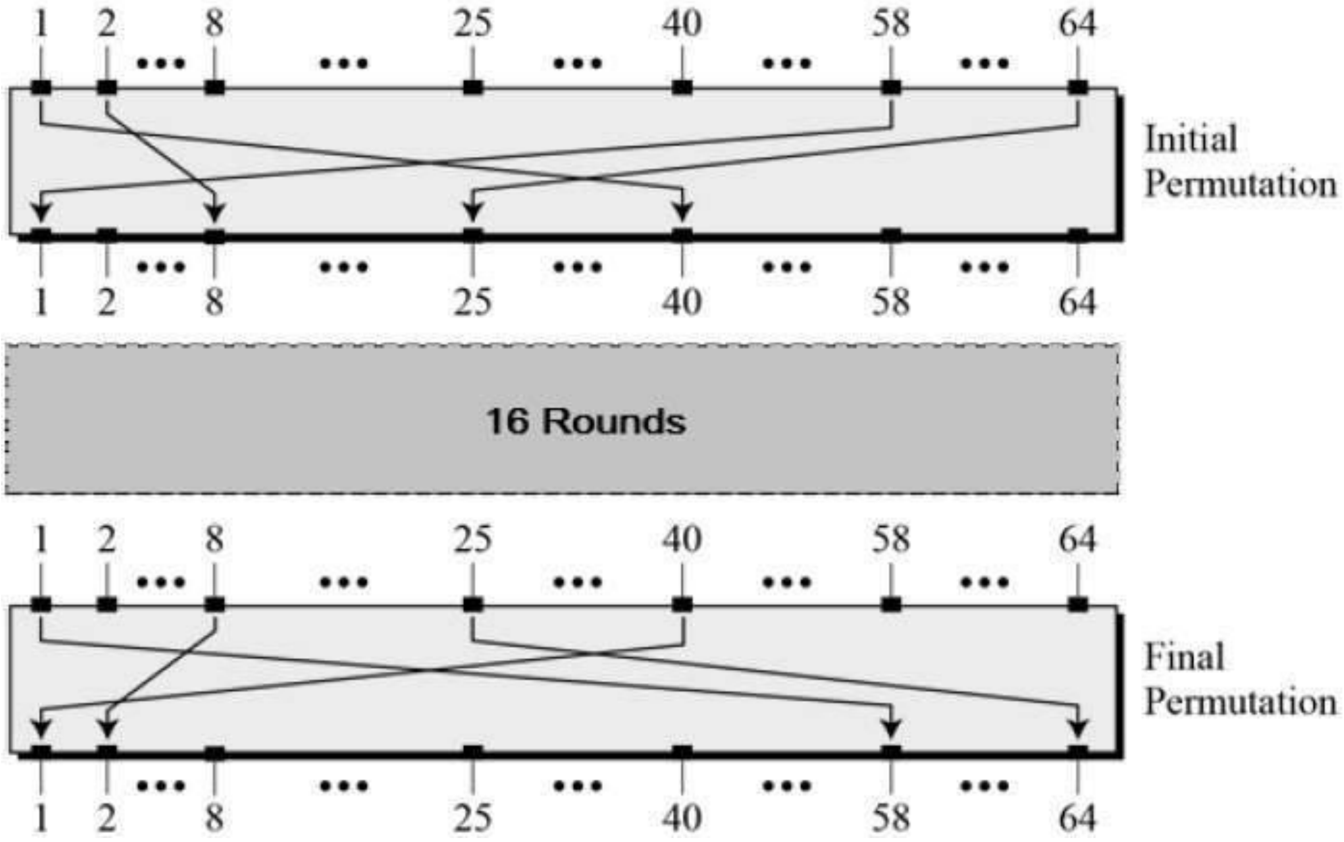


Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

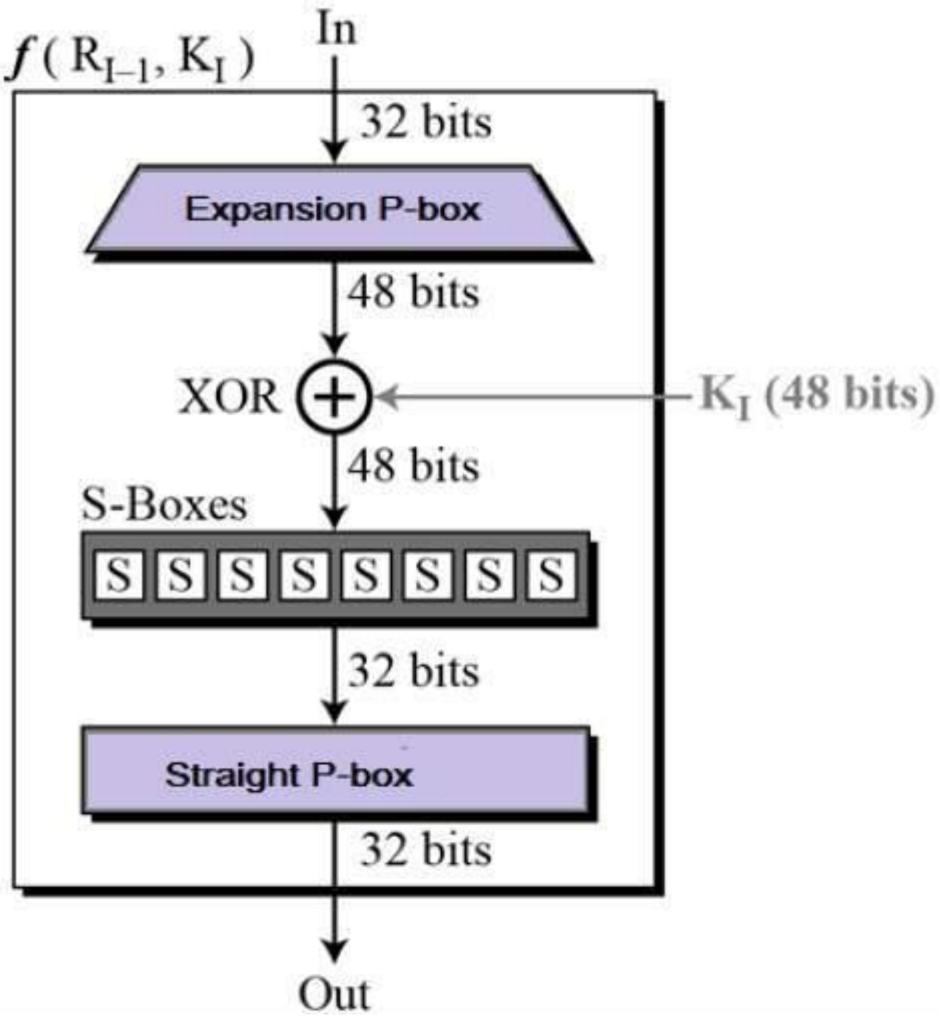
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows

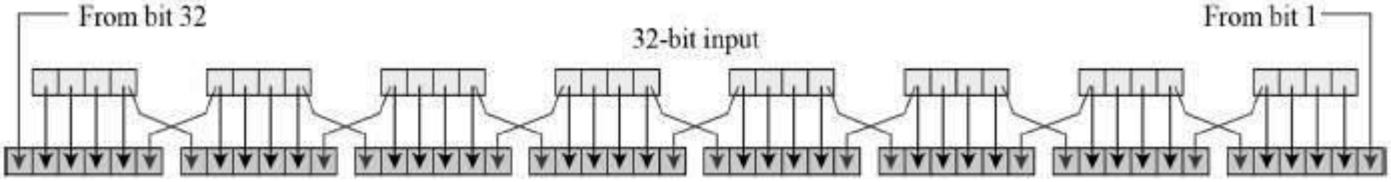


Round Function

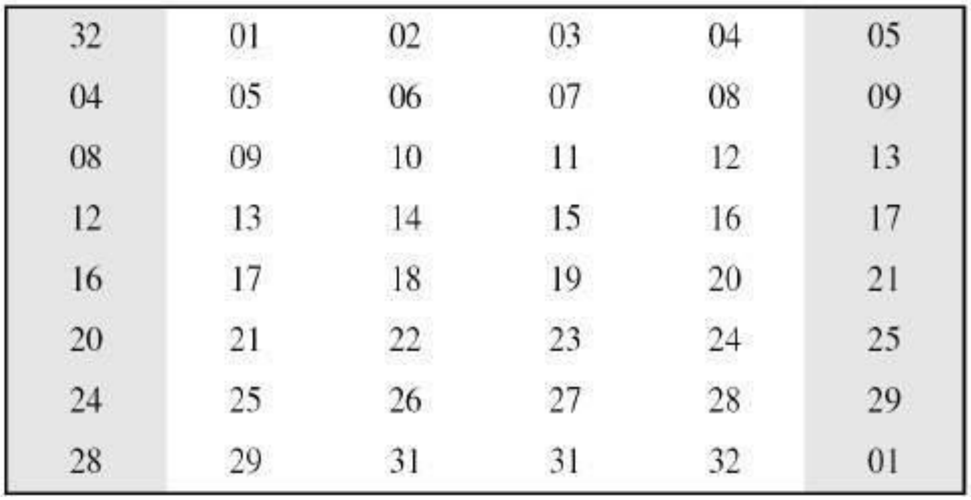
The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



- **Expansion Permutation Box** − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −

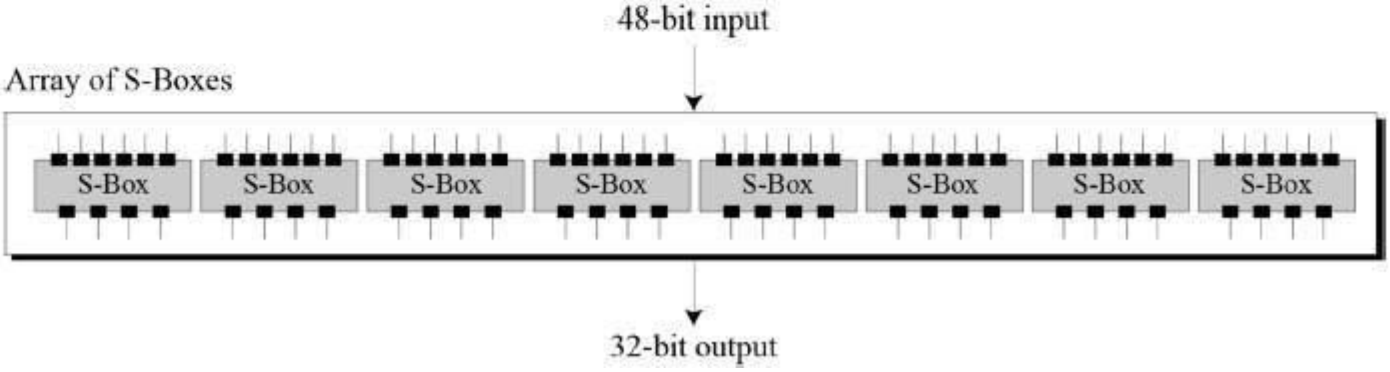


- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown −

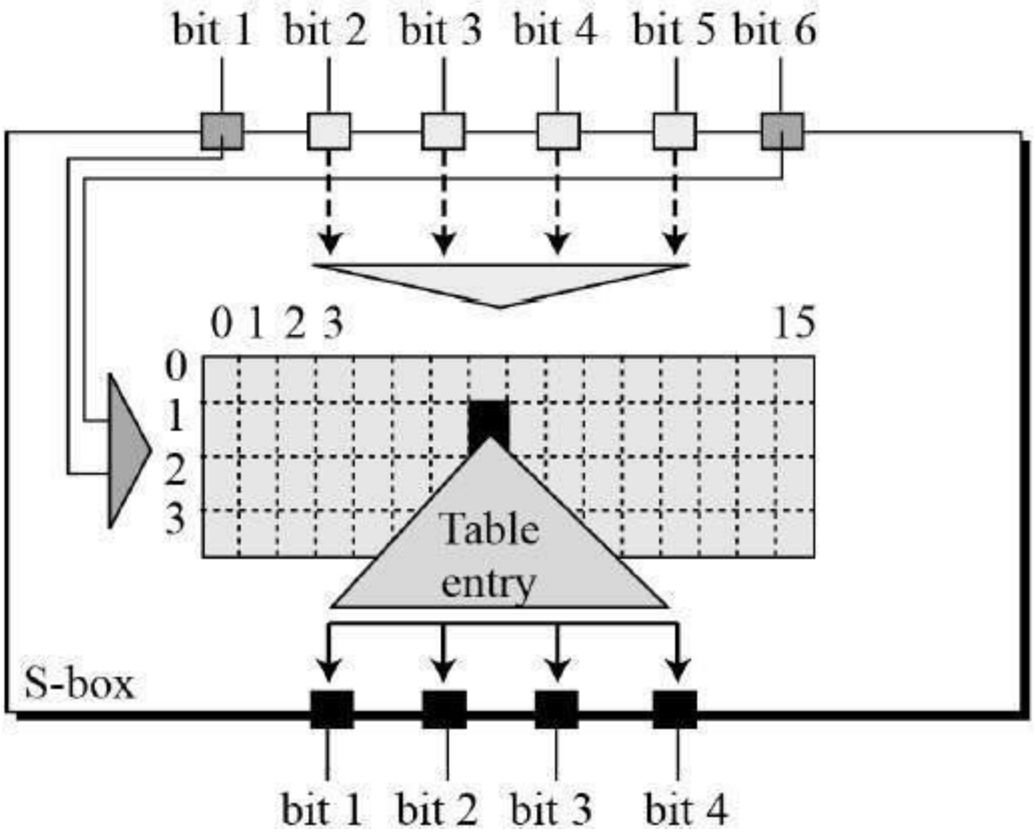


32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

- **XOR (Whitener).** – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –

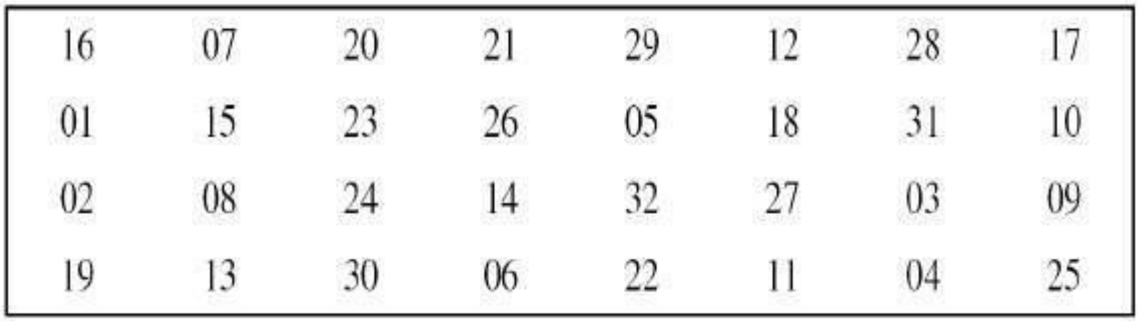


- The S-box rule is illustrated below –



- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

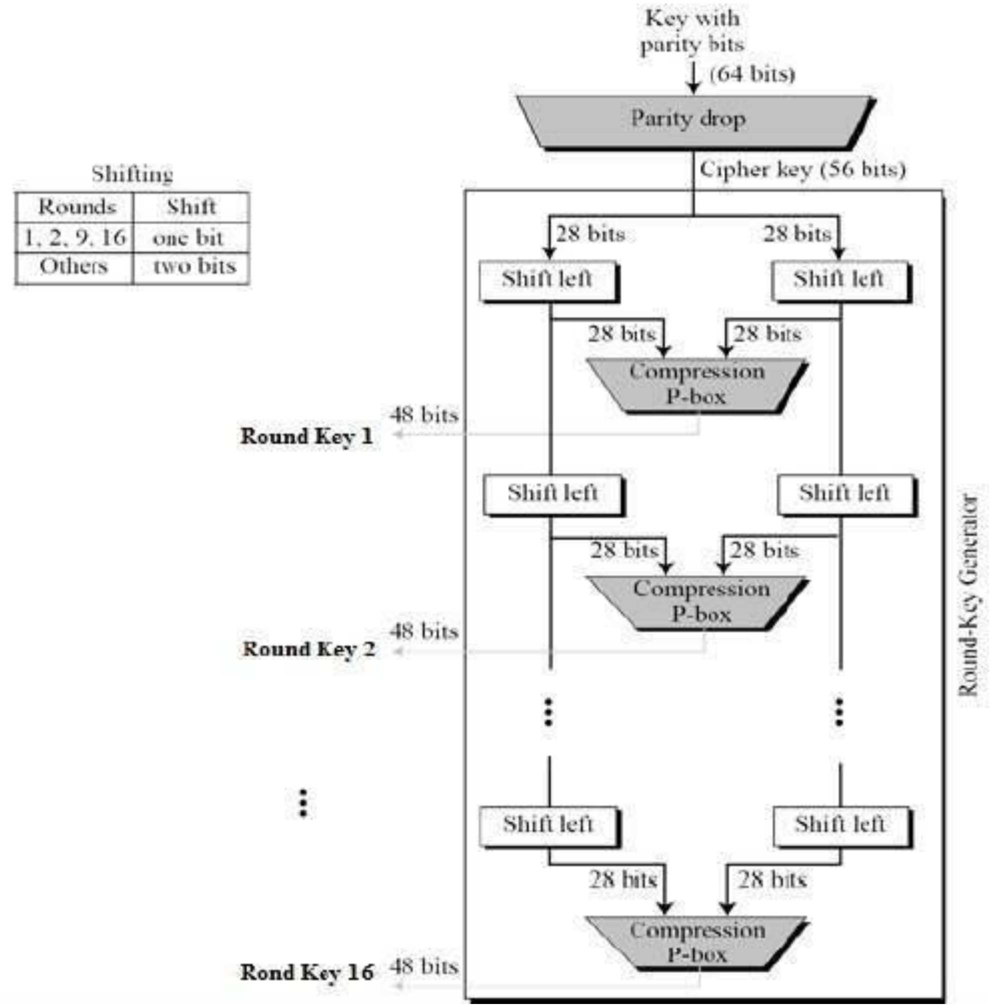
- **Straight Permutation** – The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

The logic for Parity drop, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** − Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search

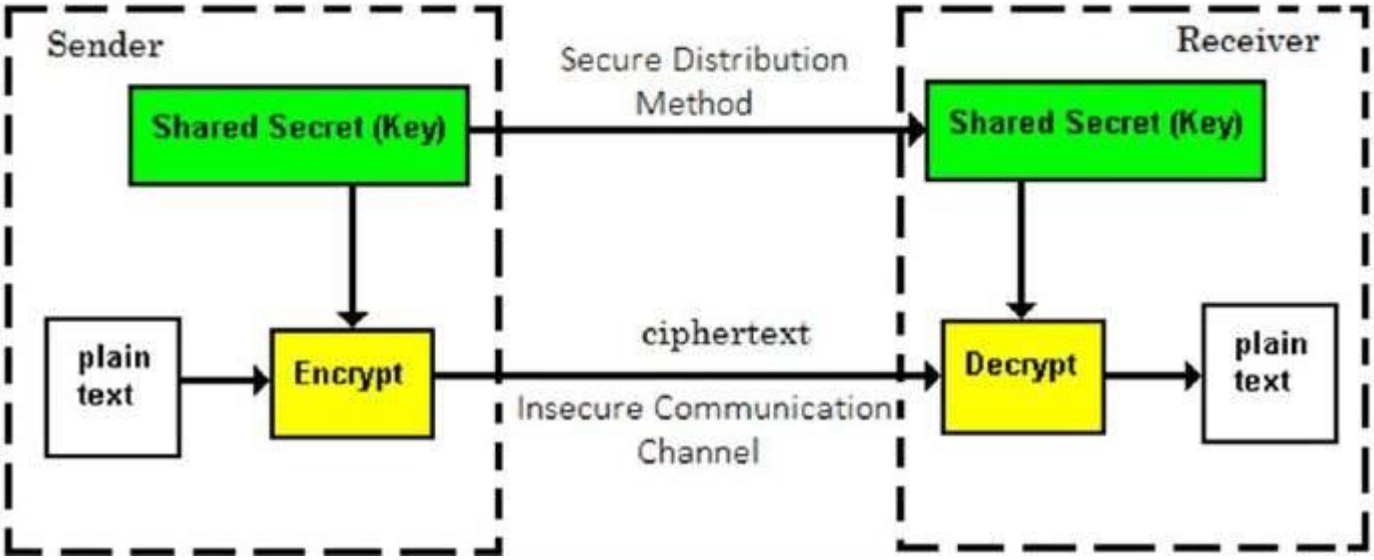
Q-3) Differentiate symmetric key and asymmetric key cryptography? (2015/16/17)

Ans-Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystems**.

A few well-known examples of symmetric key encryption methods are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The salient features of cryptosystem based on symmetric key encryption are −

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

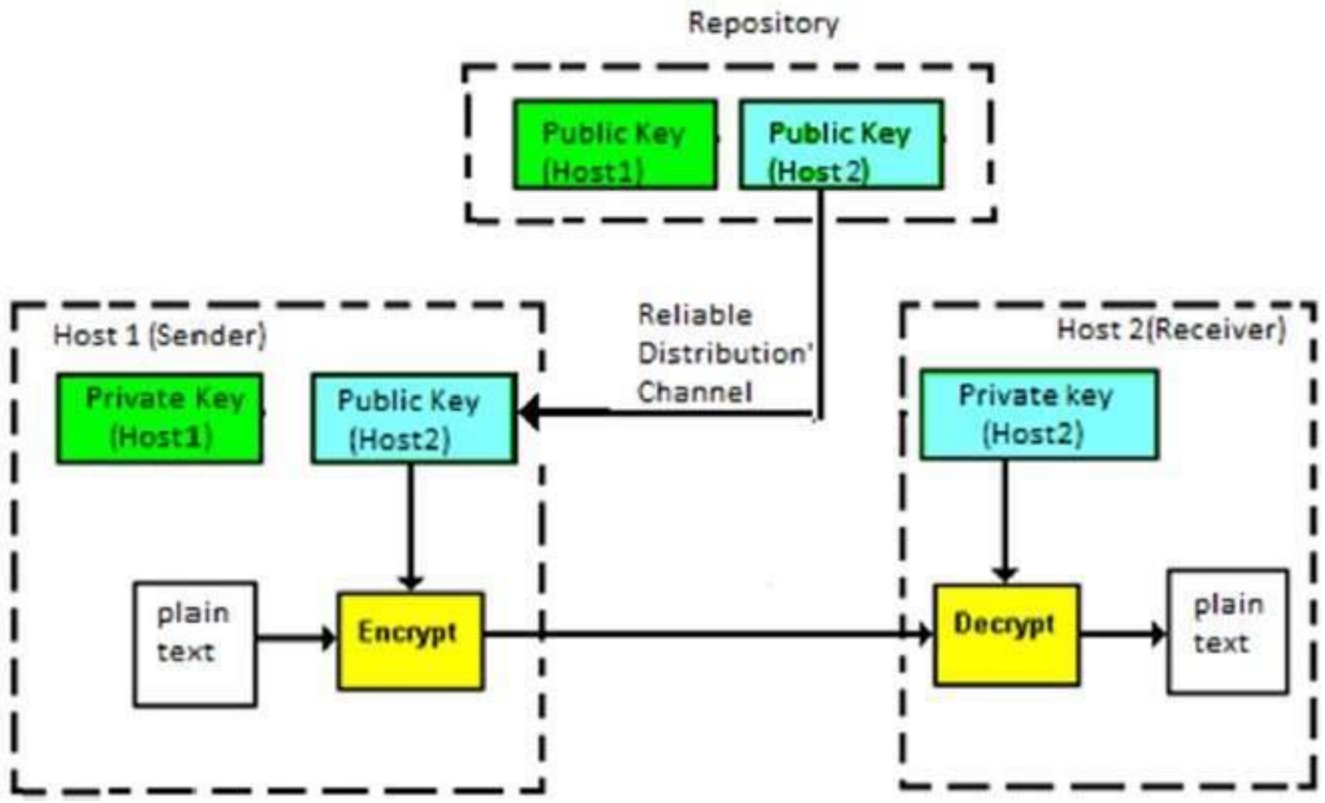
There are two restrictive challenges of employing symmetric key cryptography.

- **Key establishment** – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration –



Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows −

- Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related − when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- When *Host1* needs to send data to *Host2,* he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
- *Host2* uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.

- Processing power of computer system required to run asymmetric algorithm is higher.

Q-4) What is VPN ?explain its working principle in the field of network security. (2017/16)

Ans-VPN is *a* network that is constructed by using public wires usually the Internet to connect to a private network, such as a company's internal network. There are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Type of VPN

Early data networks allowed VPN-style remote connectivity through dial-up modems or through leased line connections utilizing Frame Relay and Asynchronous Transfer Mode(ATM) virtual circuits, provisioned through a network owned and operated by telecommunication carriers. These networks are not considered true VPNs because they passively secure the data being transmitted by the creation of logical data streams. They have been replaced by VPNs based on IP and IP/Multiprotocol Label Switching (MPLS) Networks, due to significant cost-reductions and increased bandwidth provided by new technologies such as Digital Subscriber Line (DSL) and fiber-optic networks.

VPN systems may be classified by:

The protocols used to tunnel the traffic.

The tunnel's termination point location, e.g., on the customer edge or network-provider edge.

Whether they offer site-to-site or network-to-network connectivity.

The levels of security provided.

The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity

Secure VPN protocols include the following:

Internet Protocol Security (IPsec) as initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.

Datagram Transport Layer Security (DTLS) - used in Cisco Any Connect VPN and in Open Connect VPN to solve the issues SSL/TLS has with tunneling over UDP.

Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.

Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel. (SSTP was introduced in Windows Server 2008 and in Windows Vista Service Pack 1.)

Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered trademark "MPVPN".

Secure Shell (SSH) VPN - OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. OpenSSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.

Advantages of VPNVPN can provide benefits for an organization. It can Extend geographic connectivity.

Improve security where data lines have not been ciphered.

Reduce operational costs vs. traditional costs.

Reduce transit time and transportation costs for remote users.

Simplify network topology in certain scenarios.

Private global networking opportunities.

Provide telecommunication support.

Provide broadband networking compatibility.

Provide faster ROI (return on investment) than traditional carrier leased/ owned WAN lines.

Show good economy of scale.

Scale well, when used with a public key infrastructure

Q-5) What is digital certificate and write different steps used in obtaining a digital certificate.? (2017/15)

Ans-A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.
Just like a passport, a digital certificate provides identifying information is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digitalsignatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority. The implementation of digital certification involves signature algorithm that both hashes the message and signs the hash with the private key rather than using a message digest function followed by message digest encryption algorithm. There are two types of digital certificates, such as

** Server certificates are used to authenticate the identity of websites to make sure that there is no impersonation. They facilitate the exchange of personal information like credit card numbers among website visitors. Server certificate are a necessary for e-commerce site that facilitates the exchange of confidential information among customers, vendors and clients.**

** Personal certificates are used to authenticate visitors, identity and restrict their access to specific content. These certificates are suitable for B2B transaction like inventory management, updating product availability, shipping dates and so on.**

The working of digital certificates is based on private/ public key technology. Each of these keys is a unique encryption device. Since two keys are never similar, these keys can be used to find the identity of the user. These keys are always work in pairs. The private key is kept secret while the public key is distributed among the different users who want to communicate. Whatever data is encrypted by the public key can only be decrypted by the private key. Certification Authorities: Certificates are signed by the Certificate Authority (CA) that issues them. In essence, a CA is a commonly trusted third party that is relied upon to verify the matching of public keys to identity, e-mail name, or other such information. A certificate shows that a public key stored in the

certificate belongs to the subject of that certificate. A CA is responsible for verifying the identity of a requesting entity before issuing a certificate. The CA then signs the certificate using its private key, which is used to verify the certificate. A CA's public keys are distributed in software packages such as Web browsers and operating systems, or they can also be added manually by the user. Types of Digital Certificates: There are three types of digital certificate such as :

1. Type I digital certificate
2. Type II digital certificate
3. Type III digital certificate

1. Type I digital certificate: These types of digital certificate authenticate only e-mail and are not legally recognized in India as per the IT Act 2002. 2. Type II digital certificate: These types of digital certificate authenticate e-mail, name and identity and are legally recognized in India as per the IT Act 2002. 3. Type III digital certificate: These are used to authenticate e-mail, name and identity and are globally interoperable. These certificates are legally recognized in India as per IT Act 2002.

Q-6) Explain diffie-hellman key exchange agreement algorithm. (2017/14/16)

Ans-The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel. The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key.

Steps in the algorithm: 1 Alice and Bob agree on a prime number p and a base g. 2 Alice chooses a secret number a, and sends Bob (g a mod p). 3 Bob chooses a secret number b, and sends Alice (g b mod p). 4 Alice computes ((g b mod p) a mod p). 5 Bob computes ((g a mod p) b mod p). Both Alice and Bob can use this number as their key. Notice tha t p and g need not be protected.

Alice and Bob agree on p = 23 and g = 5. 2 Alice chooses a = 6 and sends 5 6 mod 23 = 8. 3 Bob chooses b = 15 and sends 515 mod 23 = 19. 4 Alice computes 19 6 mod 23 = 2. 5 Bob computes 815 mod 23 = 2. Then 2 is the shared secret. Clearly, much larger values of a, b, and p are required. An eavesdropper cannot discover this value even if she knows p and g and can obtain each of the messages.

Suppose p is a prime of around 300 digits, and a and b at least 100 digits each. Discovering the shared secret given g, p, g a mod p and g b mod p would take longer

than the lifetime of the universe, using the best known algorithm. This is called the discrete logarithm problem.

Q-7) Explain the differences between transposition and substitution techniques. (2017/16)

Ans-In a substitution cypher, the units of plain text are still in the same sequence in the cypher text as they are in the plain text form. The only thing different is the units. They would be substituted for something else. A number, or symbol, or whatever.Kinda like Morse Code. Each letter is replaced by some sequence of dots and lines. So to decipher what's being said, all you have to do is replace each Morse Code with its correct letter, in the order that you read it.

In transposition, all the units are the same.. The only difference is that they are all rearranged in a different order, according to some algorithm.

Q-8) What are the different key aspects of algorithm?Explain different algorithm modes. (2017)

Ans- the different modes of operation of a block cipher. These are procedural rules for a generic block cipher. Interestingly, the different modes result in different properties being achieved which add to the security of the underlying block cipher.

A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

Electronic Code Book (ECB) Mode

This mode is a most straightforward way of processing a series of sequentially listed message blocks.

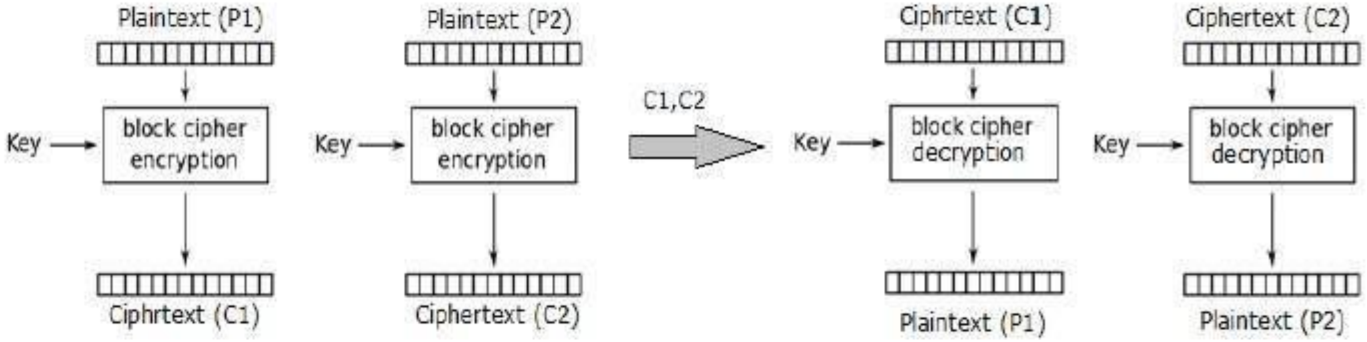
Operation

- **The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.**

- **He then takes the second block of plaintext and follows the same process with same key and so on so forth.**

The ECB mode is deterministic, that is, if plaintext block P1, P2,…, Pm are encrypted twice under the same key, the output ciphertext blocks will be the same.

In fact, for a given key technically we can create a codebook of ciphertexts for all possible plaintext blocks. Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext. Thus, the operation is analogous to the assignment of code words in a codebook, and hence gets an official name − Electronic Codebook mode of operation (ECB). It is illustrated as follows −



Analysis of ECB Mode

In reality, any application data usually have partial information which can be guessed. For example, the range of salary can be guessed. A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.

For example, if a ciphertext from the ECB mode is known to encrypt a salary figure, then a small number of trials will allow an attacker to recover the figure. In general, we do not wish to use a deterministic cipher, and hence the ECB mode should not be used in most applications.

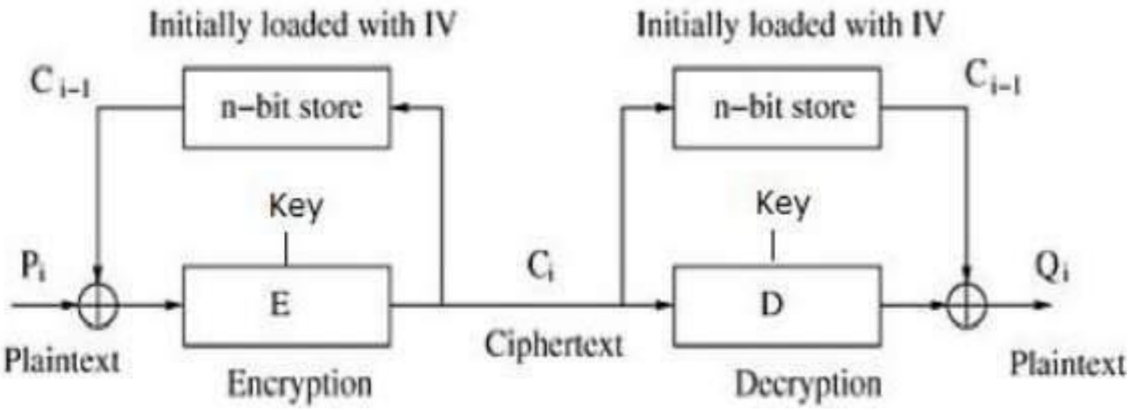
Cipher Block Chaining (CBC) Mode

CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

Operation

The operation of CBC mode is depicted in the following illustration. The steps are as follows –

- **Load the n-bit Initialization Vector (IV) in the top register.**
- **XOR the n-bit plaintext block with data value in top register.**
- **Encrypt the result of XOR operation with underlying block cipher with key K.**
- **Feed ciphertext block into top register and continue the operation till all plaintext blocks are processed.**
- **For decryption, IV data is XORed with first ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.**



Analysis of CBC Mode

In CBC mode, the current plaintext block is added to the previous ciphertext block, and then the result is encrypted with the key. Decryption is thus the reverse process, which involves decrypting the current ciphertext and then adding the previous ciphertext block to the result.

Advantage of CBC over ECB is that changing IV results in different ciphertext for identical message. On the drawback side, the error in transmission gets propagated to few further block during decryption due to chaining effect.

It is worth mentioning that CBC mode forms the basis for a well-known data origin authentication mechanism. Thus, it has an advantage for those applications that require both symmetric encryption and data origin authentication.

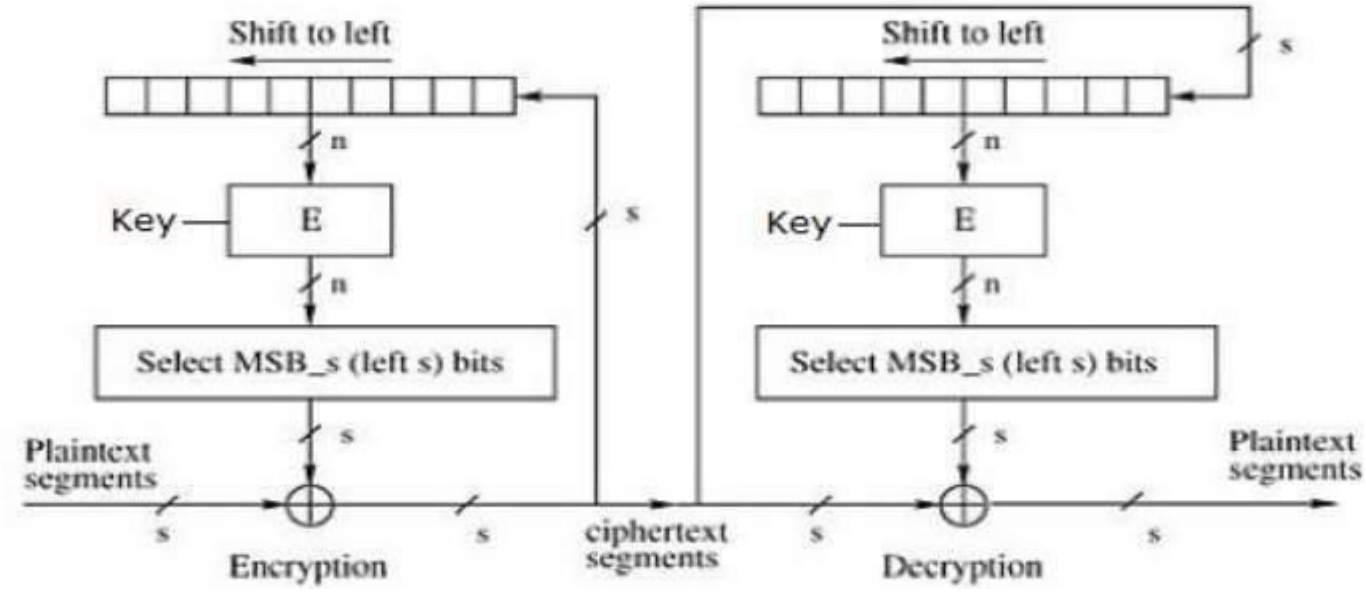
Cipher Feedback (CFB) Mode

In this mode, each ciphertext block gets 'fed back' into the encryption process in order to encrypt the next plaintext block.

Operation

The operation of CFB mode is depicted in the following illustration. For example, in the present system, a message block has a size 's' bits where 1 < s < n. The CFB mode requires an initialization vector (IV) as the initial random n-bit input block. The IV need not be secret. Steps of operation are −

- **Load the IV in the top register.**
- **Encrypt the data value in top register with underlying block cipher with key K.**
- **Take only 's' number of most significant bits (left bits) of output of encryption process and XOR them with 's' bit plaintext message block to generate ciphertext block.**
- **Feed ciphertext block into top register by shifting already present data to the left and continue the operation till all plaintext blocks are processed.**
- **Essentially, the previous ciphertext block is encrypted with the key, and then the result is XORed to the current plaintext block.**
- **Similar steps are followed for decryption. Pre-decided IV is initially loaded at the start of decryption.**



Analysis of CFB Mode

CFB mode differs significantly from ECB mode, the ciphertext corresponding to a given plaintext block depends not just on that plaintext block and the key, but also on the previous ciphertext block. In other words, the ciphertext block is dependent of message.

CFB has a very strange feature. In this mode, user decrypts the ciphertext using only the encryption process of the block cipher. The decryption algorithm of the underlying block cipher is never used.

Apparently, CFB mode is converting a block cipher into a type of stream cipher. The encryption algorithm is used as a key-stream generator to produce key-stream that is placed in the bottom register. This key stream is then XORed with the plaintext as in case of stream cipher.

By converting a block cipher into a stream cipher, CFB mode provides some of the advantageous properties of a stream cipher while retaining the advantageous properties of a block cipher.

On the flip side, the error of transmission gets propagated due to changing of blocks.

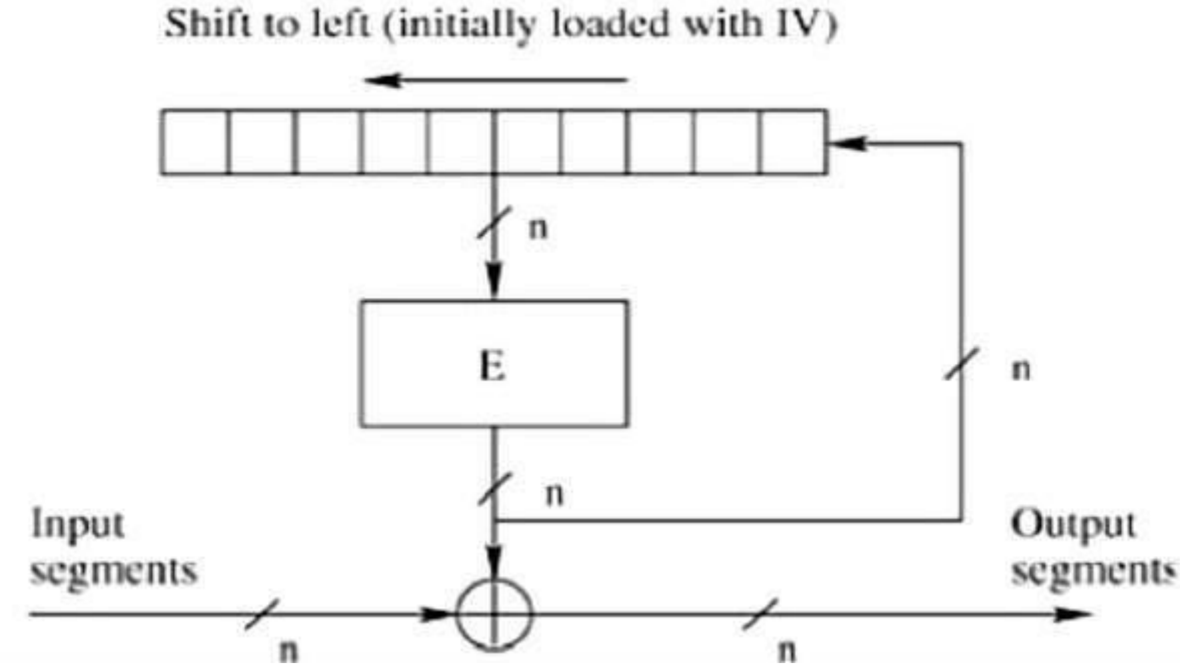
Output Feedback (OFB) Mode

It involves feeding the successive output blocks from the underlying block cipher back to it. These feedback blocks provide string of bits to

feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.

The key stream generated is XOR-ed with the plaintext blocks. The OFB mode requires an IV as the initial random n-bit input block. The IV need not be secret.

The operation is depicted in the following illustration −



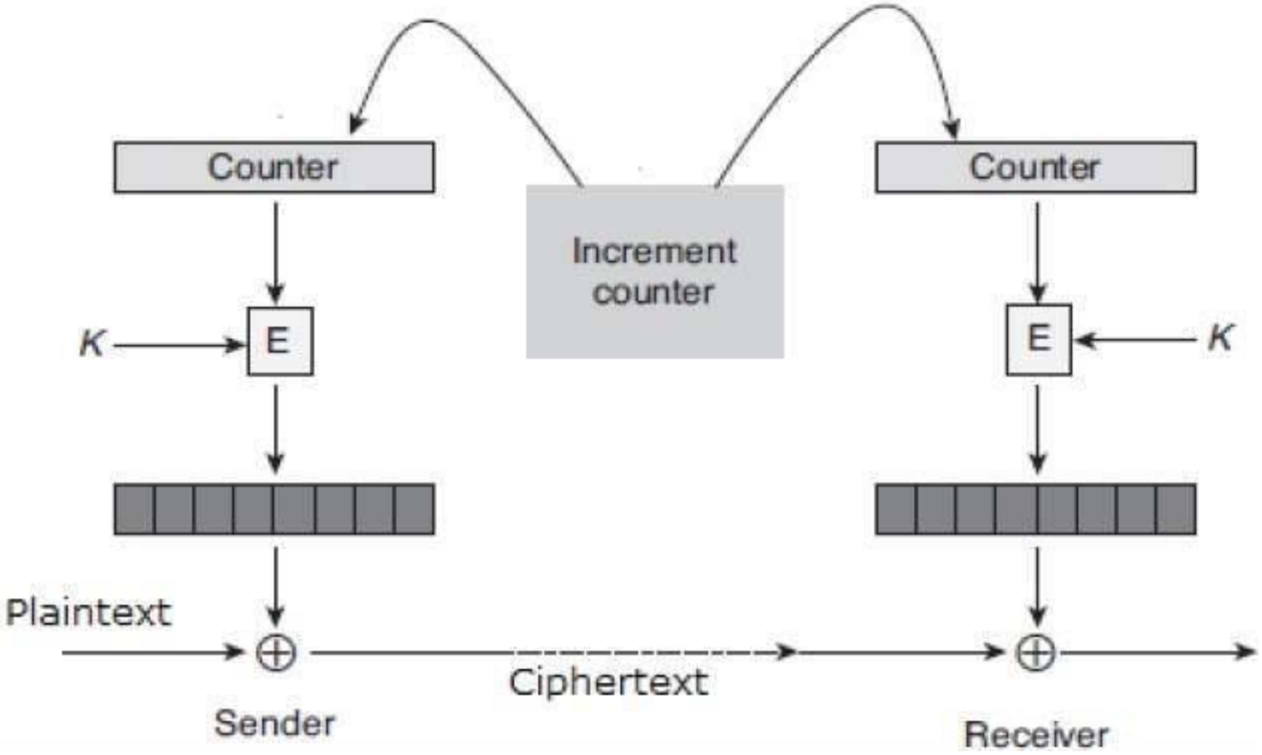
Counter (CTR) Mode

It can be considered as a counter-based version of CFB mode without the feedback. In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge is that both sides must keep the counter synchronized.

Operation

Both encryption and decryption in CTR mode are depicted in the following illustration. Steps in operation are −

- **Load the initial counter value in the top register is the same for both the sender and the receiver. It plays the same role as the IV in CFB (and CBC) mode.**
- **Encrypt the contents of the counter with the key and place the result in the bottom register.**
- **Take the first plaintext block P1 and XOR this to the contents of the bottom register. The result of this is C1. Send C1 to the receiver and update the counter. The counter update replaces the ciphertext feedback in CFB mode.**
- **Continue in this manner until the last plaintext block has been encrypted.**
- **The decryption is the reverse process. The ciphertext block is XORed with the output of encrypted contents of counter value. After decryption of each ciphertext block counter is updated as in case of encryption.**



Analysis of Counter Mode

It does not have message dependency and hence a ciphertext block does not depend on the previous plaintext blocks.

Like CFB mode, CTR mode does not involve the decryption process of the block cipher. This is because the CTR mode is really using the block cipher to generate a key-stream, which is encrypted using the XOR function. In other words, CTR mode also converts a block cipher to a stream cipher.

The serious disadvantage of CTR mode is that it requires a synchronous counter at sender and receiver. Loss of synchronization leads to incorrect recovery of plaintext.

However, CTR mode has almost all advantages of CFB mode. In addition, it does not propagate error of transmission at all.

7 marks

Q-1)Explian different types of attacks that may occur in the field of computer networking? (2017/16)

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.

Q-2)What is tcp/ip ? Explain the function of each layer in tcp/ip suite. (2017)

Ans-TCP/IP does not directly correspond to this model. TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all. The following table shows the layers of the Oracle Solaris implementation of TCP/IP. The table lists the layers from the topmost layer (application) to the bottommost layer (physical network).

Table 1-2 TCP/IP Protocol Stack

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP, SCTP
3	Network	Internet	IPv4, IPv6, ARP, ICMP
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, and others

The table shows the TCP/IP protocol layers and the OSI model equivalents. Also shown are examples of the protocols that are available at each level of the TCP/IP protocol stack. Each system that is involved in a communication transaction runs a unique implementation of the protocol stack.

Physical Network Layer

The physical network layer specifies the characteristics of the hardware to be used for the network. For example, physical network layer specifies the physical characteristics of the communications media. The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

The data-link layer identifies the network protocol type of the packet, in this instance TCP/IP. The data-link layer also provides error control and “framing.” Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Internet Layer

The Internet layer, also known as the network layer or IP layer, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

- **IP addressing – The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.**

- **Host-to-host communications – IP determines the path a packet must take, based on the receiving system's IP address.**

- **Packet formatting – IP assembles packets into units that are known as datagrams. Datagrams are fully described in Internet Layer: Where Packets Are Prepared for Delivery.**

- **Fragmentation – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.**

Oracle Solaris supports both IPv4 and IPv6 addressing formats, which are described in this book. To avoid confusion when addressing the Internet Protocol, one of the following conventions is used:

- **When the term “IP” is used in a description, the description applies to both IPv4 and IPv6.**

- **When the term “IPv4” is used in a description, the description applies only to IPv4.**

- **When the term “IPv6” is used in a description, the description applies only to IPv6.**

ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers. ARP assists IP in directing datagrams to the appropriate receiving

system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP Protocol

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

- Dropped packets – Packets that arrive too fast to be processed
- Connectivity failure – A destination system cannot be reached
- Redirection – Redirecting a sending system to use another router

Chapter 8, Administering a TCP/IP Network (Tasks) contains more information on Oracle Solaris commands that use ICMP for error detection.

Transport Layer

The TCP/IP transport layer ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. This type of communication is known as end-to-end. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service. UDP provides unreliable datagram service.

TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

- Starting point, which opens the connection
- Entire transmission in byte order
- Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a “reliable, connection-oriented” protocol.

SCTP Protocol

SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP. Moreover, SCTP can support connections between systems that have more than one address, or multihomed. The SCTP connection between sending and receiving system is called an association. Data in the association is organized in chunks. Because SCTP supports multihoming, certain applications, particularly applications used by the telecommunications industry, need to run over SCTP, rather than TCP.

UDP Protocol

UDP provides datagram delivery service. UDP does not verify connections between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use UDP.

Application Layer

The application layer defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. Many application layer protocols exist. The following list shows examples of application layer protocols:

- **Standard TCP/IP services such as the ftp, tftp, and telnet commands**
- **UNIX “r” commands, such as rlogin and rsh**
- **Name services, such as NIS and the domain name system (DNS)**
- **Directory services (LDAP)**
- **File services, such as the NFS service**
- **Simple Network Management Protocol (SNMP), which enables network management**
- **Router Discovery Server protocol (RDISC) and Routing Information Protocol (RIP) routing protocols**

Q-3)Explain various types of substitutution technique used in cryptography. (2017/16/15)

SUBSTITUTION TECHNIQUES

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 (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The
Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places
further down the alphabet.

e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z‟ is „a‟.

For each plaintext letter p, substitute the cipher text letter c such that

C = E(p) = (p+3) mod 26

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

C = E (p) = (p+k) mod 26

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

P = D(C) = (C-k) mod 26

Playfair cipher

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. 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
(minus duplicates) 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. Plaintext is encrypted two letters at a time
According to the following rules:

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.

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at thescho xol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Polyalphabetic ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common.

A set of related monoalphabetic substitution rules are used

A key determines which particular rule is chosen for a given transformation.

Vigenere cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of

26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar

cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To

aid in understanding the scheme, a matrix known as vigenere tableau is Constructed Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process oF

Q-4)Explain PKIX model in detail. (2017/16)

Ans-PKIX, in order to describe public–key infrastructures, uses the terms PKI and PMI. One can find similarities between the two. The main difference is that the PKI handles the Public Key Certificates while the PMI handles the Attribute Certificates. A good metaphor to distinguish between the two is to associate the former with the passport of a person and the latter with the visa. The one provides identity and the other permission.

PKIX standardisation areas

PKIX is working on the following five areas.

1. **Profiles of X.509 v3 Public Key Certificates and X.509 v2 Certificate Revocation Lists (CRLs).**

   It describes the basic certificate fields and the extensions to be supported for the Certificates and the Certificate Revocation Lists. Then, it talks about the basic and extended Certificate Path Validation. Finally, it covers the supported cryptographic algorithms.

2. **Management protocols.**

   First, it discusses the assumptions and restrictions of the protocols. Then, it provides the data structures used for the PKI management messages and defines the functions that conforming implementations must carry out. Finally, it describes a simple protocol for transporting PKI messages.

3. **Operational protocols.**

   Currently they describe how LDAPv2, FTP and HTTP can be used as operational protocols.

4. **Certificate policies and Certificate Practice Statements.**

   The purpose of this document is to establish a clear relationship between certificate policies and CPSs, and to present a framework to assist the writers of certificate policies or CPSs with their tasks. In particular, the framework identifies the elements that may need to be considered in formulating a certificate policy or a CPS. The purpose is not to define particular certificate policies or CPSs, per se.

5. **Time–stamping and data–certification/validation services.**

   There are no RFCs on these services yet, as the documents are still classified as Internet Drafts.

   The time–stamping services define a trusted third–party that creates time stamp tokens in order to indicate that a datum existed at a particular point in time. The data certification and validation services provide certification of possesion of data and claim of possesion of data, and validation of digitally signed documents and certificates.

Q-5)Define IP security.explain application and advantage of IP security. (2017/16)

Ans-Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.

IPsec involves two security services:

- **Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.**
- **Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.**

There are two modes of IPsec:

- Tunnel Mode: This will take the whole IP packet to form secure communication between two places, or gateways.
- Transport Mode: This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.
- Applications of IPSec
- –Secure branch office connectivity over the Internet
- –Secure remote access over the Internet
- –Establsihing extranet and intranet connectivity with partners
- –Enhancing electronic commerce security
- However, users have some security concerns that cut across protocol layers. For example, an enterprise can run a secure, private TCP/IP network by disallowing links to untrusted sites, encrypting packets that leave the premises, and authenticating packets that enter the premises. By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications.
-

Benefits of IPSec

When IPSec is implemented in a firewall or router, it provides strong security whose application is to all traffic crossing this perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing. IPSec is below the transport layer (TCP, UDP), and is thus transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper layer software, including applications is not affected. IPSec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization. IPSec can provide security for individual users if needed. This feature is useful for offsite workers and also for setting up a secure virtual subnetwork within an organization for sensitive applications.

Q-6) What is secure electronic transaction (SET)?Describe process imvolved in set. (2017)

Ans-Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different

encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

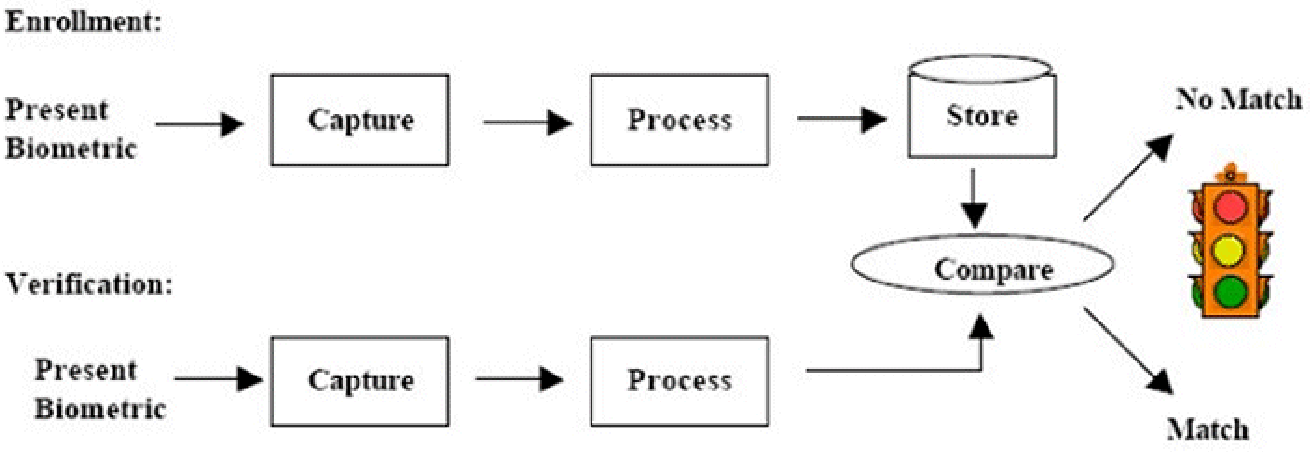
Requirements in SET :
SET protocol has some requirements to meet, some of the important requirements are :

- **It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.**
- **It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.**
- **It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.**
- **SET also needs to provide interoperability and make use of best security mechanisms.**

For set process follow class note

Q-7) Define biometric authentication.Explain its working principles. (2017)

Ans-The word ―biometrics‖ came from Greek and we can divide it into two roots: ―bio‖ means life and ―metrics‖ – to measure. Biometrics is the process of making sure that the person is who he claims to be. Authentication of identity of the user can be done in 3 three ways: 1) Something that person knows (password), 2) Something the person has (key, special card), 3) Something the person is (fingerprints, footprint



Biometrics is based on anatomic uniqueness of a person and as follow it can be used for biometric identification of a person. Unique characteristics can be used to prevent unauthorized access to the system with the help of automated method of biometric control which, by checking unique physiological features or behaviour characteristics identifies the person.

Enrolment

The system captures a characteristic trait from the person, for example his fingerprint, and it processes this information to create an electronic representation called a template. This template is saved in a database, a smart card or in another place that can be accessed during the second step. *Verification* The person tells the system who he is by presenting a card with a magnetic strip, a barcode, or using a PIN or password that only he knows. Immediately, the system asks for a biometric sample. With this sample, the system creates an electronic representation called a live template, which is compared with the reference model saved in the database. *Identification* The person does not tell the system who he is; he uses neither cards nor passwords. The device uses his trait to identify him directly. The system captures this trait and processes it to create a live template. Then, the system compares this with the reference models stored in the database to determine the person‘s identity. How does Biometrics security works The largest share of that money (48 percent) goes for fingerprint recognition systems, followed by facial recognition (12 percent). While these two are the most popular, there are other methods that analyze a person's physical or dynamic characteristics. Physical biometric methodologies also look at the following:

Eyes — Examining the lines of the iris or the blood vessels in the retina;

Hands — Taking a 3D image and measuring the height and width of bones and joints, and

Skin — Analyzing surface texture and thickness of skin layers.

Q-8) Describe different types of attack to a computer system. (2017/16/15)

Ans-Security Attacks, Services and Mechanisms

To assess the security needs of an organization effectively, the manager responsible for
security needs some systematic way of defining the requirements for security and characterization
of approaches to satisfy those requirements. One approach is to consider three aspects of
information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a
security attack.

Security service – A service that enhances the security of the data processing systems and the
information transfers of an organization. The services are intended to counter security attacks and
they make use of one or more security mechanisms to provide the service

SECURITY ATTACKS

There are four general categories of attack which are listed below.

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

Sender Receiver

Eavesdropper or forger

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.

Sender Receiver

Eavesdropper or forger

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.

Sender Receiver

Eavesdropper or forger

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.

Q-9) What is digital certificate(DC) ?Explain the procedure for cration of DC. (2017/16)

Ans-A digital certificate, also known as a public key certificate, is used to cryptographically link ownership of a public key with the entity that owns it. Digital

certificates are for sharing public keys to be used for encryption and authentication. Digital certificates include the public key being certified, identifying information about the entity that owns the public key, metadata relating to the digital certificate and a digital signature of the public key created by the issuer of the certificate.

The distribution, authentication and revocation of digital certificates are the primary purposes of the public key infrastructure (PKI), the system by which public keys are distributed and authenticated.

Public key cryptography depends on key pairs: one a private key to be held by the owner and used for signing and decrypting, and one a public key that can be used for encryption of data sent to the public key owner or authentication of the certificate holder's signed data. The digital certificate enables entities to share their public key in a way that can be authenticated.

Digital certificates are used in public key cryptography functions; they are most commonly used for initializing secure SSL connections between web browsers and web servers. Digital certificates are also used for sharing keys to be used for public key encryption and authentication of digital signatures.

When sending messages over the Internet, public key encryption may be used.

Public key encryption is the use of complex mathematical formulas to make data unreadable. Under public-key encryption, two different keys are used, one for encrypting the data and a second key to decrypt it.

Someone wanting to send a message would request the recipient's digital certificate, which contains the public key, from a trusted directory, and use the public key to encrypt the message before sending. Once the message is encrypted it can only be decrypted using the intended recipient's private key.

The sender can also digitally sign the message using their own private key to prove that the message originated from them. If the message has been digitally signed, the

recipient would verify the sender by obtaining the sender's digital certificate from a trusted directory and using this to verify the sender's digital signature.

The effectiveness and reliability of the digital certificate is based on the confidence all parties to a transaction have in the structure, policies and procedures surrounding the PKI system.