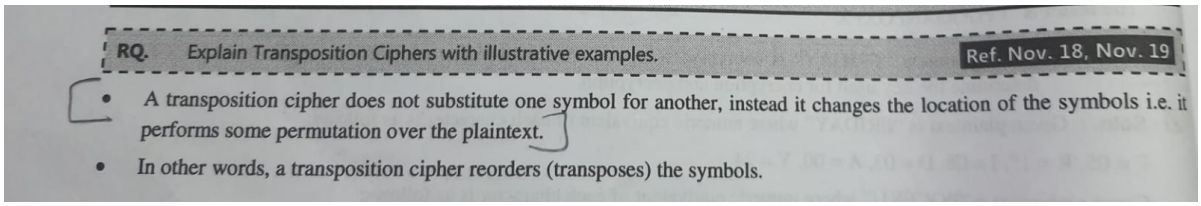
Q1)

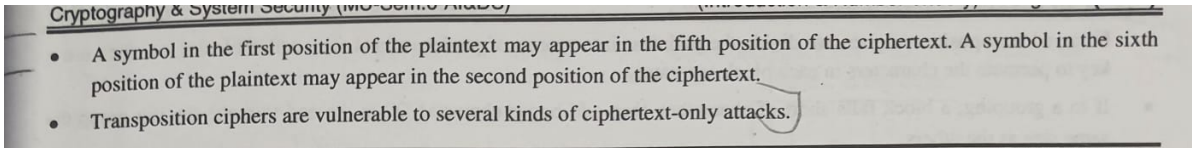
1. **What is a transposition cipher? 2 techniques of transposition cipher. (Chpt 1)**

Ans) Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.



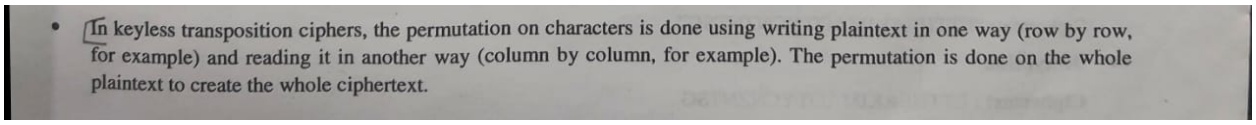
RQ. *Explain Transposition Ciphers with illustrative examples.* Ref. Nov. 18, Nov. 19

- *A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols i.e. it performs some permutation over the plaintext.*
- *In other words, a transposition cipher reorders (transposes) the symbols.*

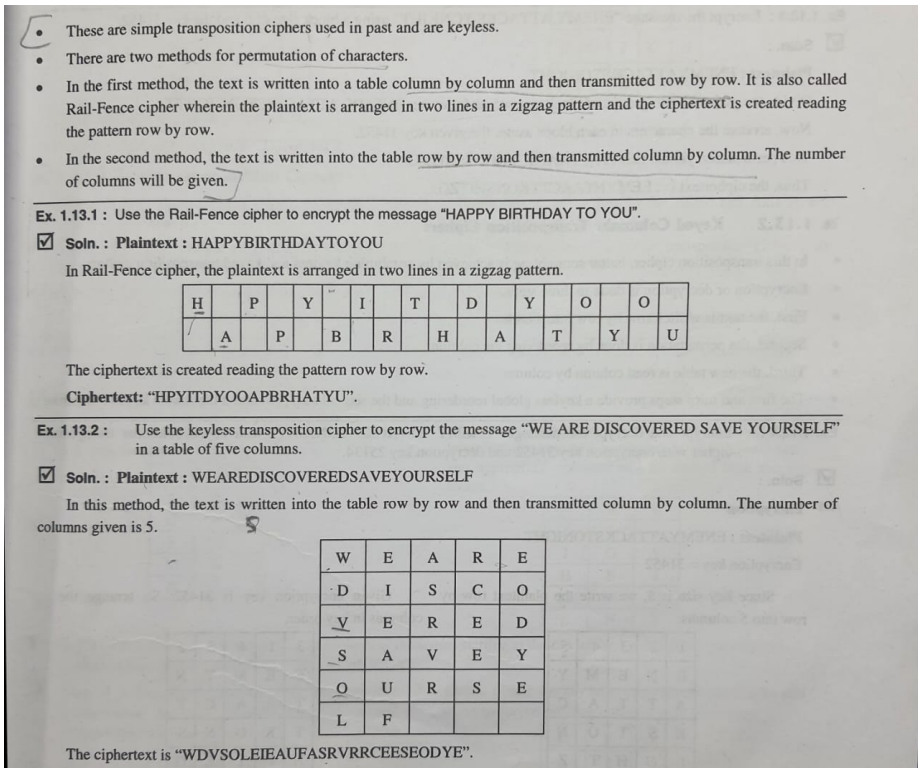


- A symbol in the first position of the plaintext may appear in the fifth position of the ciphertext. A symbol in the sixth position of the plaintext may appear in the second position of the ciphertext.
- Transposition ciphers are vulnerable to several kinds of ciphertext-only attacks.

Keyless:



- In keyless transposition ciphers, the permutation on characters is done using writing plaintext in one way (row by row, for example) and reading it in another way (column by column, for example). The permutation is done on the whole plaintext to create the whole ciphertext.



- These are simple transposition ciphers used in past and are keyless.
- There are two methods for permutation of characters.
- In the first method, the text is written into a table column by column and then transmitted row by row. It is also called Rail-Fence cipher wherein the plaintext is arranged in two lines in a zigzag pattern and the ciphertext is created reading the pattern row by row.
- In the second method, the text is written into the table row by row and then transmitted column by column. The number of columns will be given.

Ex. 1.13.1 : Use the Rail-Fence cipher to encrypt the message "HAPPY BIRTHDAY TO YOU".

☑ **Soln. : Plaintext :** HAPPYBIRTHDAYTOYOU

In Rail-Fence cipher, the plaintext is arranged in two lines in a zigzag pattern.

H		P		Y		I		T		D		Y		O		O	
	A		P		B		R		H		A		T		Y		U

The ciphertext is created reading the pattern row by row.

Ciphertext: "HPYITDYOOAPBRHATYU".

Ex. 1.13.2 : Use the keyless transposition cipher to encrypt the message "WE ARE DISCOVERED SAVE YOURSELF" in a table of five columns.

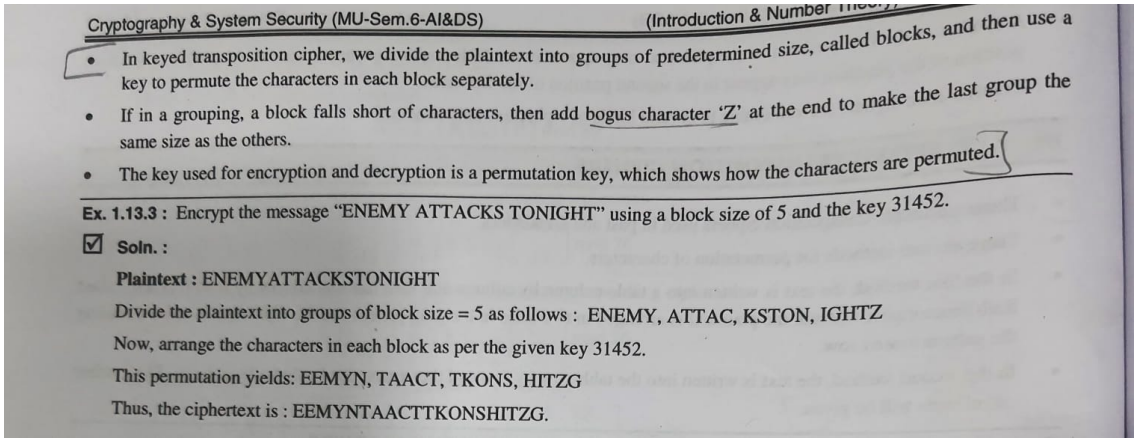
☑ **Soln. : Plaintext :** WEAREDISCOVEREDSAVEYOURSELF

In this method, the text is written into the table row by row and then transmitted column by column. The number of columns given is 5.

W	E	A	R	E
D	I	S	C	O
V	E	R	E	D
S	A	V	E	Y
O	U	R	S	E
L	F			

The ciphertext is "WDVSOLEIEAUFASRVRRCEESEODYE".

Keyed:



Cryptography & System Security (MU-Sem.6-AI&DS) (Introduction & Number

- In keyed transposition cipher, we divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.
- If in a grouping, a block falls short of characters, then add bogus character 'Z' at the end to make the last group the same size as the others.
- The key used for encryption and decryption is a permutation key, which shows how the characters are permuted.

Ex. 1.13.3 : Encrypt the message "ENEMY ATTACKS TONIGHT" using a block size of 5 and the key 31452.

☑ **Soln. :**

Plaintext : ENEMYATTACKSTONIGHT

Divide the plaintext into groups of block size = 5 as follows : ENEMY, ATTAC, KSTON, IGHTZ

Now, arrange the characters in each block as per the given key 31452.

This permutation yields: EEMYN, TAACT, TKONS, HITZG

Thus, the ciphertext is : EEMYNTAACTTKONSHITZG.

Merits:

1. Complexity: Transposition ciphers can be more complex than substitution ciphers, making them harder to break. They may involve multiple rounds of encryption or require a more complex set of rules.
2. Key space: Transposition ciphers typically have a larger key space than substitution ciphers, making them harder to break through brute force attacks.
3. Security: With a well-designed algorithm and a sufficiently long key, transposition ciphers can provide a high level of security and confidentiality.

Demerits:

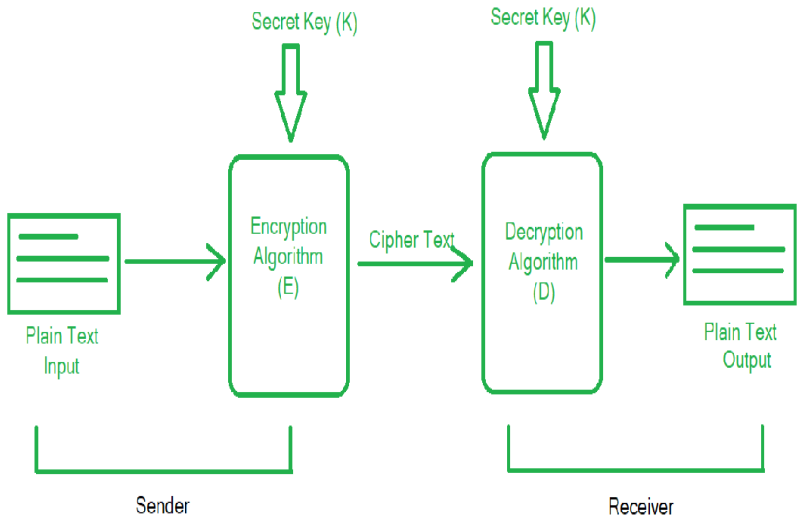
1. Vulnerability: Although transposition ciphers are more complex than substitution ciphers, they are still vulnerable to cryptanalysis. An attacker who knows the algorithm and has access to the ciphertext can use various techniques to analyze the encryption and try to reveal the plaintext.
2. Limited effectiveness: Transposition ciphers alone may not provide sufficient security against modern cryptographic attacks. They are often used in combination with other encryption techniques to provide a more secure solution.
3. Implementation complexity: Transposition ciphers can be more complex to implement than substitution ciphers, especially if they involve multiple rounds of encryption or require more complex rules for rearranging the plaintext.

2. Describe the Symmetric cipher model. (Chpt 1)

Ans)**Symmetric cipher-** Symmetric Encryption is the most basic and old method of encryption. It uses only one key for the process of both the encryption and decryption of data. Thus, it is also known as Single-Key Encryption.

Symmetric Cipher Model:

A symmetric cipher model is composed of five essential parts:



- **Plain Text (x):** This is the original data/message that is to be communicated to the receiver by the sender. It is one of the inputs to the encryption algorithm.
- **Secret Key (k):** It is a value/string/textfile used by the encryption and decryption algorithm to encode and decode the plain text to cipher text and vice-versa respectively. It is independent of the encryption algorithm. It governs all the conversions in plain text.
- **Encryption Algorithm (E):** It takes the plain text and the secret key as inputs and produces Cipher Text as output. It implies several techniques such as substitutions and transformations on the plain text using the secret key. ***E(x, k) = y***
- **Cipher Text (y):** It is the formatted form of the plain text (x) which is unreadable for humans, hence providing encryption during the transmission. It is completely dependent upon the secret key provided to the encryption algorithm. Each unique secret key produces a unique cipher text.
- **Decryption Algorithm (D):** It performs reversal of the encryption algorithm at the recipient's side. It also takes the secret key as input and decodes the cipher text received from the sender based on the secret key. It produces plain text as output. ***D(y, k) = x***

8. Define steganography with any 5 techniques. (Chpt 1)

Ans) definition from the difference on pg 1-36

Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file.

It is one of the methods employed to protect secret or sensitive data from malicious attacks.

Cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means.

steganography in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.

Steganography Techniques

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

Text Steganography

Text Steganography is hiding information inside text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences, or using context-free grammar to generate readable texts. Various techniques used to hide the data in the text are:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

For example,

1. Consider the original message: "The quick brown fox jumps over the lazy dog"
2. Choose a secret message to hide within the original message: "Meet me at the park at noon"
3. Replace certain words or letters within the original message with the letters of the secret message to hide it. For example, we could replace the word "park" with "PManOOk" which contains the letters "meet" and "noon" in order. So the modified message would be: "The quick brown fox jumps over the lazy PManOOk"
4. Send the modified message to the recipient
5. The recipient can extract the hidden message by identifying the modified letters and decoding them according to the agreed-upon method.

In this example, the secret message "Meet me at the park at noon" was hidden within the original message using steganography

Image Steganography

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used as cover sources because there are a huge number of bits present in the digital representation of an image.

There are a lot of ways to hide information inside an image. Common approaches include:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation

For example,

1. Consider the original image: An image of a sunset on a beach
2. Choose a region of the image to hide the message: A small patch of the sky
3. Convert the pixel values of the chosen region into binary code
4. Hide the secret message within the binary code by replacing the least significant bits of each pixel with the bits of the secret message
5. Convert the modified pixel values back into an image format
6. Send the modified image to the recipient
7. The recipient can extract the hidden message by identifying the chosen region of the image and decoding the least significant bits of each pixel

Audio Steganography

In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more complex process when compared to others, such as Image Steganography. Different methods of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

Video Steganography

In Video Steganography you can hide kinds of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

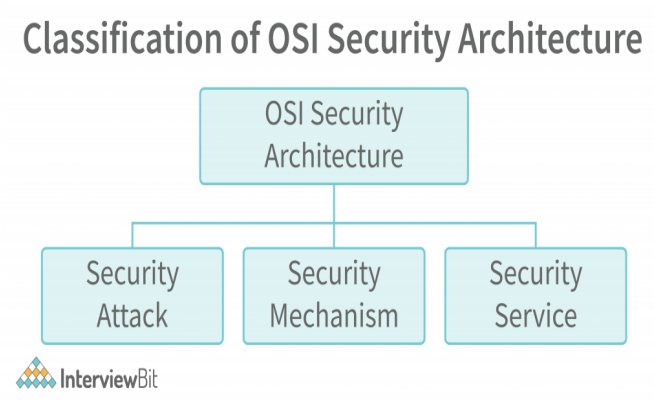
- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

Network Steganography (Protocol Steganography)

It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

12. Explain in brief OSI Security Architecture. (Chpt 1)

Ans)farhat - notebook



The OSI Security model identifies the attacks on a system (data) and also identifies various security services and the mechanisms to implement those services in various layers of the OSI model. Let us first discuss Security Attacks.

Security Attacks

A security attack means any action that puts the data or overall security of the system at risk. An attack might be successful or unsuccessful.

In case of a successful attack, the attacker can complete his/her motive of breaking the security of the system in any way he/she wants to.

In case of an unsuccessful attack, the system remains secured and no harm to the security is done. There are majorly 2 types of attacks: active attacks and passive attacks. Let's discuss them in detail.

1.Passive Attack

A passive attack is a kind of attack in which the data that is sent from the sender to the receiver is read by the attacker in the middle of the transmission. However, the main point to note here is that the passive attack is the attack in which the attacker does not modify or corrupt the data. No changes are made to the data.

The attacker just observes the data sent to the receiver from the sender and can know a lot of information about the sender and the receiver just by observing the communication between them. There are 2 types of passive attacks.

- **Traffic Analysis:** As the name suggests, this attack focuses on the amount or volume of data sent between the sender and the receiver. The attacker can predict a lot of information about the sender and the receiver by knowing the amount of data sent.
- For example, if a lot of data is being sent from the sender to the receiver, it is assumed as there is an emergency, or a task is happening on an urgent basis. If less data is shared between the sender and the receiver, it is assumed that there is a lack of communication and so on.

- **Eavesdropping:** In this kind of attack, the attacker reads the communication that happens between the sender and the receiver and then can use this information for many things. For instance, an attacker can use the information to know about the financial details of the user. Also, this can be used for criminal activities as the attacker can send a lot of personal information to a criminal.
- The difference between eavesdropping and traffic analysis is that in traffic analysis, the attacker does not even read the data. He/she is just focused on the volume of the data. Whereas on the other hand, in eavesdropping, the focus is on the actual data being exchanged between the sender and the receiver.

2. Active Attack

In an active attack, the focus of the attacker is to modify the data that is being exchanged between the sender and the receiver. The most dangerous thing about this attack is that most of the time, the sender and the receiver do not even know that an

attack has happened. There are several types of active attacks. Some of them are as follows:

- **Replay:** In a replay attack, the attacker acts as an authorized user and can use the details of the authorized user to log in to a system. This happens as follows. Suppose that there is a user, and he/she wants to log in to a system. So, they enter their username and password, and this detail reaches in the form of a data packet to the server of the system. The attacker can steal this data packet in between and use this data packet later to log in to the system. You might be wondering that the login details are encrypted, so how would the attacker use them? The encryption will not matter in this case as the data packet as it is, has been stolen and the server might not recognize this and give access to the attacker.

- **Masquerade:** In this attack too, the attacker acts to be an authorized user. Now, this is not done by stealing the data packet. It is done by stealing the login details of the user somehow. So, no technical aspect of stealing the details is involved here.

  For example,

  Mallory decides to launch a masquerade attack by pretending to be Alice. He creates a fake email that appears to be from Alice and sends it to the company's IT department. In the email, Mallory claims that she forgot her password and asks for it to be reset. The IT department, thinking that the request is legitimate, resets Alice's password and sends a temporary password to the email address on file.
  Mallory intercepts the email and gains access to Alice's account. He logs in using the temporary password and gains access to the confidential financial records. The company is unaware that an attack has taken place and only discovers the breach when they review the logs later.

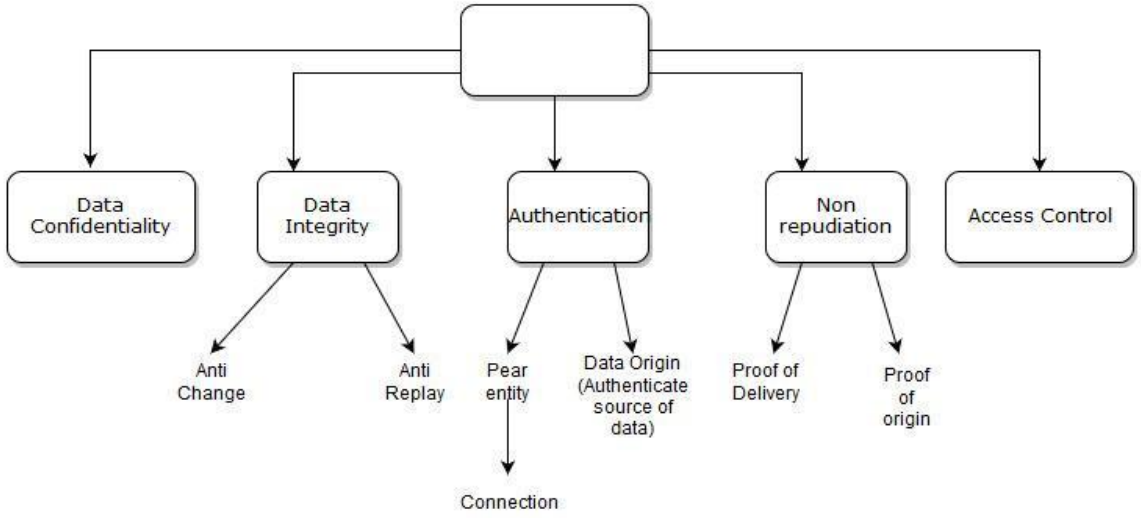
- **Denial of Service (DOS):** The denial-of-service attack is an attack in which a system is attacked by a lot of requests to the system at one time that it is not able to handle. The attacker sends multiple requests to the server at the same time and the server is not able to handle such requests. However, this attack is easily identifiable as these loads of requests come from a single sender (the attacker) and it is easy to identify the source of the attack.

- **Distributed Denial of Service (DDOS):** As we saw, in the denial-of-service attack, the source of the attack can be easily identified. Now, there is a modified version of this attack i.e., DDOS i.e., distributed version of the DOS attack. In this attack, the attacker first observes the details of a lot of authorized users. Then, the attacker uses these authorized users at the same time to send requests to

the system. Now, thousands (or even more) of requests at the same are sent to the system and the system cannot recognize the source of attack as there is each request from a different user, and all the users are authorized. So, the attacker is using the authorized users as victims too. The primary victim is the system, and the secondary victims are the authorized users. The authorized users are called Zombie PCs.

Security Services:

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



It has 5 categories:

Authentication: The assurance that the communicating entity is the one that it claims to be.

This is a very basic and easy service to implement. In authentication, the system (both sender and receiver) identifies the user first. Only the user authorized to enter the system can use it. This can be done using basic password protection.

E.g In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

- **Peer Entity Authentication:**
  Peer Entity Authentication is a security mechanism used to verify the identity of entities (computers, devices, or applications) that are communicating with each other over a logical connection, such as a network connection. The purpose of

this authentication is to provide confidence in the identity of the entities involved in the communication. This is important because without proper authentication, there is a risk that a malicious attacker may impersonate a legitimate entity and gain access to sensitive information or perform unauthorized actions.
In Peer Entity Authentication, each entity is required to provide proof of its identity before the connection is established. This is typically achieved using a set of shared keys or certificates that are verified by both parties during the connection setup process. Once the identity of both parties is verified, the connection can be established with confidence.

- **Data-Origin Authentication:**
  Data-Origin Authentication is a security mechanism used to verify the source of data that is received during a connectionless transfer. In a connectionless transfer, data is sent over the network without establishing a dedicated logical connection beforehand. This means that there is no guarantee that the data was sent by the claimed source, and there is a risk of data tampering or spoofing.
  To provide assurance that the source of received data is as claimed, Data-Origin Authentication uses a technique called Message Authentication Code (MAC). A MAC is a cryptographic checksum that is generated by combining the data with a secret key. The MAC is sent along with the data and can be verified by the receiver using the same secret key. If the MAC is correct, the receiver can be confident that the data was sent by the claimed source and has not been tampered with during transmission.

Data Confidentiality: Protects data from unauthorized disclosure.

This is one of the three pillars of the security model CIA (Confidentiality, Integrity, and Availability). Confidentiality means that the data i.e. is shared between a sender and receiver should be confidential to them only. No third party should be able to read the data.

Access Control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Data Integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Integrity means that no third party should be able to modify the data i.e. is shared between the sender and the receiver.

Non-repudiation: Protects against denial by one of the entities involved in a communication of having participated in all or part of the communication.

OR

It prevents either the sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the sender in fact sent the message.

Similarly, when the message is received, the sender can prove that the receiver in fact received the message.

Proof of Origin: Proof that the message was sent by the specified party.

Proof of Delivery: Proof that the message was received by the specified party.

Security Mechanisms

The mechanisms that help in setting up the security services in different layers of the OSI model and that help in identifying any attack or data breach are called security mechanisms. The security mechanisms provide a way of preventing, protecting, and detecting attacks. Some of the security mechanisms are as follows:

- **Encipherment (Encryption):** One of the most popular security mechanisms is encryption. The message/data sent from the sender to the receiver is usually encrypted to some format that even if the message is stolen, cannot be decrypted easily by the attacker. Some of the popular encryption algorithms are AES, RSA, Triple DES, etc.

- **Traffic Padding:** The sender and receiver send the data to each other. Now, sometimes there is a gap between the sender and receiver. This means that for some time when the sender and receiver are not sharing the data, the attacker can act as if it is the sender and send some data to the receiver to attack it. So, this can be avoided if the gap (empty time) between the sender and the receiver is not known to the attacker. For this, during the gap duration, the sender keeps on sending some dummy data to the receiver and the receiver knows that this is the dummy data by using some identification. Hence, no gap is created between the sender and the receiver and the attacker cannot attack the system.

- **Routing Control:** The messages that a sender sends to a receiver travel different routes, However, in some cases, the sender and receiver might communicate mostly via the same route. In this case, the attacker tracks this route and can make changes to the data or take advantage of this. So, routing should be controlled in such a way that mostly, a different route is selected between the sender and the receiver to deliver the message.

So, these were some of the security mechanisms that can be used to detect/prevent attacks. This is the complete OSI Security model. Let us now discuss some benefits of OSI Security Architecture.

EXTRA QUESTIONS

1. **Explain relationship between Security Services and Mechanism in detail.**

Ans) Implement services using the mechanisms from above

Security services are the goals that a secure system should achieve, while security mechanisms are the tools that are used to achieve those goals. In other words, security mechanisms are used to implement security services.

For example, the security service of confidentiality is achieved through the use of encryption mechanisms.

Encryption ensures that data is transformed into a form that can only be read by someone who has the key to decrypt it. This mechanism ensures that information remains confidential and protected from unauthorized access.

Similarly, the security service of integrity is achieved through the use of hash functions, digital signatures, and other mechanisms that ensure that information is not altered or tampered with in any way. These mechanisms help to maintain the integrity of data and ensure that it is not modified without authorization.

2. **Define non-repudiation and authentication. Show with example how it can be achieved.**

Ans) Authentication is the process of verifying the identity of a user or system, to ensure that they are who they claim to be. This is typically done by using a combination of something the user knows (such as a password or PIN), something they have (such as a smart card or security token), or something they are (such as a biometric identifier like a fingerprint).

Non-repudiation, on the other hand, is the ability to prove that a message or transaction was sent or received by a particular party, and that the sender cannot deny having sent it. Non-repudiation ensures that the sender of a message cannot later deny having sent it, and provides evidence that can be used to prove the authenticity and integrity of the message.

An example of how authentication and non-repudiation can be achieved is through the use of digital signatures. A digital signature is an electronic method of authentication that uses a cryptographic algorithm to validate the authenticity and integrity of a document or message.

To create a digital signature, the sender uses a private key to encrypt a hash of the message, which is then sent along with the message itself. The recipient can then use the sender's public key to decrypt the signature and verify that the message has not been tampered with and was indeed sent by the sender. This process ensures both authentication and non-repudiation, since the recipient can prove that the message was sent by the sender and that it has not been modified in transit.

For example, suppose Alice wants to send a confidential message to Bob. Alice can use a digital signature to authenticate the message and ensure that Bob can verify the message came from her. She can use her private key to create a signature, which is sent along with the message. Bob can then use Alice's public key to verify the signature and ensure that the message is genuine and has not been tampered with. This provides both authentication and non-repudiation, since Alice cannot deny having sent the message and Bob can prove that it came from her.

3. **Enlist security goals. Discuss their significance.**

Ans)

The CIA Triad is a benchmark model in information security designed to govern and evaluate how an organization handles data when it is stored, transmitted, or processed.

Each attribute of the triad represents a critical component (goals) of information security. The CIA triad is depicted in Fig. 1.2.1.

(1) **Confidentiality :** Data should not be accessed or read without authorization. It ensures that only authorized parties have access. Attacks against Confidentiality are disclosure attacks.

(2) **Integrity :** Data should not be modified or compromised in anyway. It assumes that data remains in its intended state and can only be edited by authorized parties. Attacks against Integrity are alteration attacks.

(3) **Availability :** Data should be accessible upon legitimate request. It ensures that authorized parties have unimpeded access to data when required. Attacks against Availability are destruction attacks.

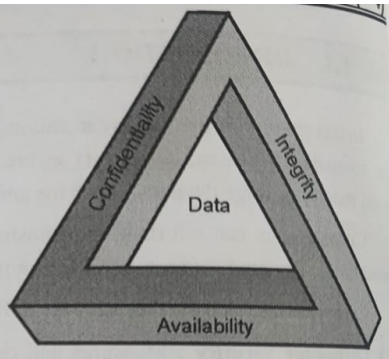


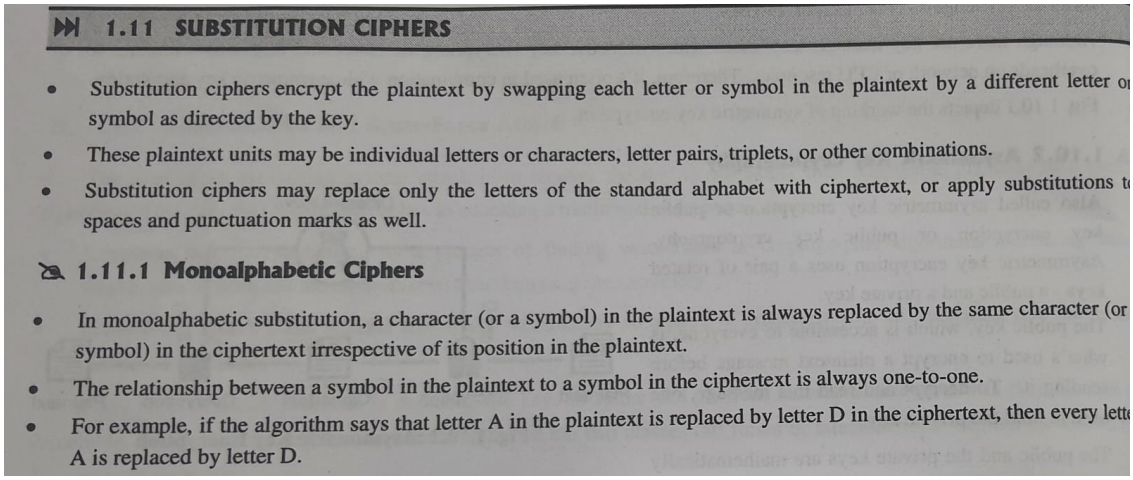
Fig. 1.2.1 : CIA Triad

4. **What are traditional ciphers? Discuss any substitution and transposition cipher with example. List their merits and demerits.**

Ans)

Traditional ciphers are a type of encryption technique that have been used for centuries to protect sensitive information. These ciphers are typically based on mathematical algorithms that transform plaintext (the original message) into ciphertext (the encoded message) using a secret key but the transformation of plain text to cipher text can be keyless as well.

The two types of traditional ciphers are Substitution Cipher and Transposition Cipher.

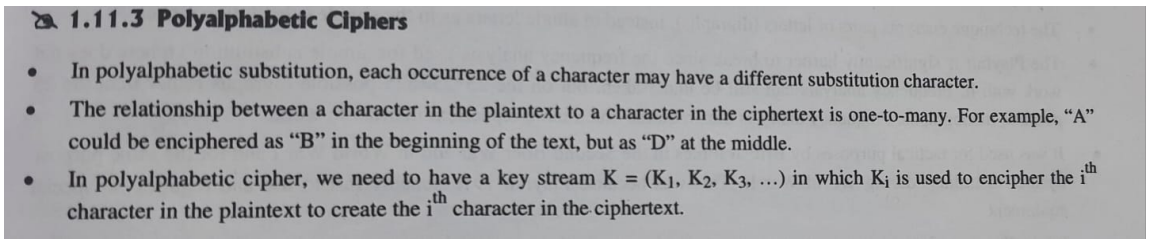


1.11 SUBSTITUTION CIPHERS

- Substitution ciphers encrypt the plaintext by swapping each letter or symbol in the plaintext by a different letter o symbol as directed by the key.
- These plaintext units may be individual letters or characters, letter pairs, triplets, or other combinations.
- Substitution ciphers may replace only the letters of the standard alphabet with ciphertext, or apply substitutions t spaces and punctuation marks as well.

1.11.1 Monoalphabetic Ciphers

- In monoalphabetic substitution, a character (or a symbol) in the plaintext is always replaced by the same character (or symbol) in the ciphertext irrespective of its position in the plaintext.
- The relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
- For example, if the algorithm says that letter A in the plaintext is replaced by letter D in the ciphertext, then every lett A is replaced by letter D.



1.11.3 Polyalphabetic Ciphers

- In polyalphabetic substitution, each occurrence of a character may have a different substitution character.
- The relationship between a character in the plaintext to a character in the ciphertext is one-to-many. For example, "A" could be enciphered as "B" in the beginning of the text, but as "D" at the middle.
- In polyalphabetic cipher, we need to have a key stream $K = (K_1, K_2, K_3, \ldots)$ in which K_i is used to encipher the i^{th} character in the plaintext to create the i^{th} character in the ciphertext.

Types of monoalphabetic : Additive/Caeser/Shift cipher, Multiplicative, Affine
Types of polyalphabetic: Playfair(i/j),Vigenere, Hill ciphers
Read theory and egs of above from TechNeo
Merits:

1. **Simplicity:** Substitution ciphers are relatively easy to understand and use. They require only a simple set of rules for encrypting and decrypting messages.
2. **Speed:** Substitution ciphers can be applied quickly, making them suitable for use in situations where time is of the essence.
3. **Historical significance:** Substitution ciphers have played an important role in many historical events, including wars, politics, and espionage. As a result, they have a rich cultural and historical significance.

Demerits:

1. **Vulnerability:** Substitution ciphers are vulnerable to cryptanalysis. With enough knowledge and resources, an attacker can analyze the ciphertext and use various techniques to break the encryption and reveal the plaintext.
2. **Limited key space:** Substitution ciphers have a relatively small key space, meaning that the number of possible keys is limited. This makes them easier to break than more complex encryption methods that use larger key spaces.
3. **Lack of security:** Substitution ciphers are generally considered to be less secure than modern encryption methods like the Advanced Encryption Standard

(AES). As a result, they are not suitable for use in situations where high levels of security are required.

Network Security Model:

1.8 NETWORK SECURITY MODEL

- A Network Security Model demonstrates how the security service has been configured over the network to prevent the opponent from jeopardizing the confidentiality or authenticity of the data being transmitted over the network.
- For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e. **Information channel** which is an **Internet** service.
- A logical route is defined through the network (Internet), from sender to the receiver and using the **communication protocols** (e.g. TCP/IP, etc.) both the sender and the receiver established communication.

ıl network security model is given in Fig. 1.8.1.

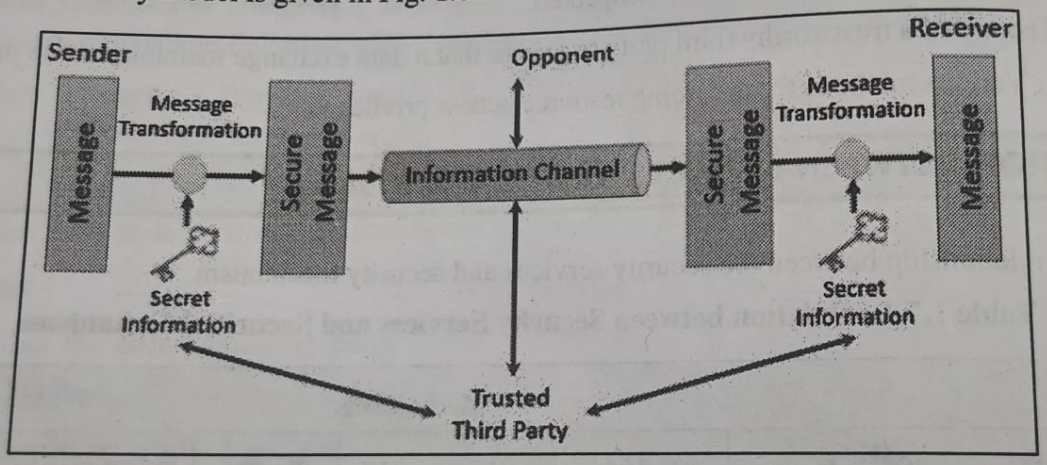
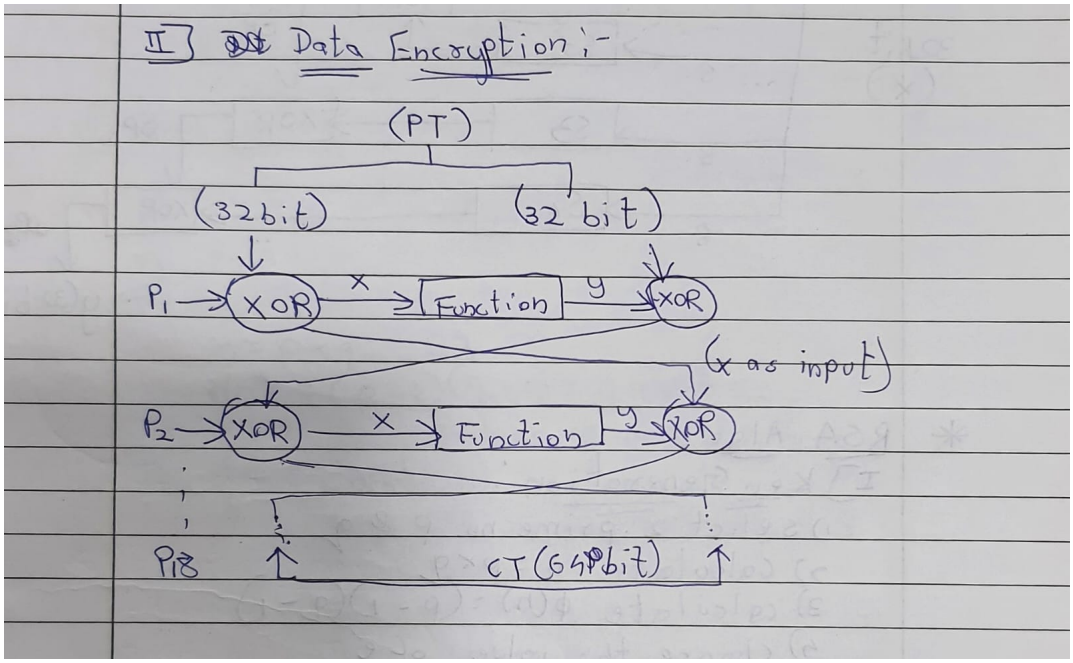


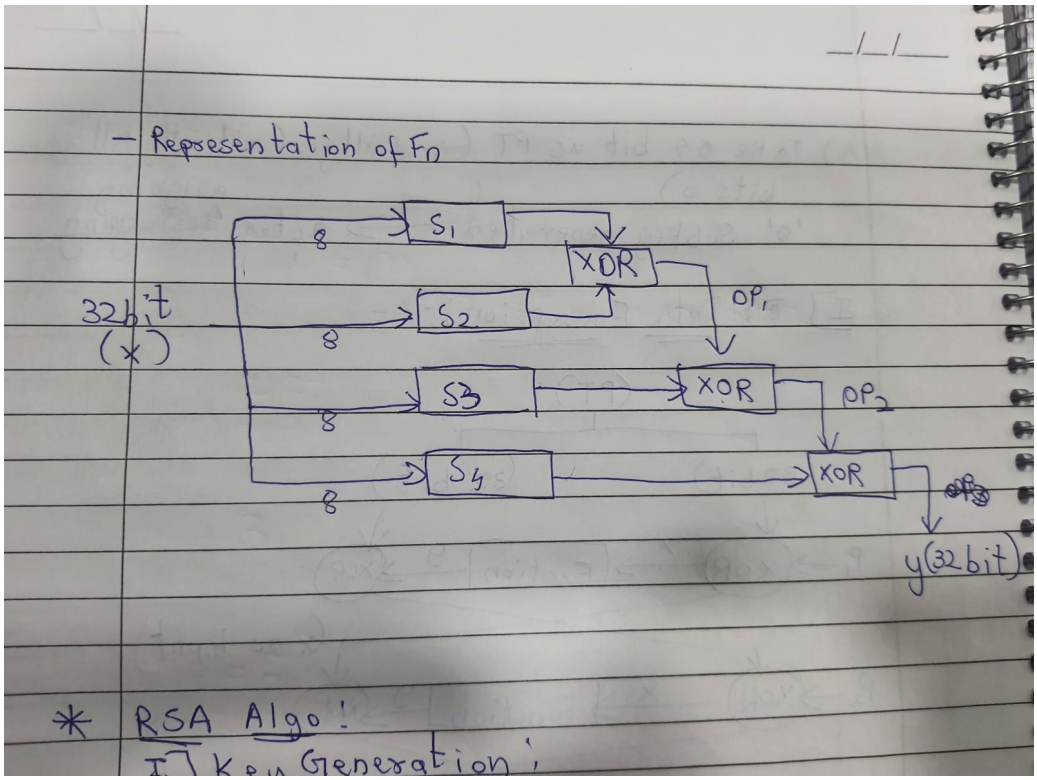
Fig. 1.8.1 : Network Security Model

MODULE - 2

3. Draw a data encryption diagram in blowfish. (Chpt 2)

Ans)





Blowfish is an encryption technique used as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block

ciphers not subject to any patents and hence freely available for anyone to use. It uses symmetric key cryptography.

- **blockSize**: 64-bits
- **keySize**: 32-bits to 448-bits variable size
- **number of subkeys**: 18 [P-array]
- **number of rounds**: 16
- **number of substitution boxes**: 4 [each having 512 entries of 32-bits each]

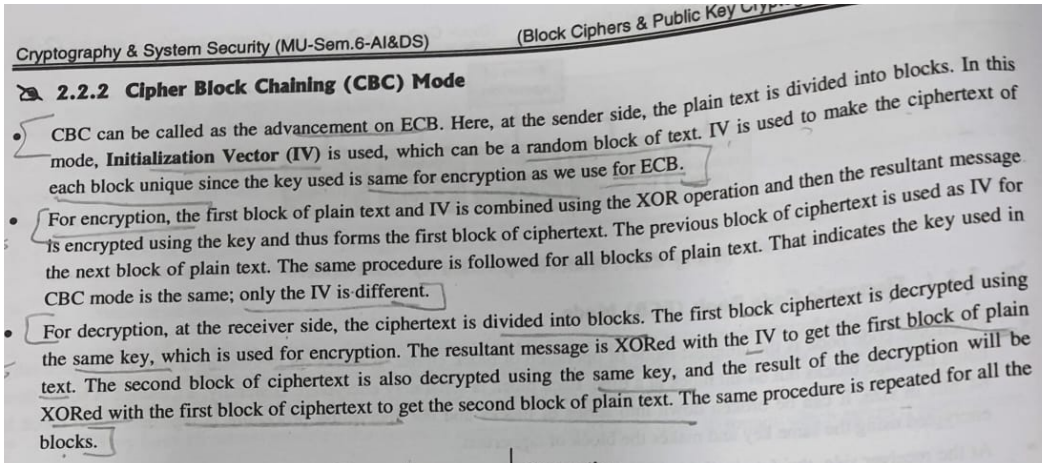
STEPS of AIGORITHM: (notes)

1. Key generation
    - Stored in array (1-14 key size)
    - Initialize P-array (1 array -> 18 words, len of 1 word-> 32 bits)
    - Initialize S-boxes(Substitution boxes)(256 size)
    - Initialize each element of P-array and S-box with hexadecimal value
    - Perform XOR operations (p1=p1 XOR k1 ....p14 = p14 XOR k14, p15=p15 XOR k1…p18)
    - Take 64-bit as PT(initially all bits are 0)

2. Data Encryption

9. Define CBC mode with flow diagram. (Chpt 2)

Ans)



Cryptography & System Security (MU-Sem.6-AI&DS) (Block Ciphers & Public Key Cryp...

2.2.2 Cipher Block Chaining (CBC) Mode

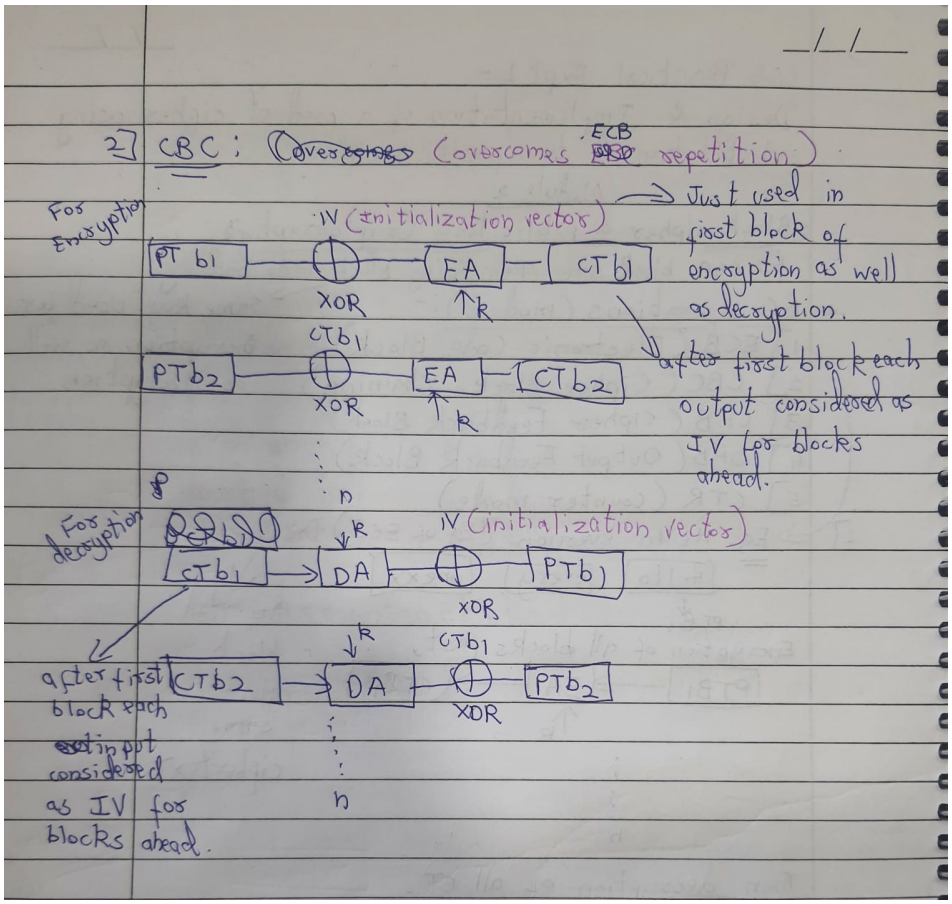
- CBC can be called as the advancement on ECB. Here, at the sender side, the plain text is divided into blocks. In this mode, **Initialization Vector (IV)** is used, which can be a random block of text. IV is used to make the ciphertext of each block unique since the key used is same for encryption as we use for ECB.
- For encryption, the first block of plain text and IV is combined using the XOR operation and then the resultant message is encrypted using the key and thus forms the first block of ciphertext. The previous block of ciphertext is used as IV for the next block of plain text. The same procedure is followed for all blocks of plain text. That indicates the key used in CBC mode is the same; only the IV is different.
- For decryption, at the receiver side, the ciphertext is divided into blocks. The first block ciphertext is decrypted using the same key, which is used for encryption. The resultant message is XORed with the IV to get the first block of plain text. The second block of ciphertext is also decrypted using the same key, and the result of the decryption will be XORed with the first block of ciphertext to get the second block of plain text. The same procedure is repeated for all the blocks.

☞ **Advantages of CBC**

1. Better resistive nature towards cryptanalysis than ECB due to changing IV.
2. CBC works well for greater inputs.
3. CBC forms the basis for a well-known data origin authentication mechanism. Thus, it is used for those applications that require both symmetric encryption and data origin authentication.

☞ **Disadvantages of CBC**

1. The error in transmission gets propagated to few further blocks during decryption due to chaining effect.
2. Parallel encryption is not possible since every encryption requires previous cipher.



EXTRA

1. Discuss DES with reference to following points
    - Block size and key size
    - Need of expansion permutation
    - Role of S-box
    - Weak keys and semi-weak keys
    - Possible attacks on DES **(repeated in dec2019)**

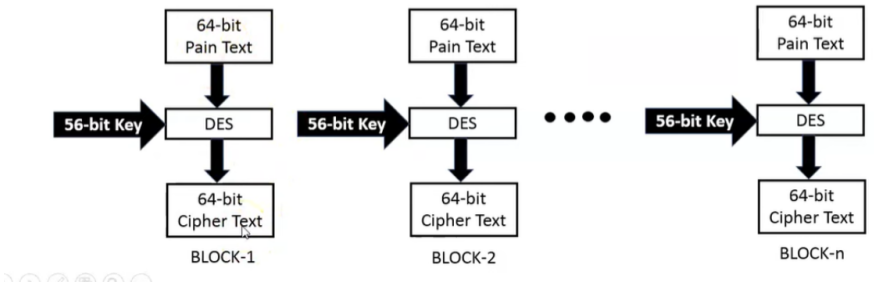
Ans)

Block size and Key size

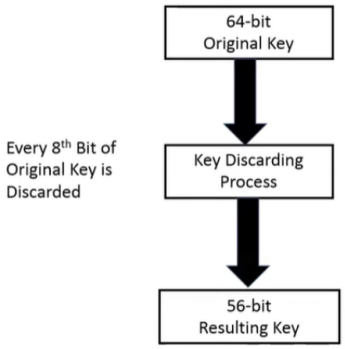
Data encryption standard (DES) is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is **56 bits**.

The basic idea is shown in the figure:

- **Figure shows process of DES**



- **Key discarding process**



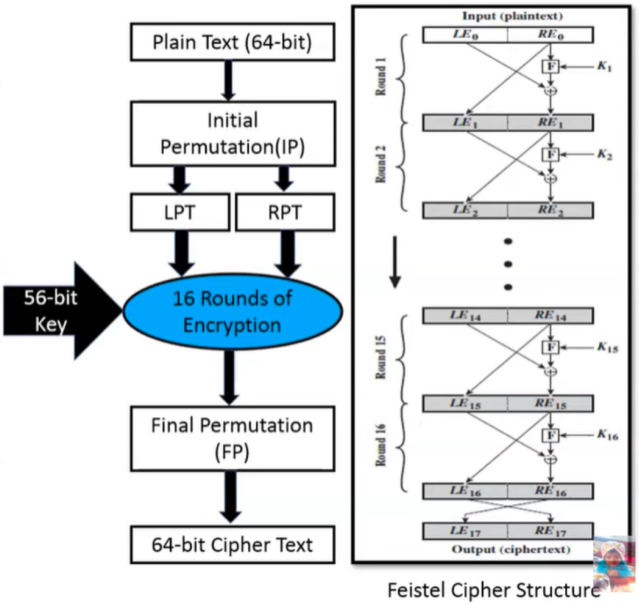
1	2	21	38	58	15	37	26
22	55	44	3	53	27	11	60
49	28	14	42	61	48	63	41
18	39	56	10	64	16	62	8
45	40	20	54	4	33	34	52
7	30	47	59	32	5	35	25
29	12	13	6	24	46	57	36
17	23	50	31	43	51	9	19

1	2	21	38	58	15	37
22	55	44	3	53	27	11
49	28	14	42	61	48	63
18	39	56	10	64	16	62
45	40	20	54	4	33	34
7	30	47	59	32	5	35
29	12	13	6	24	46	57
17	23	50	31	43	51	9

We have mentioned that DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is, bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

❖ Steps of DES

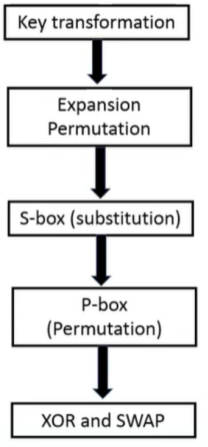
1. 64-bit plain text block is given to Initial Permutation (IP) function.
2. IP performed on 64-bit plain text block.
3. IP produced two halves of the permuted block known as Left Plain Text (LPT) and Right Plain Text (RPT).
4. Each LPT and RPT performed 16-rounds of encryption process.
5. LPT and RPT rejoined and Final Permutation (FP) is performed on combined block.
6. 64-bit Cipher text block is generated.



Feistel Cipher Structure

16 Rounds of Encryption

1. Key Transformation (56-bit key)
   - Key Bit Shifted per round
   - Compression Permutation
2. Expansion permutation of Plain Text and X-OR (P.T. size: 48 bit, C.T. size: 48 bit)
3. S-box Substitution
4. P-box (Permutation)
5. X-OR and Swap.



Need for Permutation Expansion:

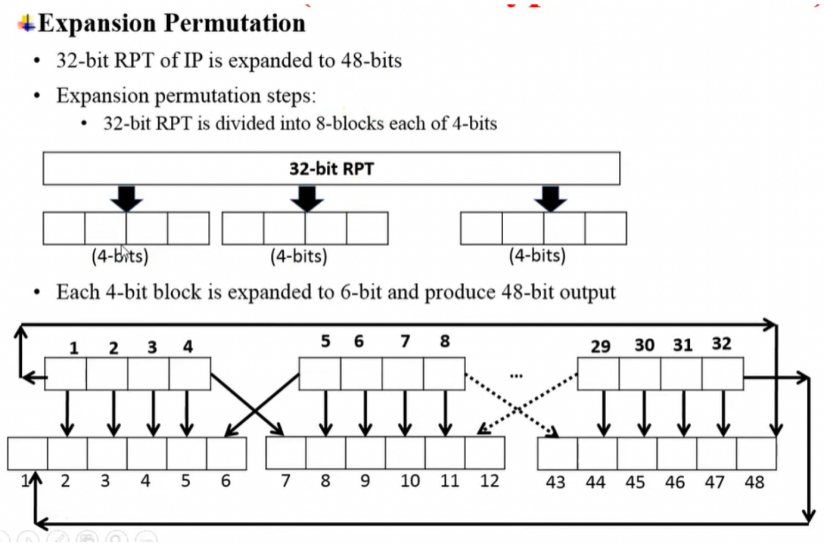
The expansion permutation is an important step in the Data Encryption Standard (DES) algorithm. It is used to expand a 32-bit block of data into a 48-bit block, which is then used in the subsequent round of DES encryption.

The expansion permutation is necessary for a few reasons:

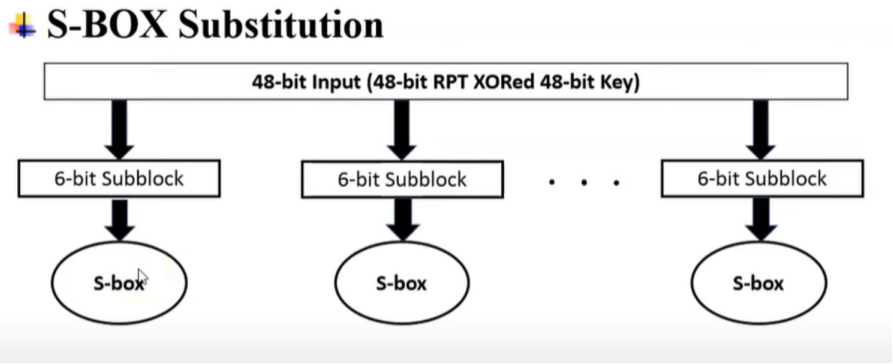
Increase the size of the data block: The 32-bit block of data is too small to provide sufficient security on its own. By expanding it to 48 bits, the security of the encryption is increased.

Introduce more diffusion: The expansion permutation shuffles the bits of the original block, introducing more diffusion into the encryption process. This helps to make the encryption stronger and more resistant to attacks.

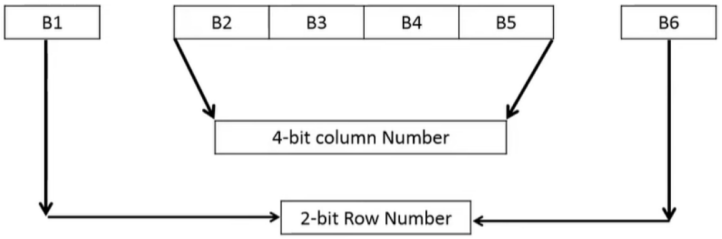
Introduce redundancy: The expansion permutation introduces some redundancy into the data block. This redundancy helps to detect errors in transmission or decryption, and can also help to prevent certain types of attacks.

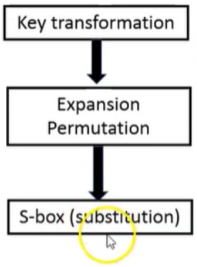


Role of S-BOX



S-BOX Working





S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Example: 011011 → 1001

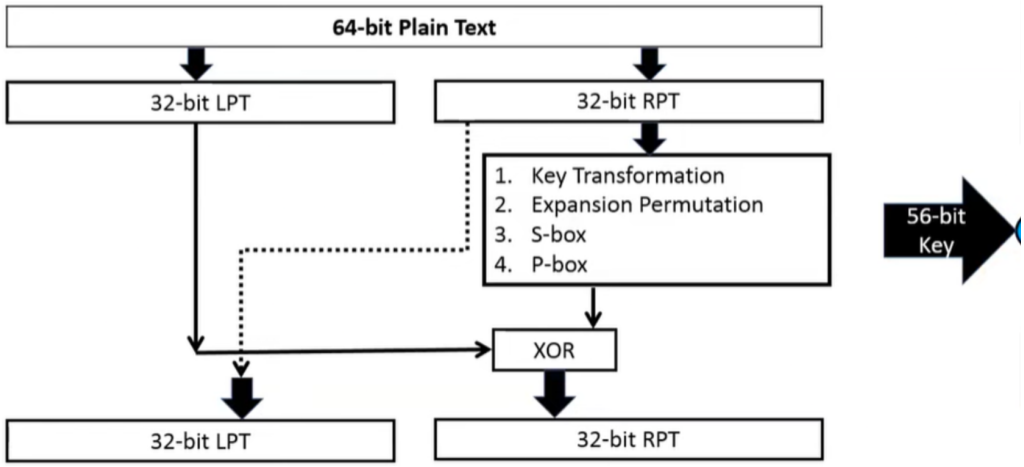
P-BOX Permutation

- Output of s-box is given to p-box
- 32-bit is permuted with 16 x 2 permutation table
- **For Example:**
  - ✓ 16th bit of S-box take 1st Position as per below permutation table.

P – Box Table															
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

XOR and SWAP

- 32-bit LPT is XORed with 32-bit p-box.



- 1st round of encryption is completed. Now remaining 15 rounds will be performed same as 1st round.

Attacks on DES

1- Brute Force Attack

Brute Force is the most simple and practical way to break a cipher. It consists in trying every key combination possible until the right one is found. Having the right key you can then break the cipher and read what was ciphered. The number of possibilities is determined by the keys size in bits, since DES only has a 64 bit key, the number of combinations is rather small and a personal computer can break it in a few days. This was the main reason why DES lost its credibility and began not to be used.

2- Differential cryptanalysis (DC)

In order to break all the 16 rounds of the DES there were 2^49 chosen texts. Since DES was designed to be DC resistant this was for sure a glitch that could make a faster attack, because the possibilities are not infinite like in brute force, but still it might be as bad, because the attacker needs to be lucky to find a suitable text not beyond the 2^49 attempt.

3- Linear cryptanalysis (LC)

Using the LC method there were "only" needed 2^43 Known plaintexts.

4- Davies Attack(DA)

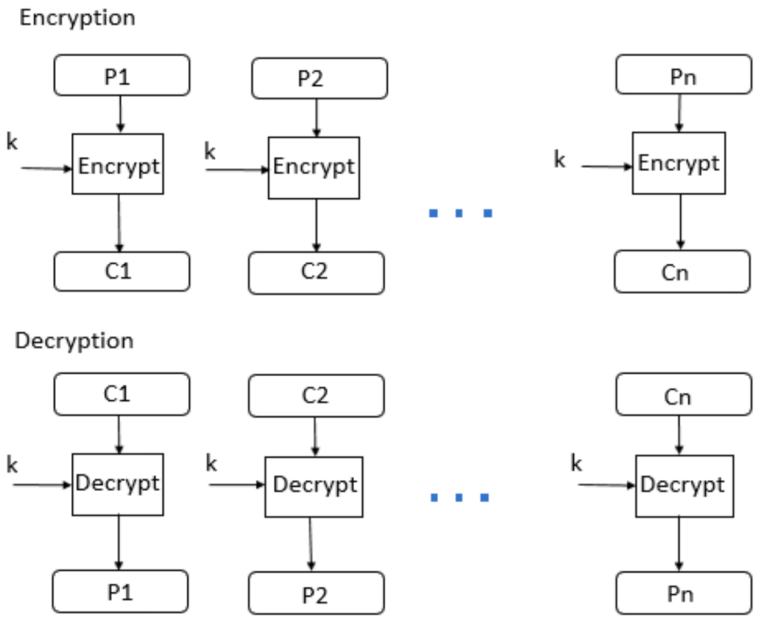
Davies attack was a specialized attack that only applies to DES. The LC and DC are general attacks suitable for a lot more algorithms. Davies said that to break the DES it is required 2^50 Known plaintexts with a success rate of 51%.

Q.Block Cipher and its type of modes:

Ans)

Block cipher is an encryption algorithm that takes a fixed size of input, say *b* bits and produces a ciphertext of *b* bits again. If the input is larger than *b* bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

ECB:



- ECB mode stands for **Electronic Code Block Mode**. It is one of the simplest modes of operation. In this mode, the plain text is divided into a block where each block is 64 bits. Then each block is encrypted separately. The same key is used for the encryption of all blocks.
- At the receiver side, the data is divided into a block, each of 64 bits. The same key which is used for encryption is used for decryption. It takes the 64-bit ciphertext and, by using the key, converts the ciphertext into plain text.
- As the same key is used for all blocks' encryption, if the block of plain text is repeated in the original message, then the ciphertext's corresponding block will also repeat. As the same key is used for all blocks, to avoid the repetition of block ECB mode is used for only small messages where the repetition of the plain text block is less.

CFB (Cipher Feedback Block):

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of s and b-s bits.The left-hand side s bits are selected along with plaintext bits to which an XOR operation is applied. The result is given as input to a shift register having b-s bits to lhs,s bits to rhs and the process continues. The encryption and decryption process

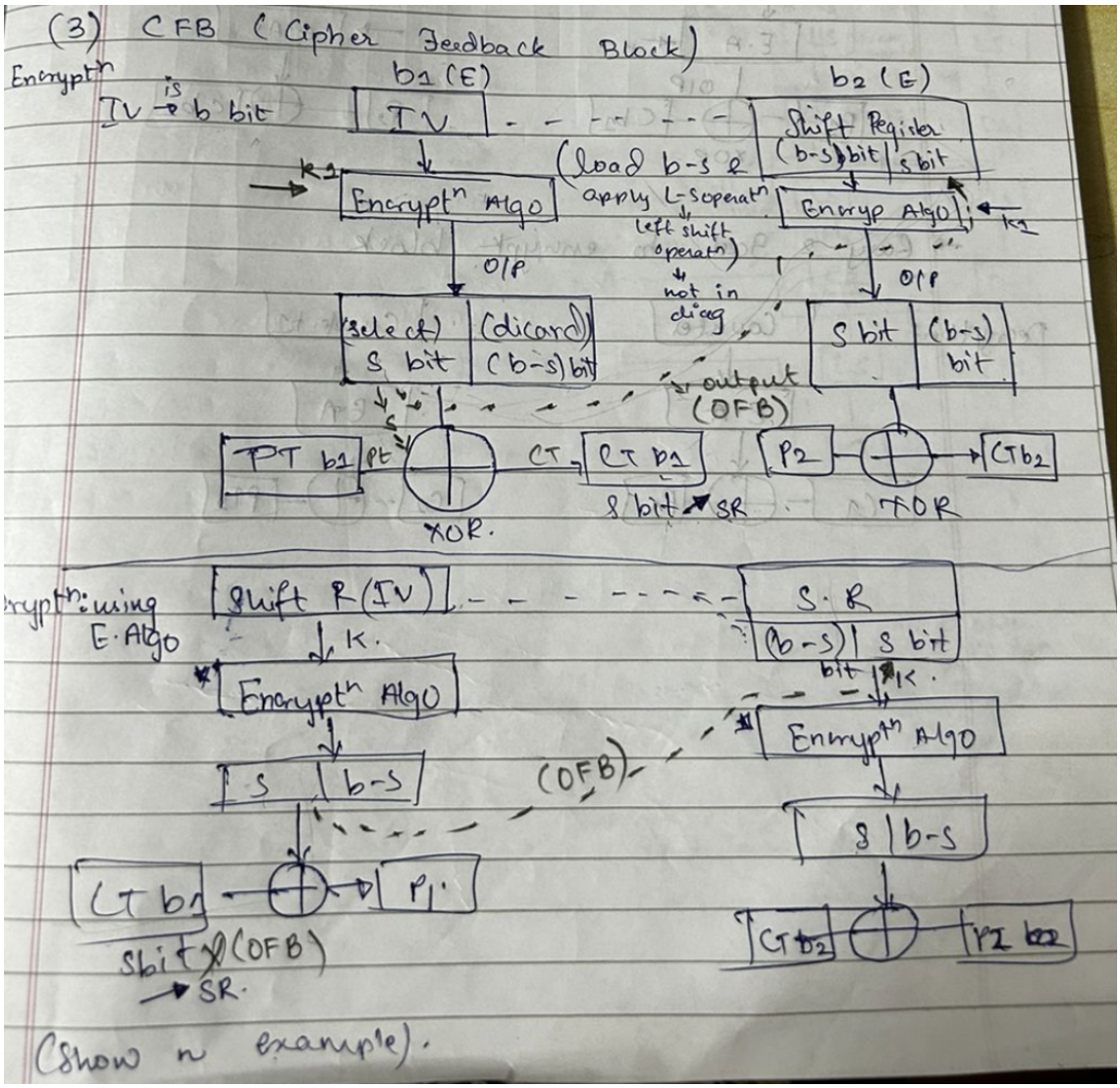
for the same is shown below, both of them use encryption algorithms.

OFB mode:

● OFB Mode stands for output feedback Mode. OFB mode is similar to CFB mode; the only difference is in CFB, the ciphertext is used for the next stage of the encryption process, whereas in OFB, the output of the IV encryption is used for the next stage of the encryption process.

● The IV is encrypted using the key and forms an encrypted IV. Plain text and leftmost 8 bits of encrypted IV are combined using XOR and produce the ciphertext.

● For the next stage, the ciphertext, which is the form in the previous stage, is used as an IV for the next iteration. The same procedure is followed for all blocks.

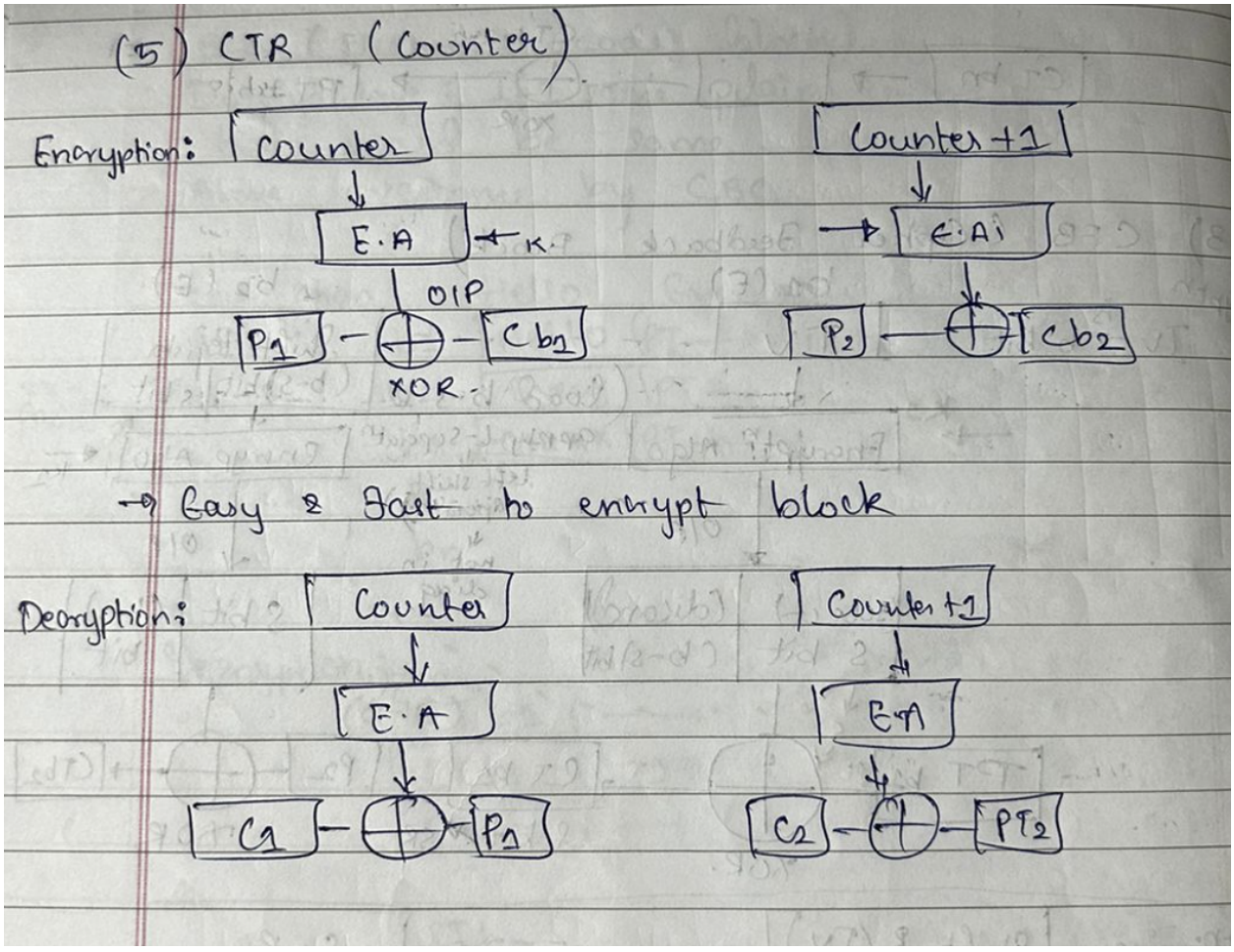


CTR Mode:

● CTR Mode stands for counter mode. As the name is counter, it uses the sequence of numbers as an input for the algorithm. When the block is encrypted, to fill the next register the next counter value is used.
Note: the counter value will be incremented by 1.

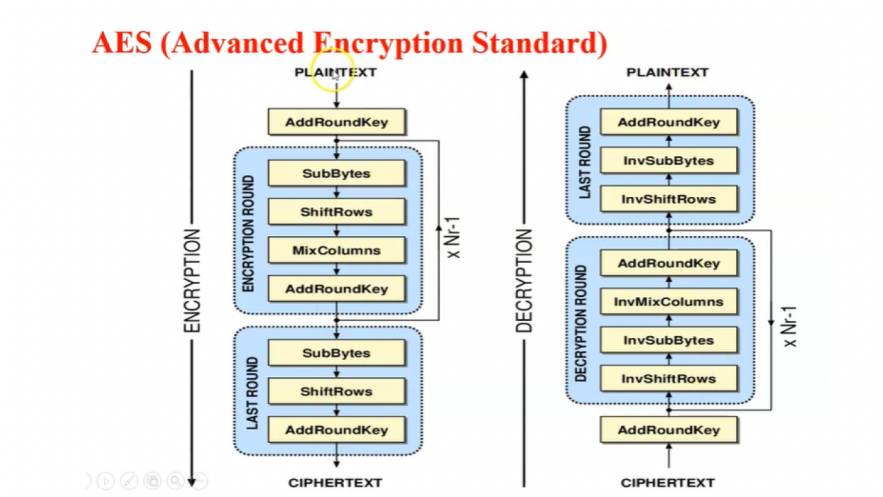
● For encryption, the first counter is encrypted using a key, and then the plain text is XOR with the encrypted result to form the ciphertext.

● The counter will be incremented by 1 for the next stage, and the same procedure will be followed for all blocks. For decryption, the same sequence will be used. Here to convert ciphertext into plain text, each ciphertext is XOR with the encrypted counter. For the next stage, the counter will be incremented by the same will be repeated for all Ciphertext blocks.

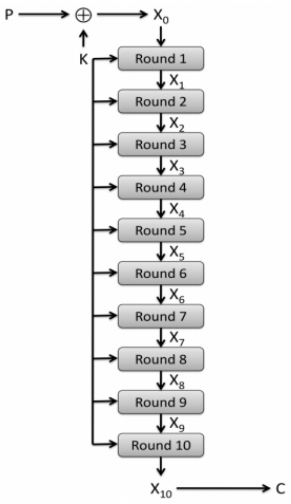


AES Algorithm:

Ans)



The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A **128-bit key size** dictates **10 rounds**, a **192-bit key size** dictates **12 rounds,** and a **256-bit key size** has **14 rounds**. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

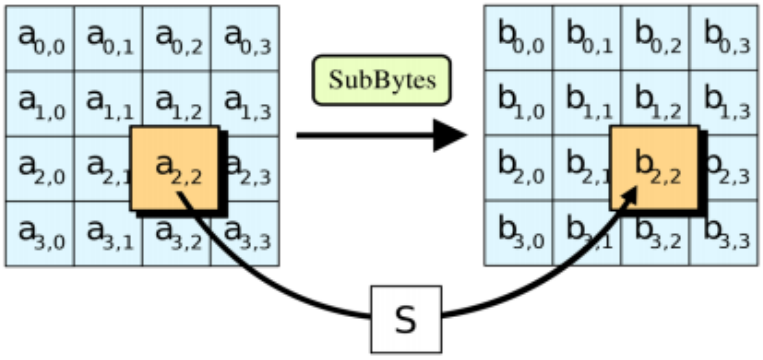


Steps in each round

Each round in the algorithm consists of four steps.

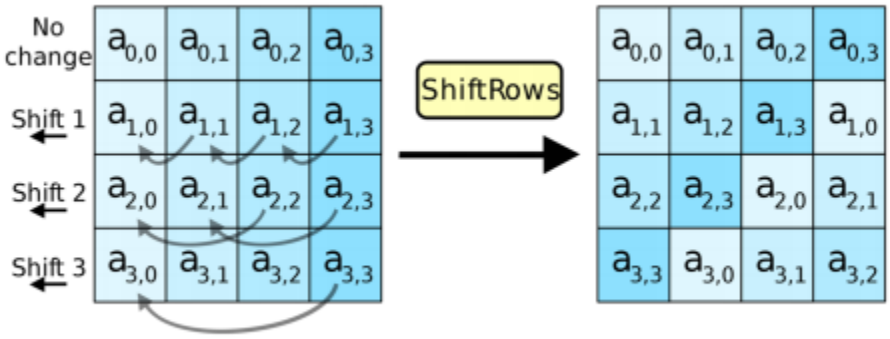
1. Substitution of the bytes

In the first step, the bytes of the block text are substituted based on rules dictated by predefined S-boxes (short for substitution boxes).



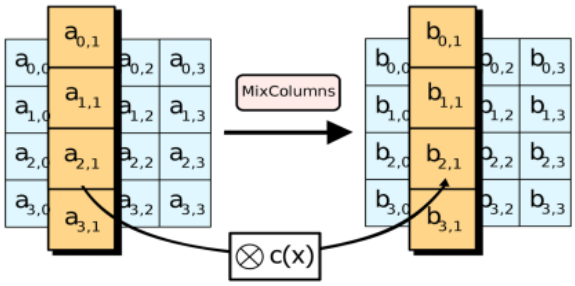
2. Shifting the rows

Next comes the permutation step. In this step, all rows except the first are shifted by one, as shown below.



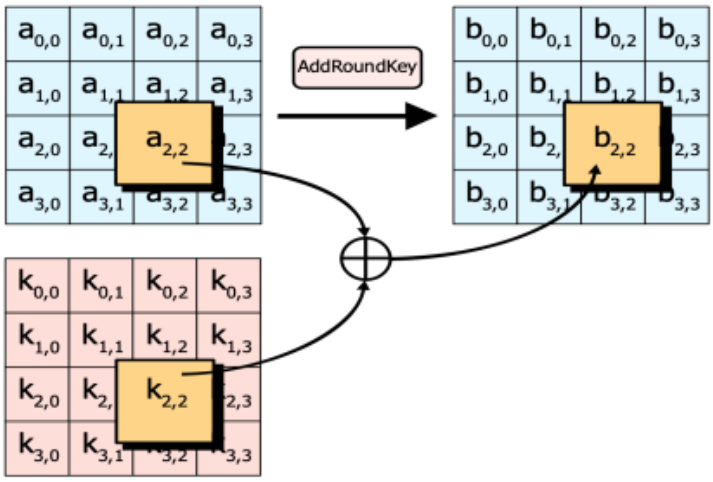
3. Mixing the columns

In the third step, the Hill cipher is used to jumble up the message more by mixing the block's columns.

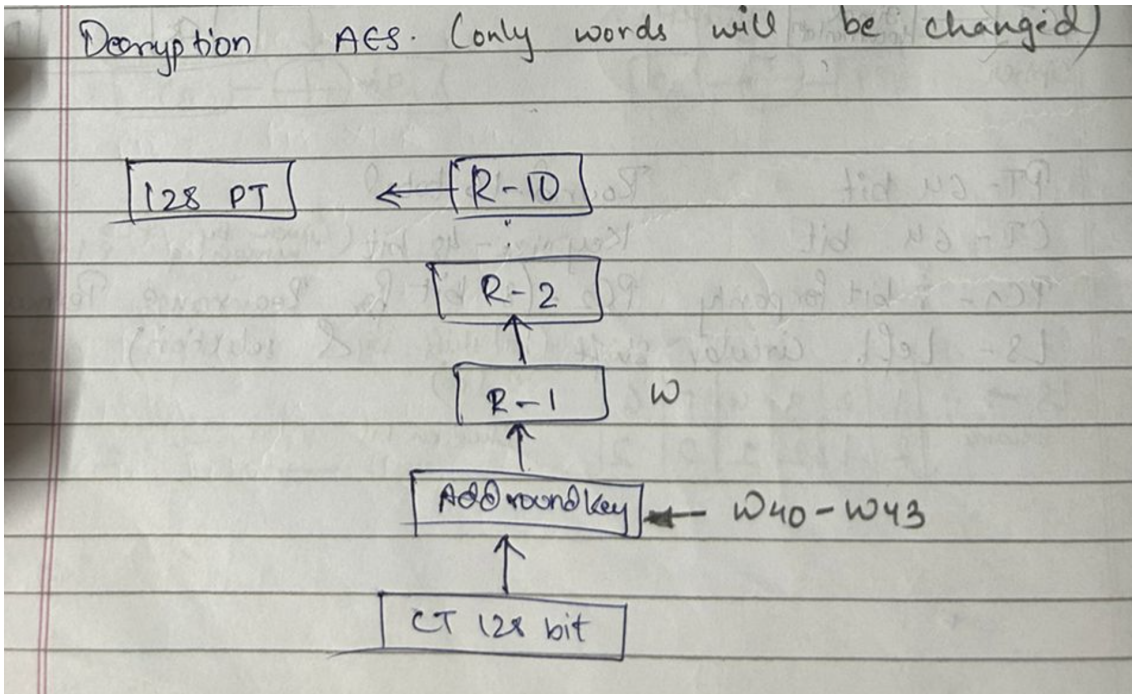


4. Adding the round key

In the final step, the message is XORed with the respective round key.



When done repeatedly, these steps ensure that the final ciphertext is secure.
Decryption:



TRIPLE AND DOUBLE DES:

Data encryption standard (DES) uses 56 bit key to encrypt any plain text which can be easily cracked by using modern technologies. To prevent this from happening double DES and triple DES were introduced which are much more secure than the original DES because it uses 112 and 168 bit keys respectively. They offer much more security than DES.

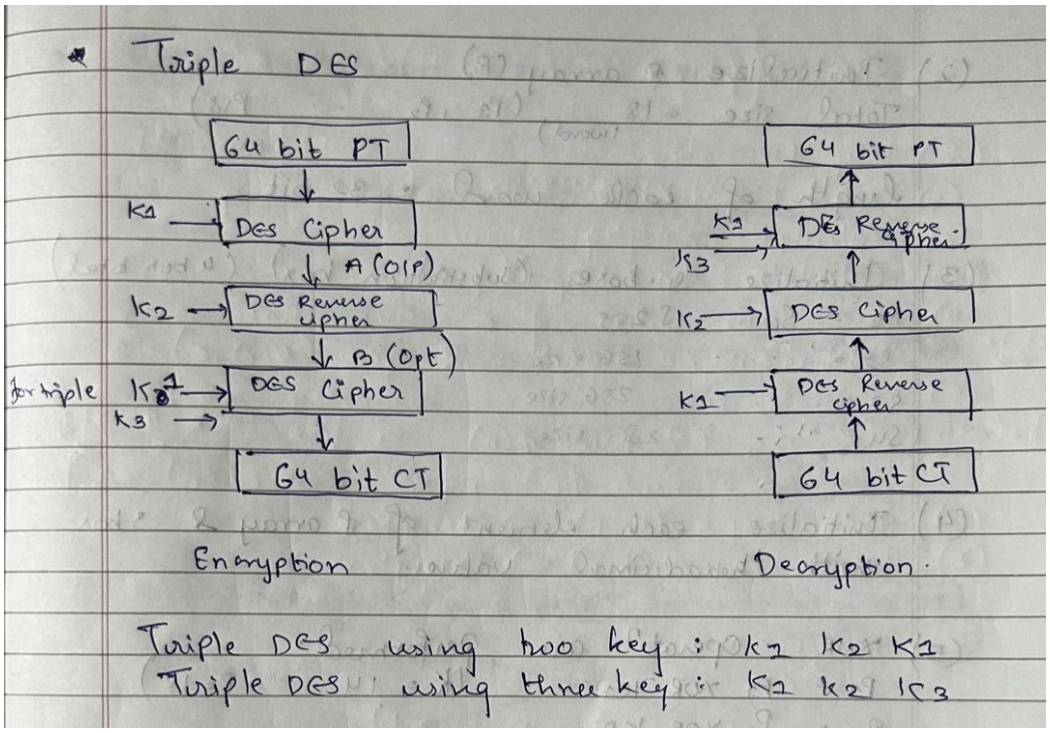
Double DES:

Double DES is a encryption technique which uses two instance of DES on

same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64 bit plain text goes into first DES instance which then converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using a second key.
However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

Triple DES:

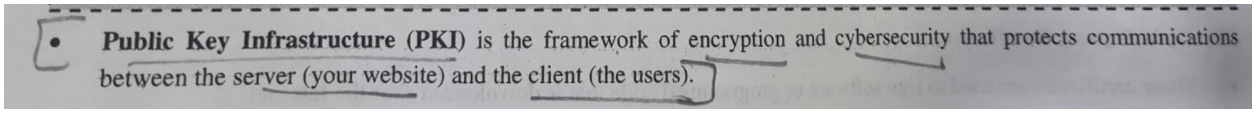
Triple DES is a encryption technique which uses three instance of DES on same plain text. It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are the same.
Triple DES is also vulnerable to meet-in-the middle attack because of which it give a total security level of 2^112 instead of using 168 bits of key. The block collision attack can also be done because of short block size and using same key to encrypt a large size of text. It is also vulnerable to sweet32 attacks.



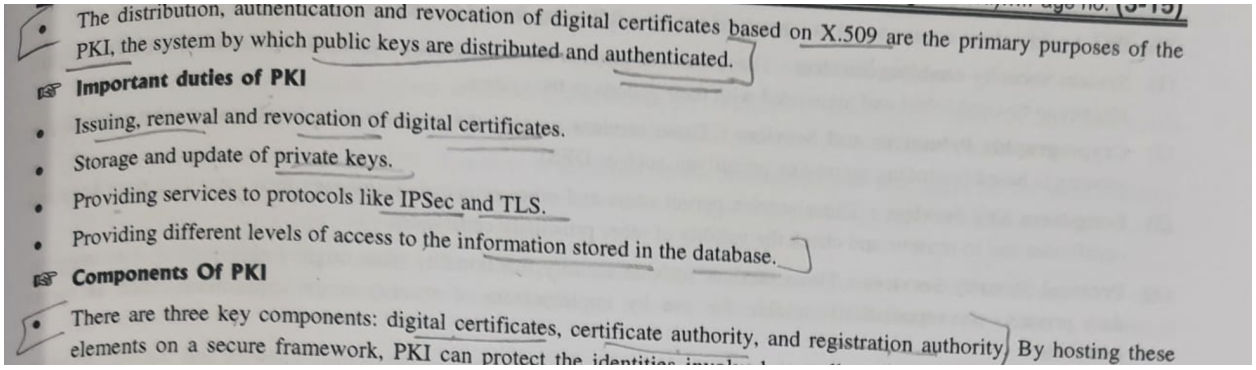
MODULE - 3

4. What is public key infrastructure in key generation? (Chpt 3)

Ans)



- **Public Key Infrastructure (PKI)** is the framework of encryption and cybersecurity that protects communications between the server (your website) and the client (the users).



- The distribution, authentication and revocation of digital certificates based on X.509 are the primary purposes of the PKI, the system by which public keys are distributed and authenticated.

☞ **Important duties of PKI**

- Issuing, renewal and revocation of digital certificates.
- Storage and update of private keys.
- Providing services to protocols like IPSec and TLS.
- Providing different levels of access to the information stored in the database.

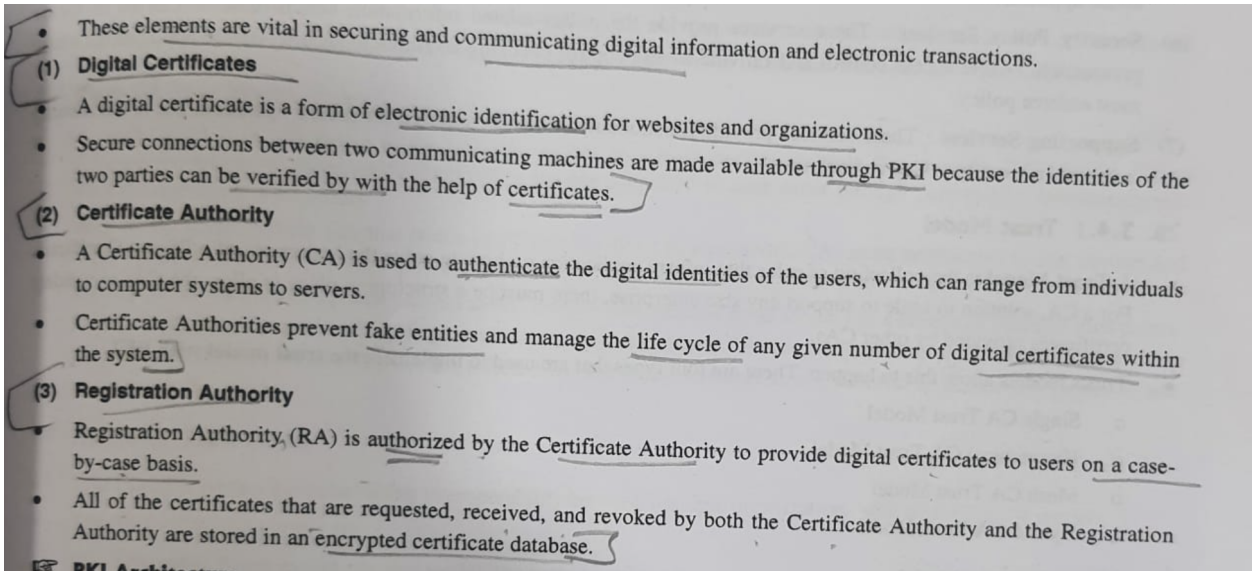
☞ **Components Of PKI**

- There are three key components: digital certificates, certificate authority, and registration authority. By hosting these elements on a secure framework, PKI can protect the identities

The public key infrastructure uses a pair of keys: the public key and the private key to achieve security. The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them.

Public key infrastructure affirms the usage of a public key. PKI identifies a public key along with its purpose. It usually consists of the following components:

- A digital certificate also called a public key certificate
- Private Key tokens
- Registration authority
- Certification authority
- CMS or Certification management system



- These elements are vital in securing and communicating digital information and electronic transactions.

(1) **Digital Certificates**

- A digital certificate is a form of electronic identification for websites and organizations.
- Secure connections between two communicating machines are made available through PKI because the identities of the two parties can be verified by with the help of certificates.

(2) **Certificate Authority**

- A Certificate Authority (CA) is used to authenticate the digital identities of the users, which can range from individuals to computer systems to servers.
- Certificate Authorities prevent fake entities and manage the life cycle of any given number of digital certificates within the system.

(3) **Registration Authority**

- Registration Authority (RA) is authorized by the Certificate Authority to provide digital certificates to users on a case-by-case basis.
- All of the certificates that are requested, received, and revoked by both the Certificate Authority and the Registration Authority are stored in an encrypted certificate database.

☞ **PKI Architecture**

Private Key Tokens

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

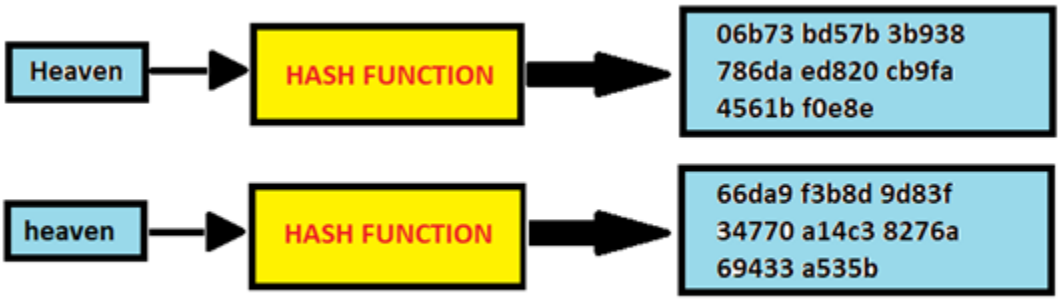
Certificate Management System (CMS)

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with an associated RA runs certificate management systems to be able to track their responsibilities and liabilities.
Different vendors often use different and sometimes proprietary storage formats for storing keys.

5. Working steps of SHA. (Chpt 3)

Ans) SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data and **certificates**. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions.

Hashing is similar to **encryption**, the only difference between hashing and encryption is that hashing is one-way, meaning once the data is hashed, the resulting hash digest cannot be cracked, unless a brute force attack is used. See the image below for the working of the SHA algorithm. SHA works in such a way even if a single character of the message changed, then it will generate a different hash. For example, hashing of two similar, but different messages i.e., Heaven and heaven is different. However, there is only a difference between a capital letter and a small letter.



This effect is important in cryptography, as it means even the slightest change in the input message completely changes the output. This will stop attackers from being able to understand what the hash digest originally said and telling the receiver of the message whether or not the message has been changed while in transit.

SECURE HASH ALGORITHM (SHA): (NIST) Process Block → Copy of C.V
→ 512 → 16 sub Blck
→ four Round (32)
(20 steps)

SHA is a modified version of MD5.

↳ o/p is a message digest of 160 bits in Length.

SHA Properties:-

(i) Generating original message from digest
(ii) finding two messages generating same digest } Infeasible.

(i) Padding is done such that total length is 64 bit less than exact multiple of 512.

1000 bits + 472 = 1472

512 × 2 = 1024

512 × 3 = 1536

64 bit less than exact multiple of 512.

(ii) Append original length bef. padding (modulo 64)

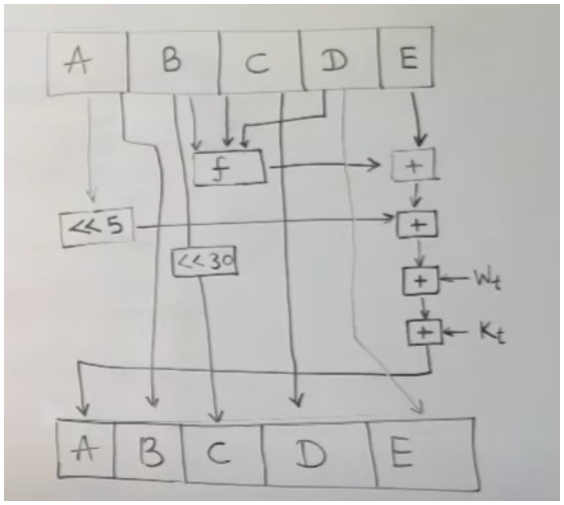
1000] length mod 2^{64}.

(iii) Divide it in 512-bit blocks.

~~(iv)~~ Five chaining Variables (A, B, C, D, E)

(V) Process Blocks.

$$abcde = (e + \text{Process P} + s^5(a) + W[t] + K[t]), a, s^{30}(b), c, d.$$



DIFF : Message digest in SHA is 160 bit in length whereas in MD5 it is 128 bit.

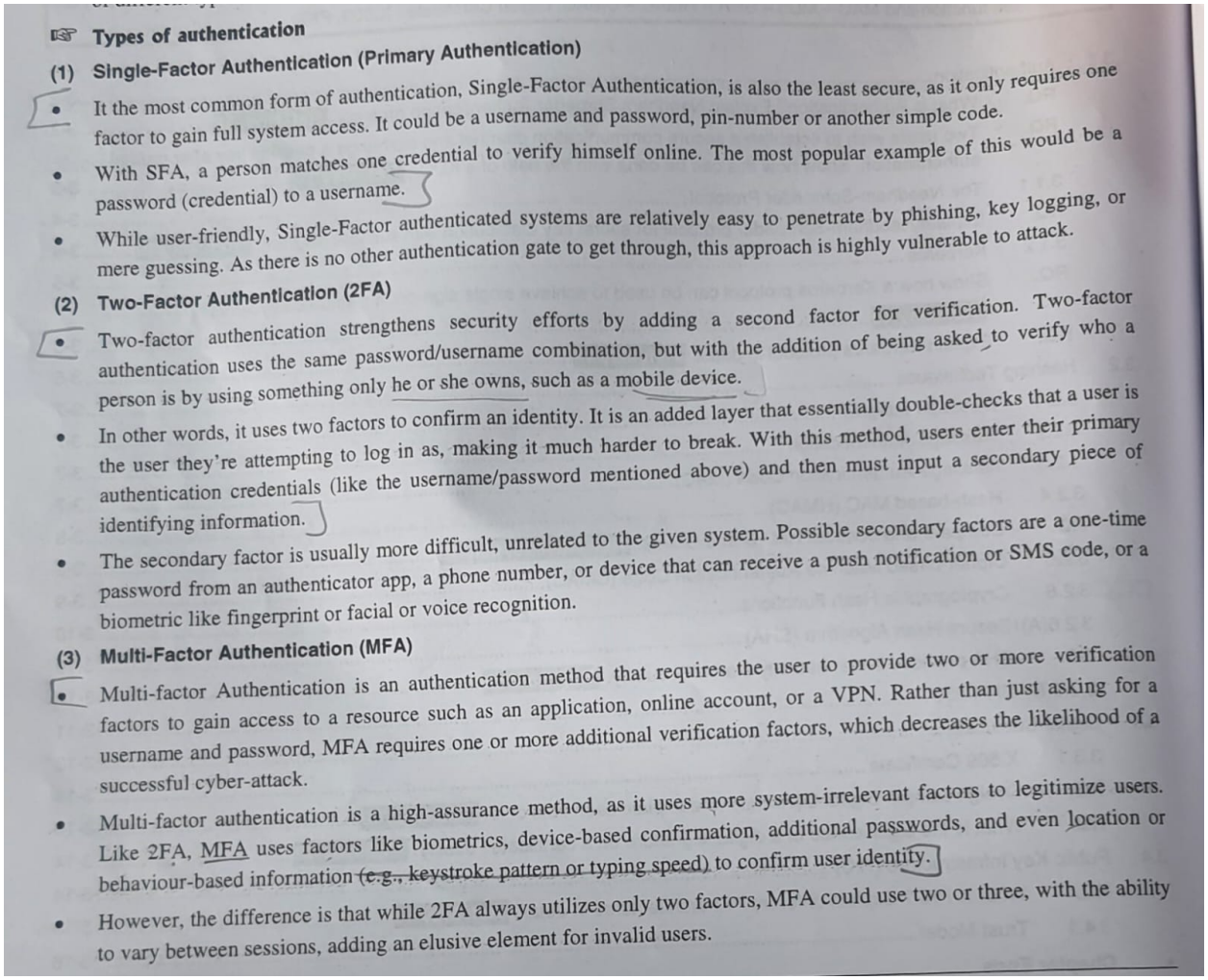
Character variables in SHA are A,B,C,D,E whereas in MD5 it is A,B,C,D.

6. What is authentication? Define its types. (Chpt 3)

Ans) Data is prone to various attacks. One of these attacks includes message authentication. This threat arises when the user does not have any information about the originator of the message. Message authentication can be achieved using cryptographic methods which further make use of keys.

Message authentication is a procedure to verify that received messages come from the alleged source and have not been altered. Message authentication may also verify sequencing and timeliness. A digital signature is an authentication technique that also includes measures to counter repudiation by either source or destination.

Types of Authentication:



☞ **Types of authentication**

(1) Single-Factor Authentication (Primary Authentication)

- It the most common form of authentication, Single-Factor Authentication, is also the least secure, as it only requires one factor to gain full system access. It could be a username and password, pin-number or another simple code.
- With SFA, a person matches one credential to verify himself online. The most popular example of this would be a password (credential) to a username.
- While user-friendly, Single-Factor authenticated systems are relatively easy to penetrate by phishing, key logging, or mere guessing. As there is no other authentication gate to get through, this approach is highly vulnerable to attack.

(2) Two-Factor Authentication (2FA)

- Two-factor authentication strengthens security efforts by adding a second factor for verification. Two-factor authentication uses the same password/username combination, but with the addition of being asked to verify who a person is by using something only he or she owns, such as a mobile device.
- In other words, it uses two factors to confirm an identity. It is an added layer that essentially double-checks that a user is the user they're attempting to log in as, making it much harder to break. With this method, users enter their primary authentication credentials (like the username/password mentioned above) and then must input a secondary piece of identifying information.
- The secondary factor is usually more difficult, unrelated to the given system. Possible secondary factors are a one-time password from an authenticator app, a phone number, or device that can receive a push notification or SMS code, or a biometric like fingerprint or facial or voice recognition.

(3) Multi-Factor Authentication (MFA)

- Multi-factor Authentication is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.
- Multi-factor authentication is a high-assurance method, as it uses more system-irrelevant factors to legitimize users. Like 2FA, MFA uses factors like biometrics, device-based confirmation, additional passwords, and even location or behaviour-based information (e.g., keystroke pattern or typing speed) to confirm user identity.
- However, the difference is that while 2FA always utilizes only two factors, MFA could use two or three, with the ability to vary between sessions, adding an elusive element for invalid users.

Authentication Requirements:

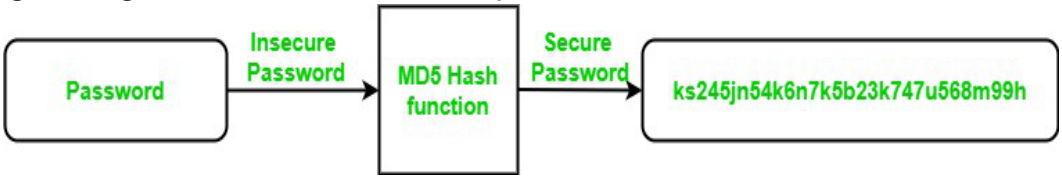
- **Revelation:** It means releasing the content of the message to someone who does not have an appropriate cryptographic key.
- **Analysis of Traffic:** Determination of the pattern of traffic through the duration of connection and frequency of connections between different parties.
- **Deception:** Adding out of context messages from a fraudulent source into a communication network. This will lead to mistrust between the parties communicating and may also cause loss of critical data.
- **Modification in the Content:** Changing the content of a message. This includes inserting new information or deleting/changing the existing one.
- **Modification in the sequence:** Changing the order of messages between parties. This includes insertion, deletion, and reordering of messages.
- **Modification in the Timings:** This includes replay and delay of messages sent between different parties. This way session tracking is also disrupted.
- **Source Refusal:** When the source denies being the originator of a message.
- **Destination refusal:** When the receiver of the message denies the reception.

10. What is working steps of MD5 hashing algo?(Chpt 3)

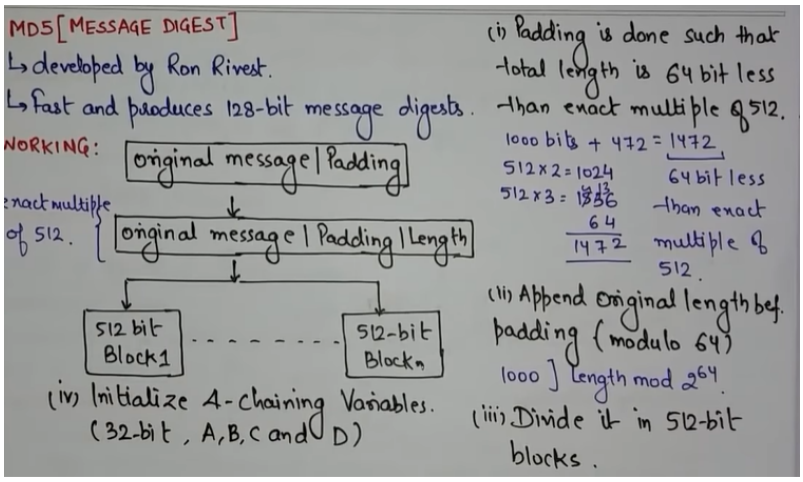
Ans)**MD5** is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the **message-digest algorithm**. MD5 was developed as an improvement of MD4, with advanced security purposes. The output of MD5 (Digest size) is always **128 bits.** **MD5** was developed in 1991 by **Ronald Rivest.**

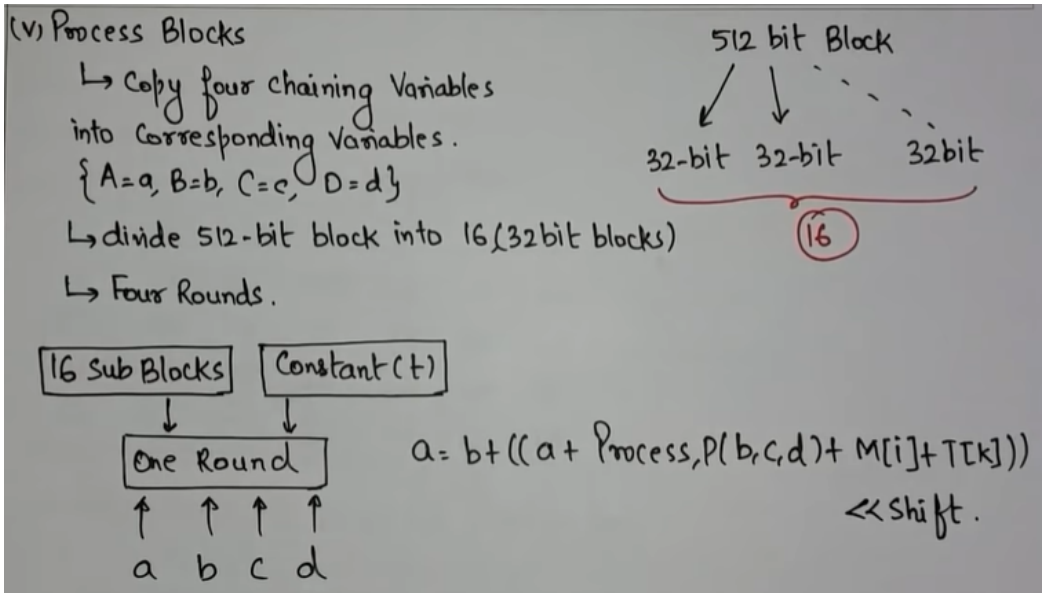
Use Of MD5 Algorithm:

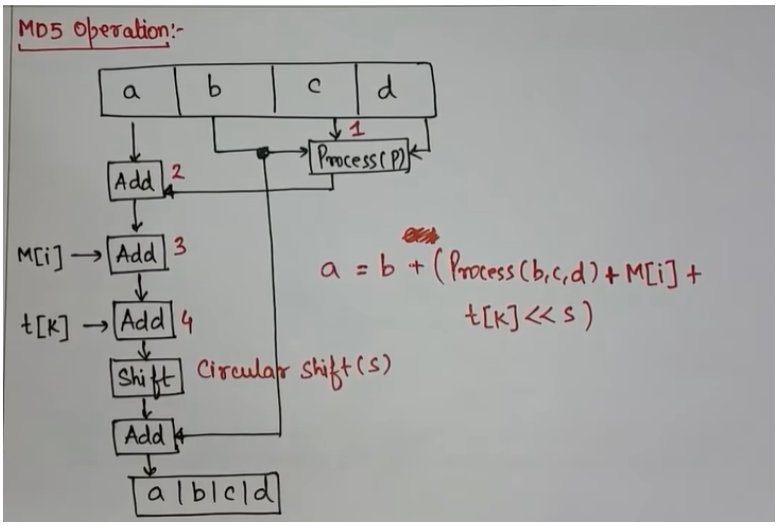
- It is used for file authentication.
- In a web application, it is used for security purposes. e.g. Secure password of users etc.
- Using this algorithm, We can store our password in 128 bits format.



Working of the MD5 Algorithm:







11. Explain MAC in authentication function. (Chpt 3)

Ans)Message Authentication Code (MAC)

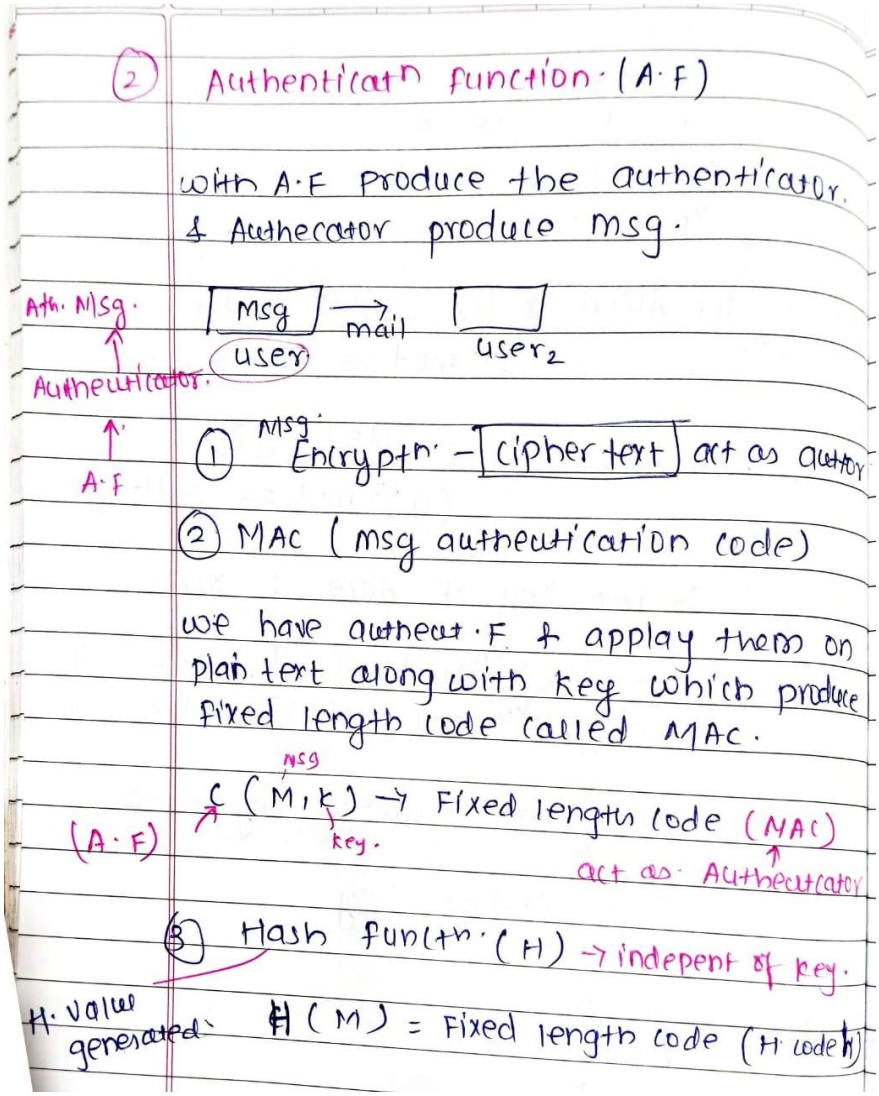
MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.

Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

Limitations of MAC

There are two major limitations of MAC, both due to its symmetric nature of operation −

- Establishment of Shared Secret.
    - It can provide message authentication among pre-decided legitimate users who have shared key.
    - This requires establishment of shared secret prior to use of MAC.
- Inability to Provide Non-Repudiation
    - Non-repudiation is the assurance that a message originator cannot deny any previously sent messages and commitments or actions.
    - MAC technique does not provide a non-repudiation service. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender.
    - Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.



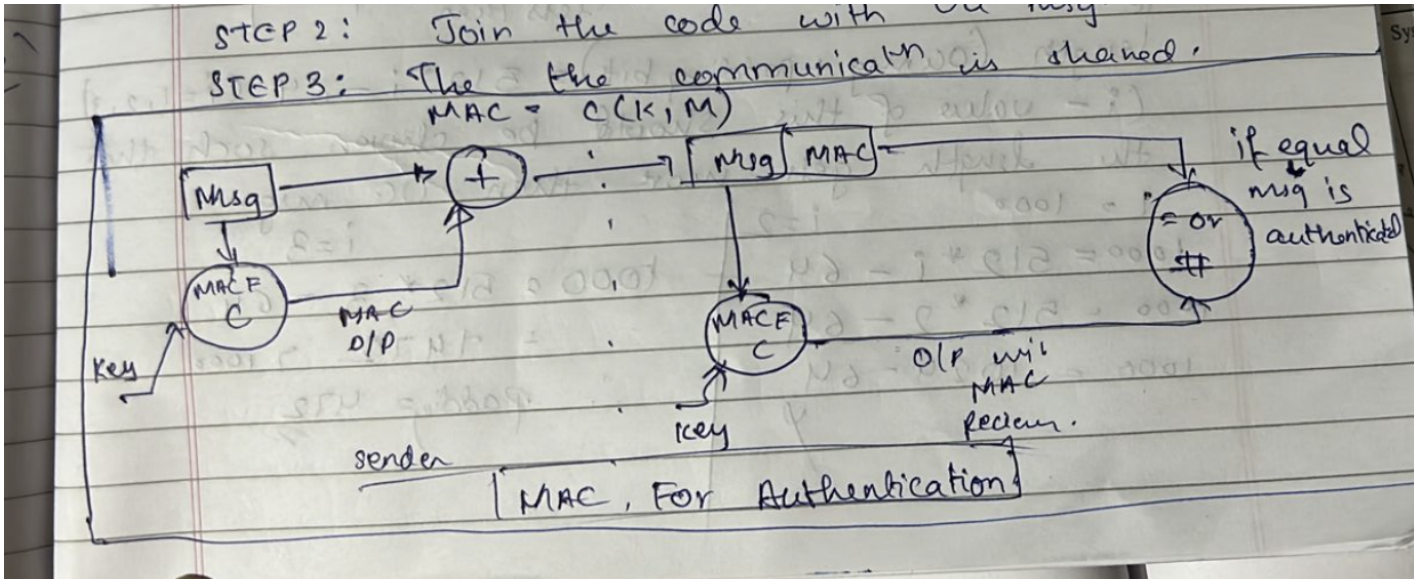
Authentication function in cryptography and system security is used to ensure that the communication between two parties is secure and authentic.

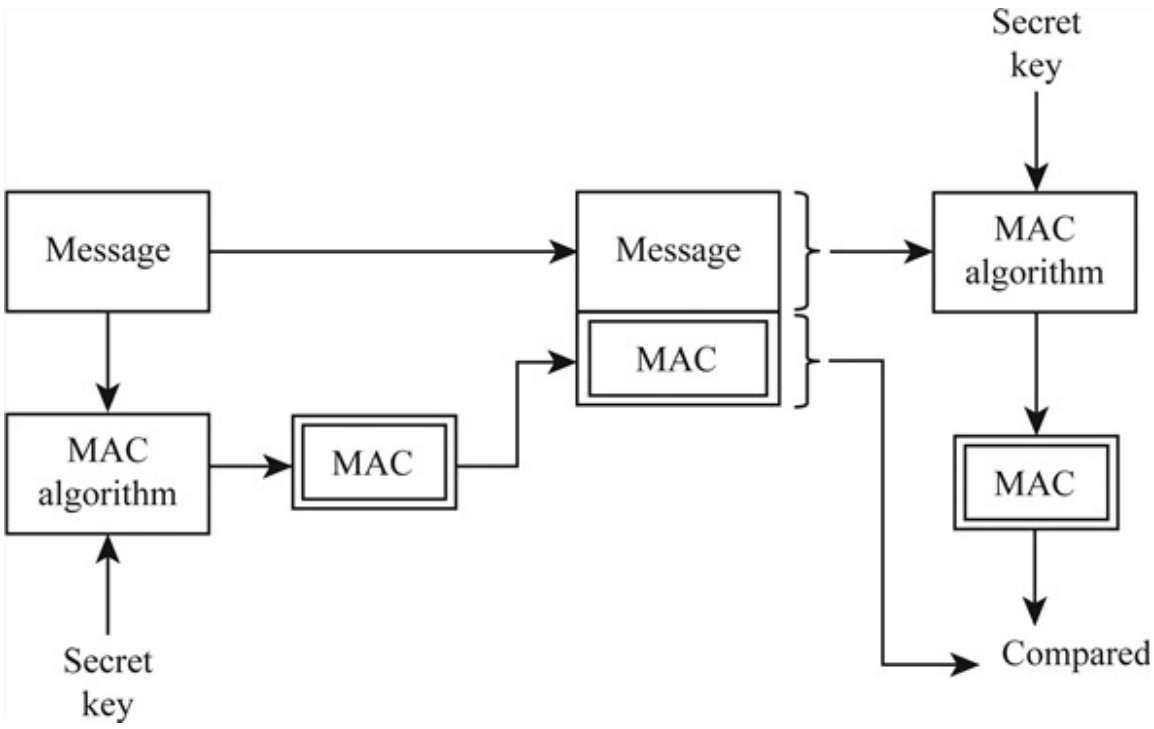
In cryptography, an authentication function is used to verify the identity of the sender and receiver of a message. It is also used to ensure that the message has not been tampered with or altered during transmission. The authentication function can be achieved through the use of digital signatures, message authentication codes (MACs), or hash functions.

Digital signatures are cryptographic techniques that use public-key cryptography to provide authentication and integrity of a message. A digital signature is a unique digital code that is attached to a message, which can be verified by the recipient using the sender's public key. The digital signature ensures that the message has not been tampered with and is authentic.

Message authentication codes (MACs) are cryptographic techniques that use a secret key to generate a code that is attached to the message. The recipient uses the same secret key to verify the code and ensure that the message has not been tampered with.

Hash functions are used to ensure the integrity of the message by generating a fixed-size message digest, which is a unique code that is calculated from the message. Any alteration in the message will result in a different message digest, which can be detected by the recipient.





EXTRA:
Q.KERBEROS:
Ans)

- **Kerberos** is a computer network security protocol that authenticates service requests between two or more trusted users across the internet. It uses **secret-key cryptography** and a trusted third party (KDC) for authenticating client-server applications and verifying users' identities.
- Kerberos was initially developed by the Mi...

Key Distribution center

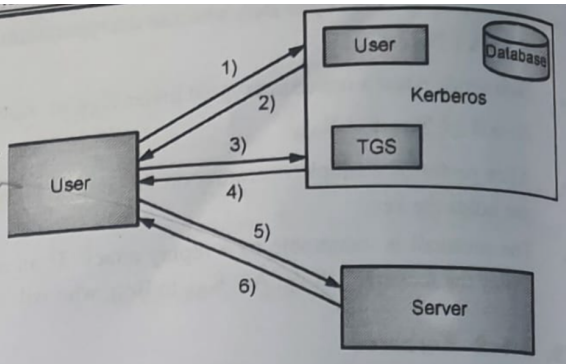
- Users, machines, and services that use Kerberos depend on the KDC alone, which works as a single process that provides two functions: **authentication** and **ticket-granting**. KDC **tickets** offer authentication to all parties, allowing users to verify their identity securely.

☞ **Components of Kerberos**

- **Client (user) :** The client initiates communication for a service request.
- **Server :** The server hosts the service the user wants to access.
- **Authentication Server (AS) :** The AS performs the desired client authentication. If the authentication happens successfully, the AS issues the client a ticket called TGT (Ticket Granting Ticket). This ticket assures the other servers that the client is authenticated.
- **Key Distribution Center (KDC) :** In a Kerberos environment, the authentication server logically separated into three parts: A database (db), the Authentication Server (AS), and the Ticket Granting Server (TGS). These three parts, in turn, exist in a single server called the Key Distribution Center.
- **Ticket Granting Server (TGS) :** The TGS is an application server that issues the ticket for the server.

☞ **Secret Keys**

- There are three vital secret keys involved in the Kerberos flow. There are unique secret keys for the client, the TGS, and the server shared with the AS.
  - Client/user - Hash derived from the user's password.
  - TGS secret key - Hash of the password used in determining the TGS.
  - Server secret key - Hash of the password used to determine the server providing the service.



(1B49)**Fig. 3.1.2 : Overview of Kerberos**

Q. properties of the Hash function? Explain the role of hash functions in security.
Ans) The properties of hash functions that make them useful in security applications are:

1. **Deterministic:** Hash functions always produce the same output for the same input. This property is essential in verifying the integrity of data and detecting any changes in the input data.
2. **Collision-resistant:** It is computationally infeasible to find two different inputs that produce the same hash value. This property ensures that hash functions are used to prevent unauthorized modification of data, ensure message integrity, and verify data authenticity.

3. **One-way:** It is computationally infeasible to derive the original input data from the hash value. This property is essential in protecting passwords, digital signatures, and other confidential data.
4. **Quick to compute:** Hash functions are designed to be computationally efficient and quick to compute. This property makes them suitable for use in applications that require fast processing, such as digital signatures, message authentication codes, and password protection.

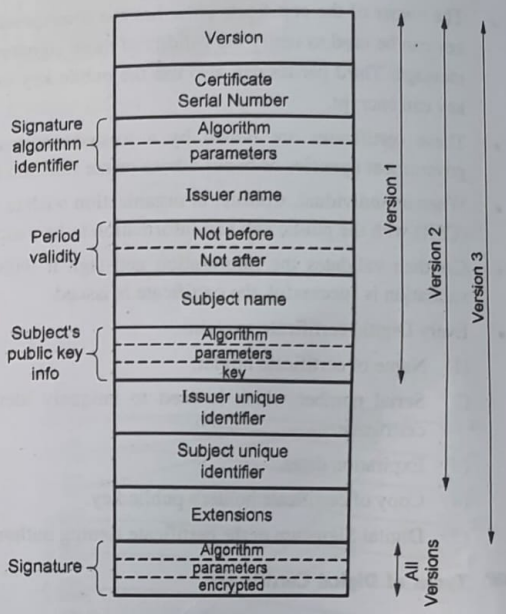
The role of hash functions in security is crucial. Hash functions are used in a wide range of security applications, including:

1. **Password protection:** Hash functions are used to protect passwords by storing only the hash value of the password instead of the actual password. When a user logs in, the system computes the hash value of the entered password and compares it to the stored hash value to verify the authenticity of the user.
2. **Message integrity:** Hash functions are used to ensure the integrity of messages transmitted over untrusted networks. The sender computes the hash value of the message and sends it along with the message. The receiver then computes the hash value of the received message and compares it with the sent hash value to verify the authenticity and integrity of the message.
3. **Digital signatures:** Hash functions are used in digital signature schemes to ensure the authenticity and integrity of the signed data. The sender computes the hash value of the data, signs the hash value using their private key, and sends the signed hash value along with the data. The receiver verifies the signature by computing the hash value of the received data, verifying the signature using the sender's public key, and comparing the computed hash value with the received signed hash value.

Q. X.509 Certificate:

RQ. What is the significance of a digital signature on a certificate?

- **X.509** is a standard format for public key certificates, digital documents to verify that a public key belongs to the user, computer or service identity contained within the certificate. X.509 has been adapted for internet use by the IETF's Public-Key Infrastructure (X.509) (PKIX) working group.
- Common fields in X.509 certificates are:
  - **(1) Version number** : This field defines which X.509 version applies to the certificate. The version number started at 0 and currently it is version 2.
  - **(2) Serial number** : This field defines serial number assigned to the certificate that distinguishes it from other certificates.
  - **(3) Signature Algorithm information** : This field identifies the algorithm used by the issuer to sign the certificate.
  - **(4) Issuer name** : This filed defines the name of the entity issuing the certificate (usually a certificate authority).
  - **(5) Validity period of the certificate :** This filed defines start/end date and time the certificate is valid.
  - **(6) Subject name :** This field defines the name of the identity the certificate is issued to, the entity to which the public key belongs.
  - **(7) Subject public key information :** This field defines the public key associated with the identity (heart of the certificate) as well as the corresponding algorithm.



(1B50)Fig. 3.3.1 : Format of X.509 Digital Certificate

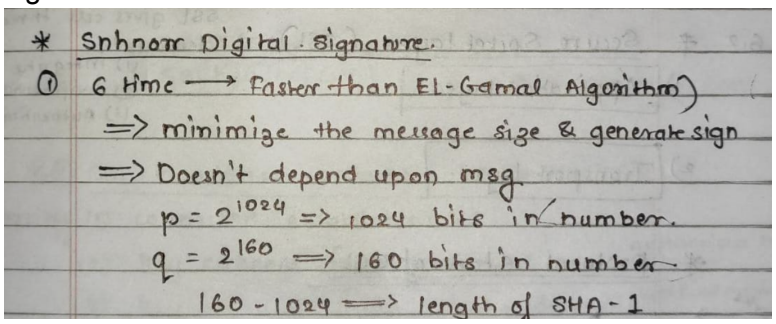
- **(8) Issuer unique identifier :** This is an optional field which allows two issuers to have same issuer field value.
- **(9) Subject unique identifier :** This is an optional field which allows two subjects to have same subject field value.
- **(10) Extensions :** This is an optional field which allows issuers to add more private information to the certificate.
- **(11) Signature** : This field is comprised of three sub-fields: algorithms, parameters and encrypted.
- Every certificate can be renewed after period of validity. The CA generally issues a new certificate if there is no problem, before the old certificate expires.

MODULE 4

1. What are the steps of Schorr Digital Signature?

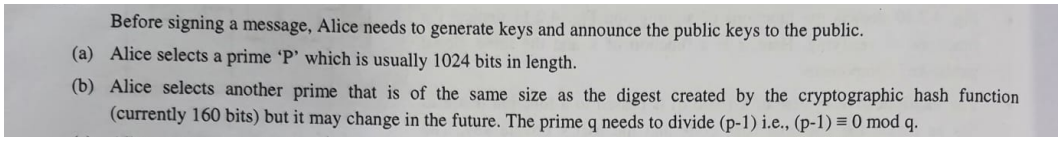
Ans)

It is a digital signature scheme known for its simplicity, and efficiency and generates short signatures.



The steps of Schorr Digital Signature are as follows:

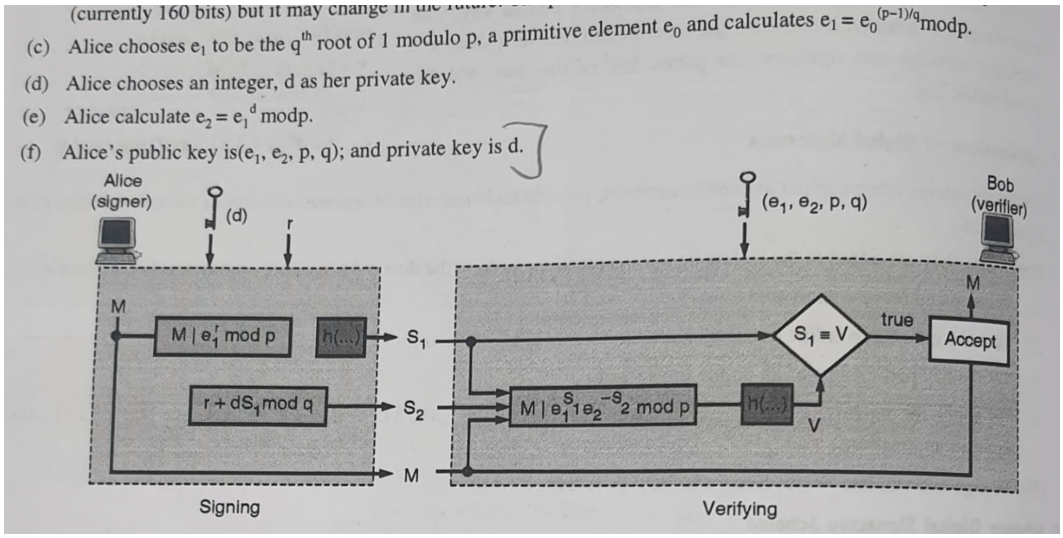
1. Key Generation:



Before signing a message, Alice needs to generate keys and announce the public keys to the public.

(a) Alice selects a prime 'P' which is usually 1024 bits in length.

(b) Alice selects another prime that is of the same size as the digest created by the cryptographic hash function (currently 160 bits) but it may change in the future. The prime q needs to divide (p-1) i.e., (p-1) ≡ 0 mod q.



(currently 160 bits) but it may change in the future.

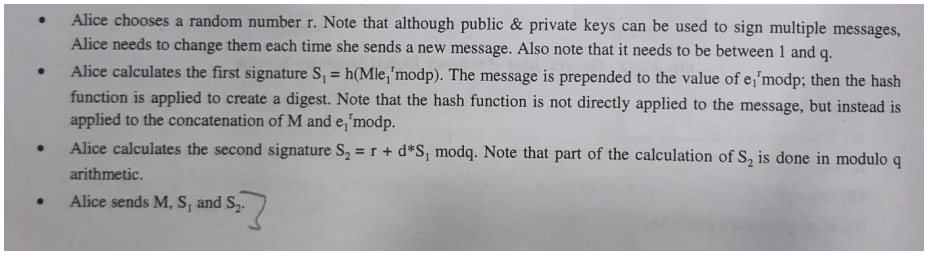
(c) Alice chooses e_1 to be the q^{th} root of 1 modulo p, a primitive element e_0 and calculates $e_1 = e_0^{(p-1)/q} \bmod p$.

(d) Alice chooses an integer, d as her private key.

(e) Alice calculate $e_2 = e_1^{d} \bmod p$.

(f) Alice's public key is(e_1, e_2, p, q); and private key is d.

2. Signing:



- Alice chooses a random number r. Note that although public & private keys can be used to sign multiple messages, Alice needs to change them each time she sends a new message. Also note that it needs to be between 1 and q.
- Alice calculates the first signature $S_1 = h(M|e_1^r \bmod p)$. The message is prepended to the value of $e_1^r \bmod p$; then the hash function is applied to create a digest. Note that the hash function is not directly applied to the message, but instead is applied to the concatenation of M and $e_1^r \bmod p$.
- Alice calculates the second signature $S_2 = r + d*S_1 \bmod q$. Note that part of the calculation of S_2 is done in modulo q arithmetic.
- Alice sends M, S_1 and S_2.

Where,

M : message, r: Random secret, | : concatenation

S_1, S_2 : Signature, d: Alice's Private key, h(…) hash algorithm.

V : verification

(e_1, e_2, p, q) : Alices public key

3. Verifying Message:

- Assume that the receiver Bob, receives M, S_1 and S_2.
- Bob calculates $V = h(M|e_1^{S_2} e_2^{-S_1} \bmod p)$

If S_1 is congruent to V modulo p, the message is accepted otherwise rejected.

2. Write the Working process of El Gamal algorithm.

Ans)

2. ElGamal Digital Signature Scheme (1B43)**Fig. 4.2.7 : Verification**

- The **ElGamal digital signature scheme** stems from the ElGamal cryptosystem based upon the security of the one-way function of exponentiation in modular rings and the difficulty of solving the discrete logarithm problem.
- The ElGamal encryption scheme is designed to enable encryption by a receiver's public key and decryption by the receiver's private key.
- The ElGamal signature scheme involves the use of the private key of sender for encryption and the public key of sender for decryption. This scheme uses the same keys but the algorithm is different. The algorithm creates two digital signatures, these two signatures, are used in the verification phase.

* EL. Gamal ⟶ Digital Signature.

(1) Select prime no. q

(2) Select primitive root α

(3) Generate Random integer X_A

$1 < X_A < q-1$

(4) Find $y_A = \alpha^{X_A} \bmod q$

(5) Find key for user A

Private key = X_A ⟹ Decryption.

Public key = $\{q, \alpha, y_A\}$ = Encryption.

(6) Find hash code (M|h) for PT

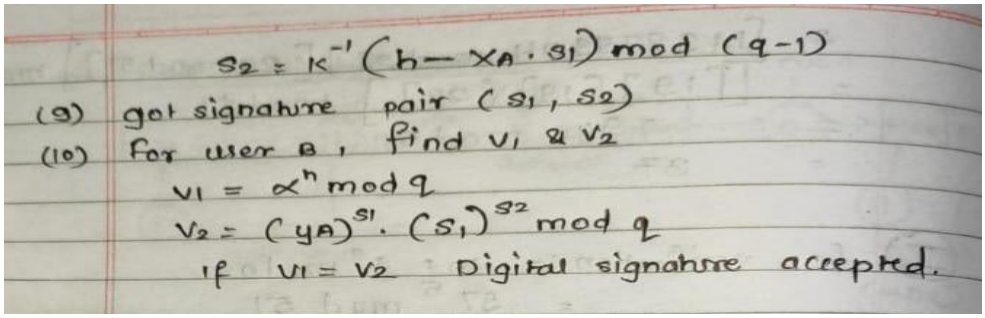
$h = H(M)$ ∴ $(h = 0 \leq h \leq q-1)$

(7) find Random integer K

$1 \leq K \leq q-1$ & $GCD(K, q-1) = 1$

(8) find S_1 & S_2

$S_1 = \alpha^K \bmod q$



7. What are the steps of RSA Digital Signature?

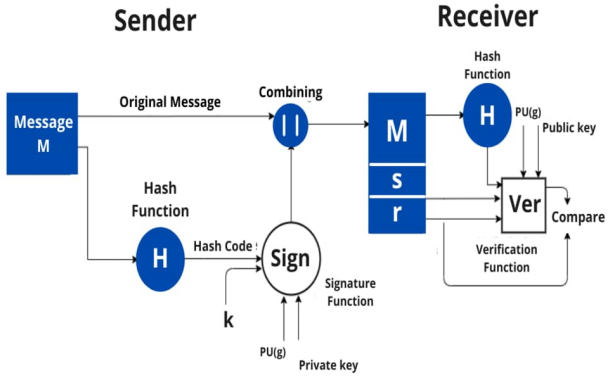
Ans)

- Select two large prime numbers, p and q.
- Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.
- φ (n) = (p - 1) x (q -1)
- Choose a number e less than n, such that n is relatively prime to φ (n). It means that e and have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), gcd (e,φ(n)) =1
- d = e^-1 mod n
- Public key is <e, n>.
  Private key is <d, n>
- Signing: $s = m^d \bmod n$
- Verification : $m = s^e \bmod n$

8. Define what is meant by Digital Signature with its process.

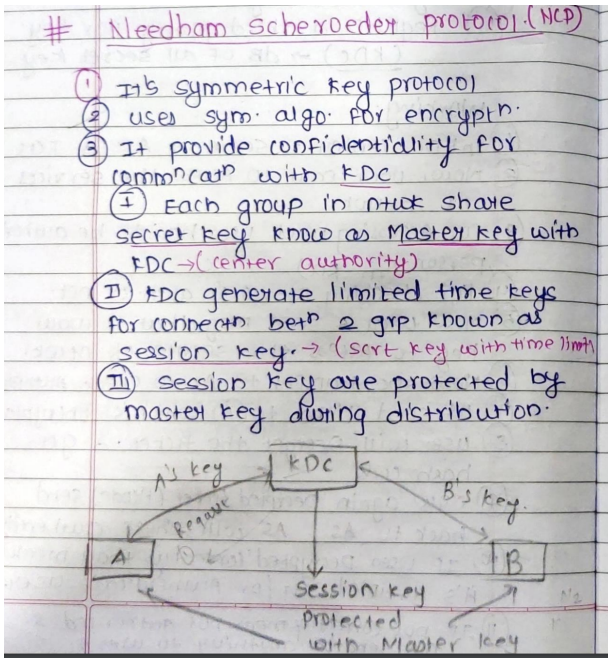
Ans)

Digital Signature is a way to validate the authenticity and integrity of the message or digital or electronic documents. Authenticity means to verify the identity of the sender and integrity means to check that the data or message should not be altered during the transmission.



A hash code is generated from the message and given as input to the signature function on the sender side. The other inputs to a signature function include a unique random number k for the signature, the private key of sender PR(a), and the global public key i.e., PU(g).
The output of the signature function consists of two components: s & r, which are concatenated with the input message and then sent to the receiver.
Signature = {s, r}.
On the receiver side, the hash code for the message sent is generated by the receiver by applying a hash function. The verification function is used for verifying the message and signature sent by the sender. The verification function takes the hash code generated, signature components s and r, the public key of the sender (PU(a)), and the global public key.
The signature function is compared with the output of the verification function and if both the values match, the signature is valid because A valid signature can only be generated by the sender using its private key.

Q.Needham Schroeder Protocol:



Working.

1. User A want to comm^n to user B.
2. It send a Request msg to KDC
   KDC is db of all user secret key. it store all secret key.
3. $A \rightarrow KDC : ID_A \| ID_B \| N_1$

A send KDC with

ID_A = User A identificatn, ID_B = for B

N = Nounce ⇒ some simple msg.

K_s = Session key,

K_A ⇒ Master key of A, K_B = for B (Mstr)
(secret key)

2. $KDC \rightarrow A : E(K_a, [K_s \| ID_B \| N_1] \| E(K_b, [K_s \| ID_A])$

Now KDC send Reply User A with Session key i.e Master key of A & B i.e K_a & K_B which is in encrypted

User A ~~Encrypt~~ Decrypt the msg with Master key & get session key (K_S), ID_B & N_1

Blw part

But it can't decrpt the 2nd part. ( )
Becoz it's encrypted with Master key of B & user don't have Master key (sect k.g)

3. $A \rightarrow B : E(K_b, [K_s \| ID_A])$

Now user A send Encrpid part of B to B.
B will decrpt with Master key and get session key & identificatn of A.

4. $B \rightarrow A : E(K_s, N_2)$

Now Authectn acheived, so B send to A encrypted session key & Nouch B

nouch B ⇒ N_2 which is created by User B.

5. $A \rightarrow B : E(K_s, f(N_2))$

Now User A Reply the Nounce using the session key (secret key) in Encrypted formate.
& User B get decrpt that Replay of Nonce (N_2).

MODULE - 5

6. What is meant by the Multilevel Security Model in System Security.

Ans) The Multilevel Security Model (MLS) is a security model that allows for the protection of sensitive information by controlling access to it based on the security clearance level of the user. It is commonly used in environments where multiple users with different levels of clearance need to access the same system, such as government or military organizations.

In the MLS model, information is classified into different levels, each of which is associated with a specific level of clearance. Access to information at a particular security level is granted only to users with an equal or higher level of clearance. This ensures that sensitive information is only accessible to authorized personnel.

To ensure the confidentiality, integrity, and availability of information, the MLS model employs various security mechanisms.

Authentication is used to verify the identity of users and ensure that only authorized users can access the system. Authorization controls are used to determine what actions a user is allowed to perform on the system, based on their security clearance level.

Encryption is used to protect data at rest and in transit, so that even if it is intercepted by an unauthorized party, it cannot be read.

The MLS model also uses techniques such as mandatory access control (MAC) and discretionary access control (DAC) to provide an additional layer of security. MAC is a security mechanism that enforces a strict set of rules regarding which users can access specific resources, based on their security clearance level. DAC, on the other hand, allows users to determine who can access resources they own, and to what extent.

12. What is Inference Attacks in System Security.

Ans)

Inference attacks are a type of attack in system security that involves extracting sensitive information from a system by analyzing the patterns in non-sensitive data. A real-world example of an inference attack is as follows:

Let's say that a healthcare organization has a database of patient records that includes their medical histories, diagnoses, and treatments. The database is encrypted to ensure the confidentiality of the data. However, the organization also provides researchers with access to some non-sensitive data, such as demographic information, without encryption.

An attacker who gains access to this non-sensitive data could use statistical analysis techniques to infer sensitive information about individual patients. For example, they could use clustering algorithms to group patients based on their age, gender, and zip code. By analyzing the medical histories of the patients in each cluster, the attacker could infer information about the prevalence of certain diseases in each group. This could reveal sensitive information about individual patients, such as their medical conditions, without directly accessing the encrypted data.

In this example, the attacker is able to use non-sensitive data to infer sensitive information about the patients, highlighting the need for organizations to carefully manage and protect all data, even if it is not directly sensitive.

To protect against inference attacks, there are several ways to ensure that sensitive information is not inadvertently disclosed:

1. Data anonymization: The organization can remove or encrypt all identifying information from the non-sensitive data, such as names, addresses, or social security numbers. This can prevent attackers from being able to link non-sensitive data to sensitive data.
2. Differential privacy: This technique involves adding noise or random data to the non-sensitive data before releasing it to researchers. This makes it more difficult for attackers to identify individual records.
3. Access control: Limiting access to the non-sensitive data can prevent unauthorized users from being able to use it to infer sensitive information.
4. Data segmentation: The organization can segment the data into different subsets, with different access levels based on the sensitivity of the data. This can limit the amount of non-sensitive data that is accessible to any individual user.
5. Regular monitoring: The organization can regularly monitor access to the non-sensitive data, and analyze patterns of access to identify any potential inference attacks.

13. How Multilevel Database Security will work in Web Security. Illustrate with diagrams and examples. (NOT SURE)

Ans) Multilevel database security is an approach to database security that provides different levels of access to data based on the user's security clearance level. This approach is commonly used in government and military applications where access to sensitive information must be restricted based on the user's security clearance level. In web security, multilevel database security can be implemented by using various security mechanisms such as access control, authentication, and encryption.

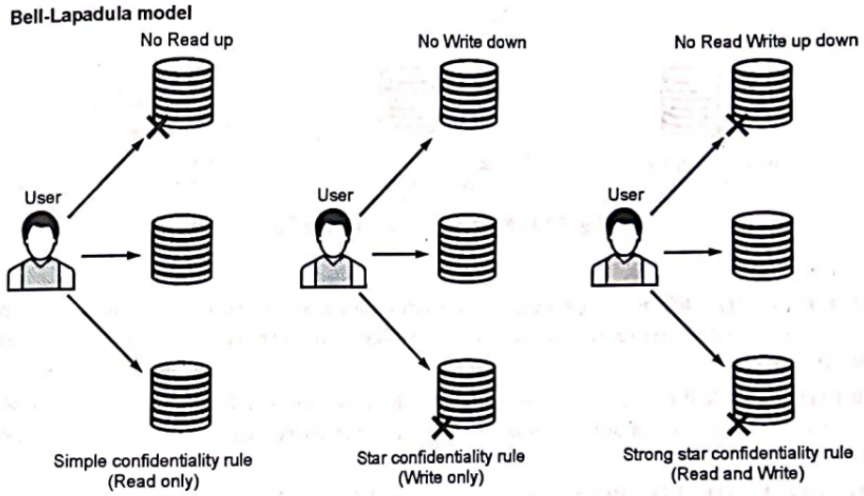


Fig. 5.2.2 : No Read Up, No Write Down

It has mainly 3 Rules :

- **SIMPLE CONFIDENTIALITY RULE :** Simple Confidentiality Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as **NO READ-UP.**

- **STAR CONFIDENTIALITY RULE :** Star Confidentiality Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as **NO WRITE-DOWN**
- **STRONG STAR CONFIDENTIALITY RULE :** Strong Star Confidentiality Rule is highly secured and strongest which states that the Subject can Read and Write the files on the Same Layer of Secrecy only and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which we call this rule as **NO READ WRITE UP DOWN**

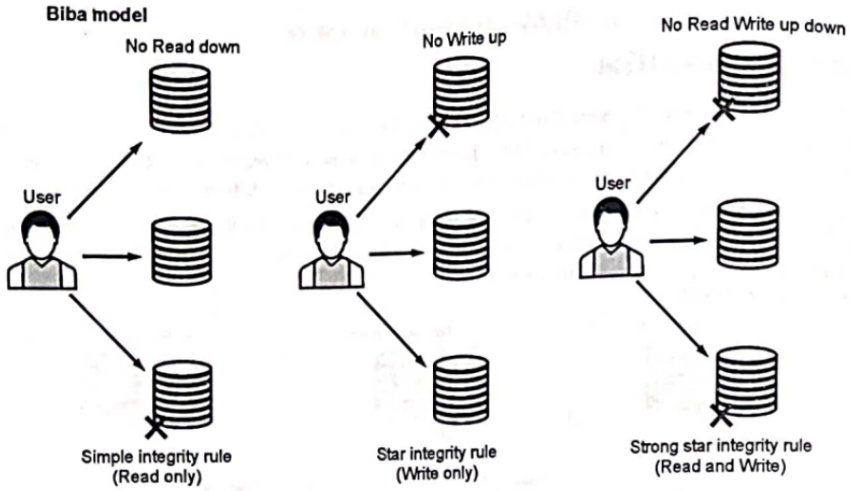


Fig. 5.2.3 : No Read Down, No Write Up

It has mainly 3 Rules :

- **SIMPLE INTEGRITY RULE :** Simple Integrity Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as **NO READ DOWN**
- **STAR INTEGRITY RULE :** Star Integrity Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as **NO WRITE-UP**
- **STRONG STAR INTEGRITY RULE :** Strong Star Integrity Rule is highly secured and strongest which states that the Subject can Read and Write the files on the Same Layer of Secrecy only and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which we call this rule as **NO READ WRITE UP DOWN**

Examples of multilevel database security in web applications include:

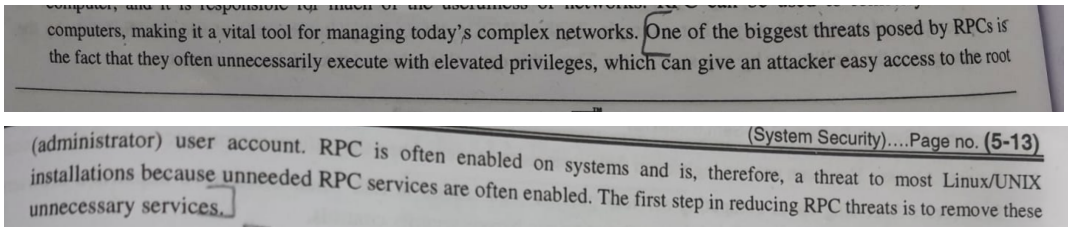
1. Military or government applications: In these applications, different security clearance levels are assigned to users based on their role and responsibilities. For example, a low-level security clearance user may be a soldier, while a high-level security clearance user may be a general. Access to sensitive information is restricted based on the user's security clearance level.
2. Healthcare applications: In these applications, access to patient records is restricted based on the user's role and responsibilities. For example, a nurse may have access to patient records but not be allowed to modify them, while a doctor may have full access to the patient records and be allowed to modify them.

Overall, the multilevel database security approach provides a comprehensive and effective method for ensuring that sensitive data is protected from unauthorized access or modification.

14. Illustrate Vulnerability in Linux and Windows Operating systems. Also, Explain File System Security with examples.

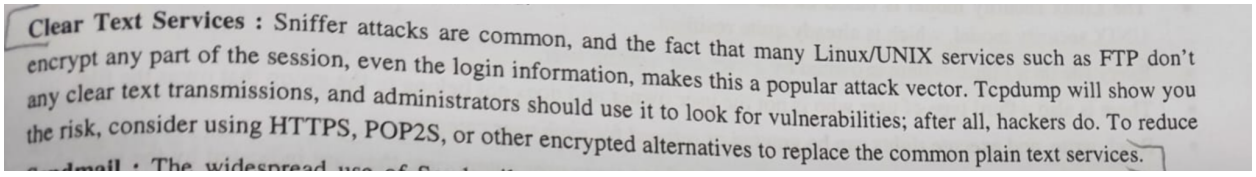
Ans) Vulnerability in linux are as follows:

1. Remote Procedure Call:

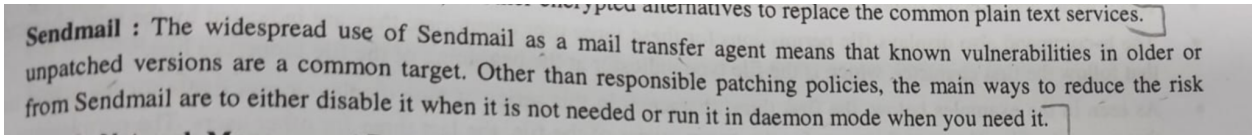

computers, making it a vital tool for managing today's complex networks. One of the biggest threats posed by RPCs is the fact that they often unnecessarily execute with elevated privileges, which can give an attacker easy access to the root

(administrator) user account. RPC is often enabled on systems and is, therefore, a threat to most Linux/UNIX installations because unneeded RPC services are often enabled. The first step in reducing RPC threats is to remove these unnecessary services.

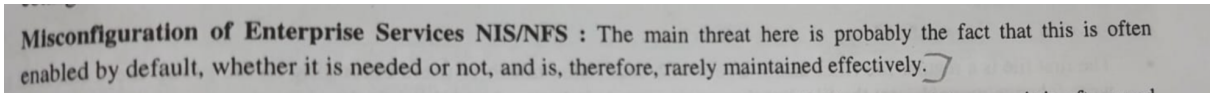
2. Clear Text Services:


Clear Text Services : Sniffer attacks are common, and the fact that many Linux/UNIX services such as FTP don't encrypt any part of the session, even the login information, makes this a popular attack vector. Tcpdump will show you any clear text transmissions, and administrators should use it to look for vulnerabilities; after all, hackers do. To reduce the risk, consider using HTTPS, POP2S, or other encrypted alternatives to replace the common plain text services.

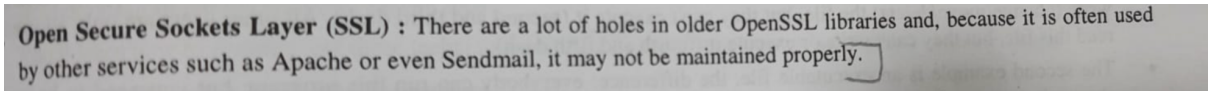
3. Sendmail:

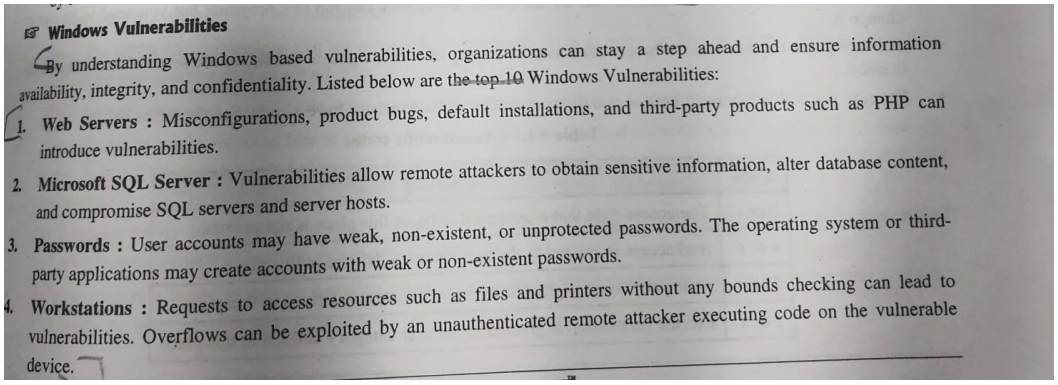

Sendmail : The widespread use of Sendmail as a mail transfer agent means that known vulnerabilities in older or unpatched versions are a common target. Other than responsible patching policies, the main ways to reduce the risk from Sendmail are to either disable it when it is not needed or run it in daemon mode when you need it.

4. Misconfiguration of Enterprise Services NIS/NFS:


Misconfiguration of Enterprise Services NIS/NFS : The main threat here is probably the fact that this is often enabled by default, whether it is needed or not, and is, therefore, rarely maintained effectively.

5. Open Secure Sockets Layer (SSL):

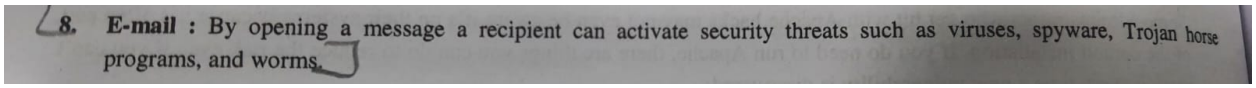

Open Secure Sockets Layer (SSL) : There are a lot of holes in older OpenSSL libraries and, because it is often used by other services such as Apache or even Sendmail, it may not be maintained properly.



☞ **Windows Vulnerabilities**

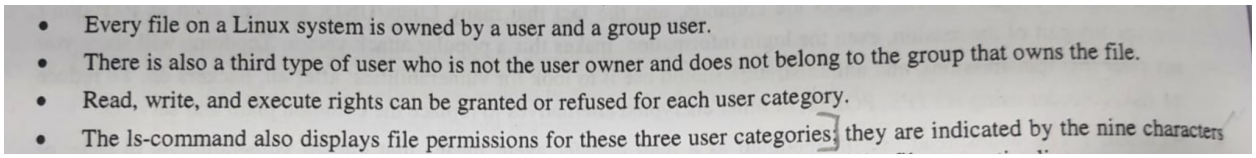
By understanding Windows based vulnerabilities, organizations can stay a step ahead and ensure information availability, integrity, and confidentiality. Listed below are the top 10 Windows Vulnerabilities:

1. **Web Servers :** Misconfigurations, product bugs, default installations, and third-party products such as PHP can introduce vulnerabilities.
2. **Microsoft SQL Server :** Vulnerabilities allow remote attackers to obtain sensitive information, alter database content, and compromise SQL servers and server hosts.
3. **Passwords :** User accounts may have weak, non-existent, or unprotected passwords. The operating system or third-party applications may create accounts with weak or non-existent passwords.
4. **Workstations :** Requests to access resources such as files and printers without any bounds checking can lead to vulnerabilities. Overflows can be exploited by an unauthenticated remote attacker executing code on the vulnerable device.



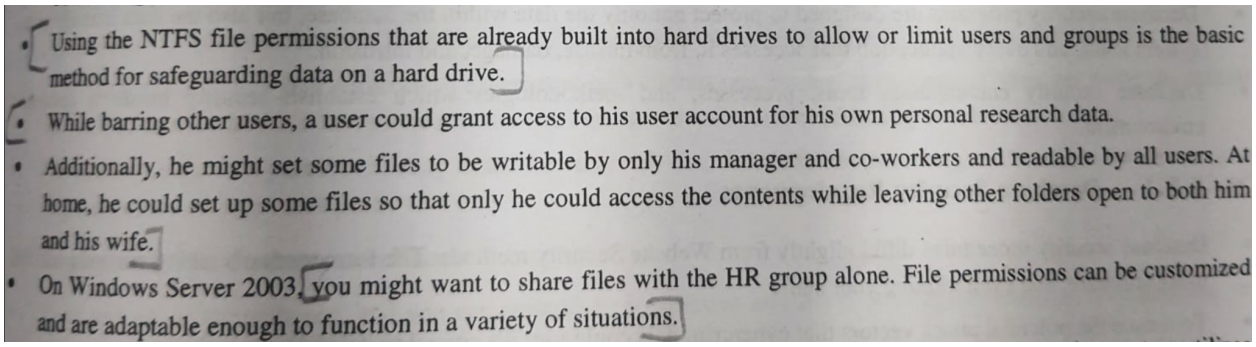
8. **E-mail :** By opening a message a recipient can activate security threats such as viruses, spyware, Trojan horse programs, and worms.

Linux File System Security:



- Every file on a Linux system is owned by a user and a group user.
- There is also a third type of user who is not the user owner and does not belong to the group that owns the file.
- Read, write, and execute rights can be granted or refused for each user category.
- The ls-command also displays file permissions for these three user categories; they are indicated by the nine characters

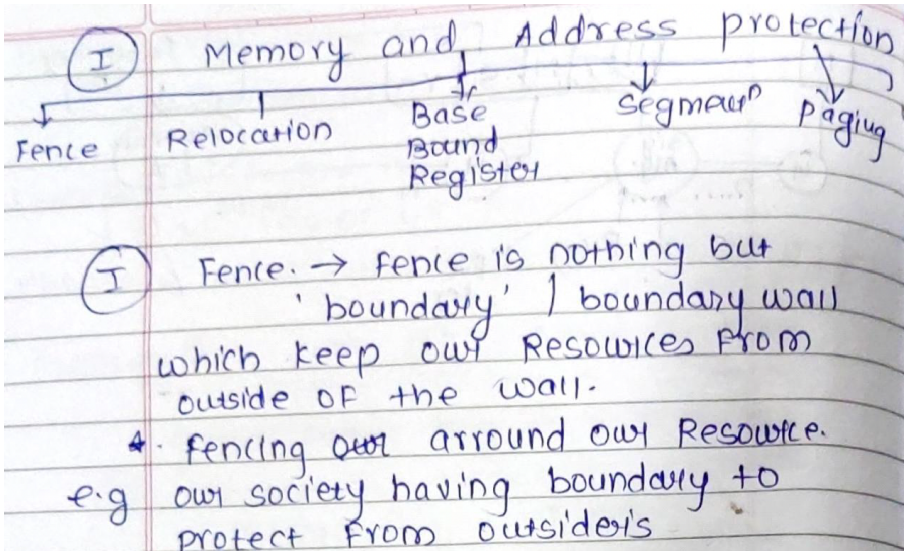
For example, consider that the user's permissions for some files is "rw-" as the first three characters. This means that the owner of the file ("aditya314", i.e. me) can "read" it (look at its contents) and "write" it (modify its contents). I cannot execute it because it is not a program; it is a text file.
If "r-x" is the second set of 3 characters it means that the members of the group "aditya314" can only read and execute the files.
The final three characters show the permissions allowed to anyone who has a UserID on this Linux system. Let us say we have the permission ("r–"). This means anyone in our Linux world can read, but they cannot modify the contents of the files or execute it.
Windows File System Security:



- Using the NTFS file permissions that are already built into hard drives to allow or limit users and groups is the basic method for safeguarding data on a hard drive.
- While barring other users, a user could grant access to his user account for his own personal research data.
- Additionally, he might set some files to be writable by only his manager and co-workers and readable by all users. At home, he could set up some files so that only he could access the contents while leaving other folders open to both him and his wife.
- On Windows Server 2003, you might want to share files with the HR group alone. File permissions can be customized and are adaptable enough to function in a variety of situations.

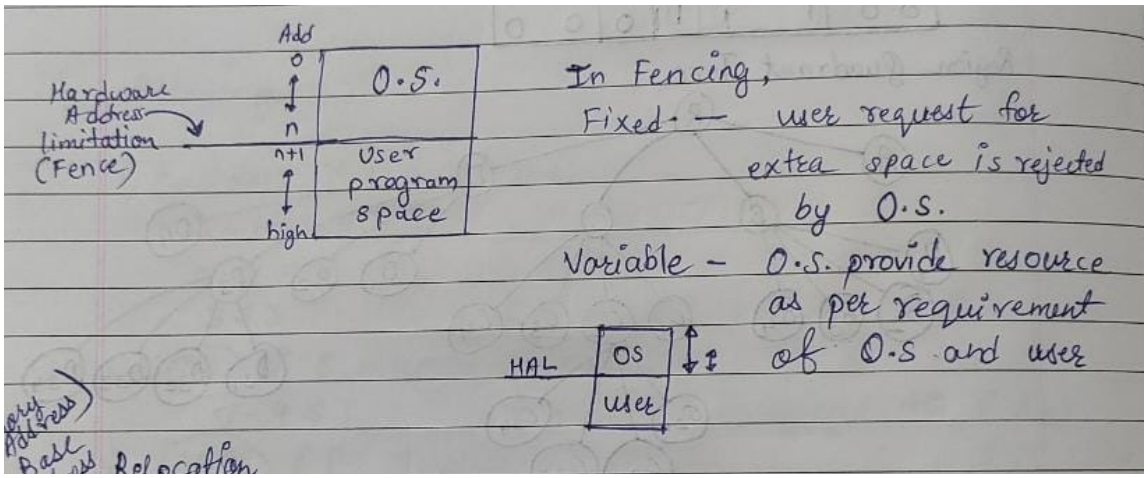
17. How memory and address protection is implemented in system security. Illustrate with an example.

Ans)



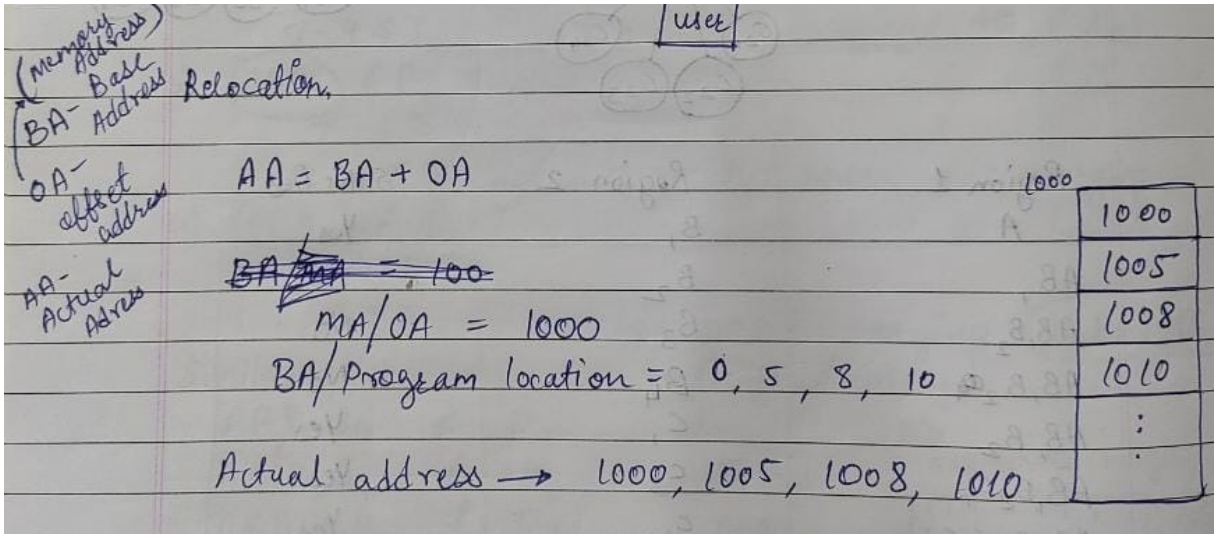
Types of Fencing:

1. Fixed Fence Mechanism: Using network address define fixed area for os and user to use separately
2. Variable Fence Mechanism: The size of area can be vary as per the need of OS (i.e give the unused memory to user)



Relocation

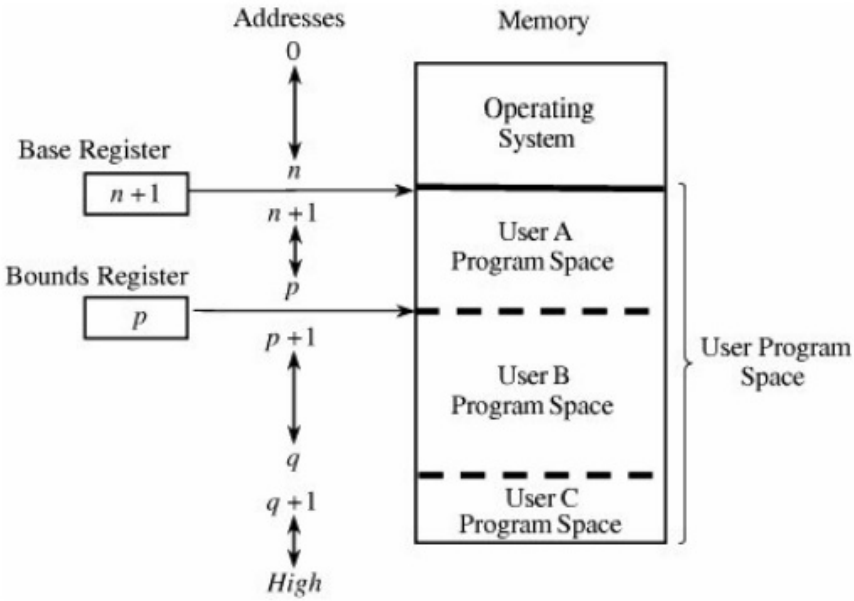
Relocation is the process of taking a program written as if it began at address 0 and changing all addresses to reflect the actual address at which the program is located in memory. In many instances, this effort merely entails adding a constant relocation factor to each address of the program. That is, the relocation factor is the starting address of the memory assigned for the program.



Base & Bound

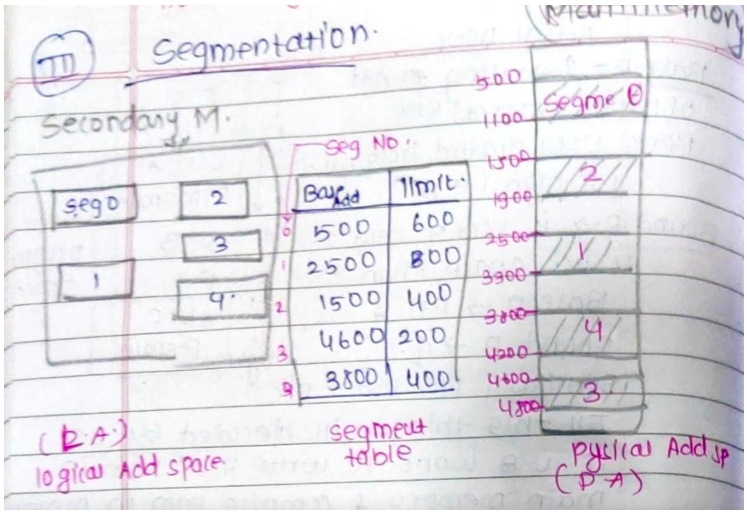
The second register, called a bounds register, is an upper address limit, in the same way that a base or fence register is a lower address limit. Each program address is forced to be above the base address because the contents of the base register are added to the address; each address is also checked to ensure that it is below the bounds address. In this way, a program's addresses are neatly confined to the space between the base and the bounds registers.

Figure 4-3. Pair of Base/Bounds Registers.



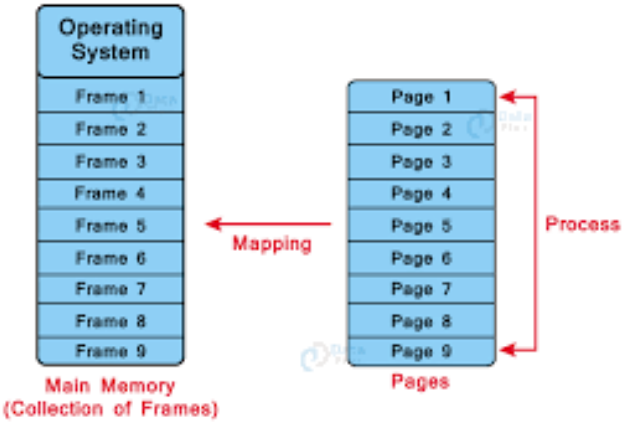
SEGMENTATION:

Segmentation involves the simple notion of dividing a program into separate pieces. Each piece has a logical unity, exhibiting a relationship among all of its code or data values. For example, a segment may be the code of a single procedure, the data of an array, or the collection of all local data values used by a particular module.



PAGING:

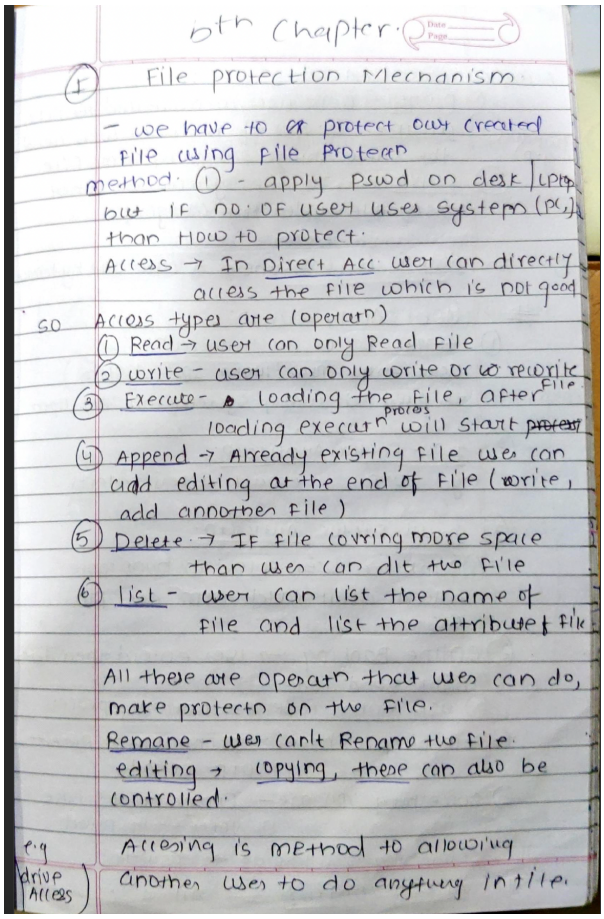
One alternative to segmentation is paging. The program is divided into equal-sized pieces called pages, and memory is divided into equal-sized units called page frames. Each address is again translated by a process similar to that of segmentation: The operating system maintains a table of user page numbers and their true addresses in memory.

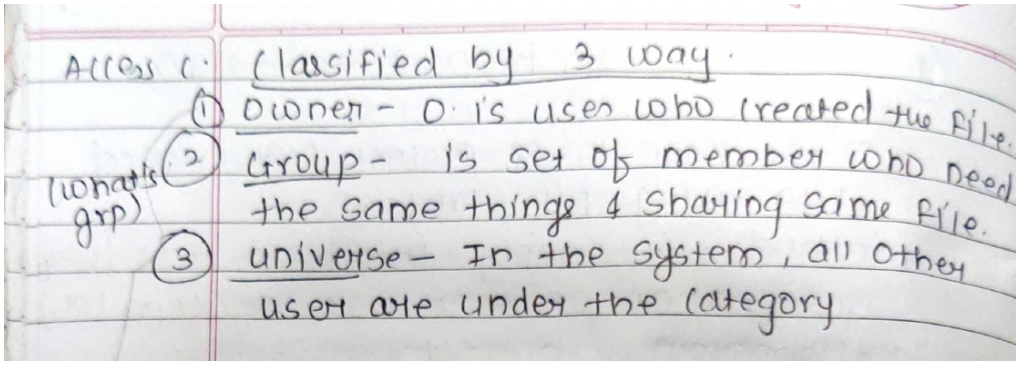


For example, consider a process running on a system that needs to access a file stored on disk. When the process requests to access the file, the operating system loads the file into memory and maps the file's pages to the process's virtual address space. The page table entries for these pages are marked as read-only, preventing the process from modifying the file's contents.

Additionally, the operating system may also use access control mechanisms like user permissions to restrict which processes can access specific files or resources. For example, a file may be marked as readable only by a specific user or group, preventing other users or processes from accessing the file.

18. How file protection mechanism works in software security. Illustrate with an example.
Ans) (ADD USER AUTHENTICATION FROM ABOVE 1STEP, 2STEP, MULTI FACTOR)
File protection mechanism is an essential aspect of software security that aims to ensure the confidentiality, integrity, and availability of sensitive data stored in files.





EXTRA:

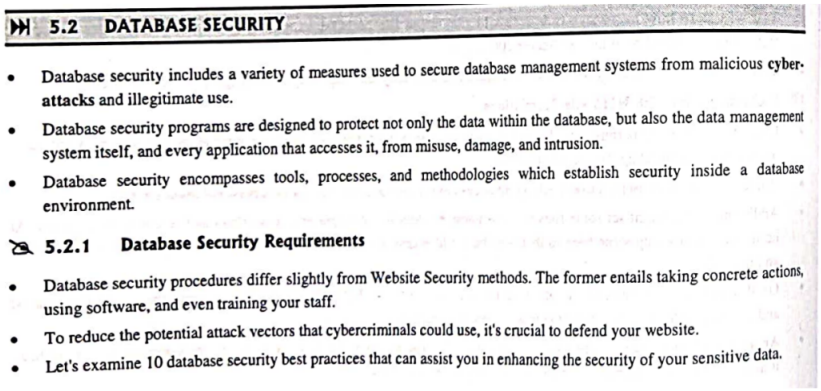
Q.Sensitive Data:

The sensitivity of data is generally classified into different types depending on sensitivity. Sensitive data can be classified into four main types:

- **Low data sensitivity or public classification :** This class of data poses little or no risk to an individual, private organizations, or government agencies when it gets disclosed. Data in this group can be accessed by anyone, as there are little or no restrictions on its accessibility. It is more or less a piece of public information that can be discussed anywhere, and with anyone.
- **Moderate data sensitivity or internal classification :** Moderate sensitivity covers data that is subject to a contractual obligation to protect. This means that the leakage of such data would only cause minimal harm to individuals or organizations concerned
- **High data sensitivity or confidential classification :** Highly sensitive and confidential data must be protected by law or other policies that apply to it. If such data is breached, it could cause significant harm to an individual or any organization.

Q.DataBase Requirements:

Ans)



5.2 DATABASE SECURITY

- Database security includes a variety of measures used to secure database management systems from malicious **cyber-attacks** and illegitimate use.
- Database security programs are designed to protect not only the data within the database, but also the data management system itself, and every application that accesses it, from misuse, damage, and intrusion.
- Database security encompasses tools, processes, and methodologies which establish security inside a database environment.

5.2.1 Database Security Requirements

- Database security procedures differ slightly from Website Security methods. The former entails taking concrete actions, using software, and even training your staff.
- To reduce the potential attack vectors that cybercriminals could use, it's crucial to defend your website.
- Let's examine 10 database security best practices that can assist you in enhancing the security of your sensitive data.

Q. DataBase Reliability & Integrity:

5.2.2 Database Reliability and Integrity

- Users expect a DBMS to give access to the data in a trustworthy manner because databases combine data from numerous sources.
- When software engineers refer to a piece of software as reliable, they indicate that it can operate flawlessly for very extended stretches of time.
- Users expect a DBMS to be dependable since the data are frequently essential to meeting organizational or corporate needs.
- Additionally, consumers trust DBMSs with their data and expect them to safeguard it against loss or harm.

We will examine some of the methods a DBMS protects against loss or damage in this section. The controls we take into account, nevertheless, are not rigid: No security measure can stop a legitimate user from accidentally submitting a valid but inaccurate value.

- Three perspectives can be used to analyze reliability and integrity issues with databases:
  - **Database integrity :** the idea that the database is safeguarded against damage, such as from a disc drive failure or a master database index corruption. Operating system integrity controls and recovery methods take care of these issues.
  - **Element integrity :** the worry that only authorized users can write to or modify the value of a particular data element. A database is shielded from corruption by unauthorized users by effective access controls.
  - **Element accuracy :** the worry that only accurate values are entered into database elements. The insertion of incorrect values can be avoided with the aid of checks on element values. Constrained conditions can also identify false values.

MODULE- 6

3. Define DNS attack and web Browser Attack with examples.

Ans)

DNS Attack:

- A DNS attack is a cyberattack in which the attacker exploits vulnerabilities in the Domain Name System. This is a grave issue in cybersecurity because the DNS system is a crucial part of the internet infrastructure and at the same time, it has many security holes.
- There are many ways in which DNS can be attacked. DNS reflection attacks, DoS, DDoS, and DNS poisoning are just some of the attack types DNS is susceptible to.

Denial of Service (DOS): The denial-of-service attack is an attack in which a system is attacked by a lot of requests to the system at one time that it is not able to handle. The attacker sends multiple requests to the server at the same time and the server is not able to handle such requests. However, this attack is easily identifiable as these loads of requests come from a single sender (the attacker) and it is easy to identify the source of the attack.

● **Distributed Denial of Service (DDOS):** As we saw, in the denial-of-service attack, the source of the attack can be easily identified. Now, there is a modified version of this attack i.e., DDOS i.e., distributed version of the DOS attack. In this attack, the attacker first observes the details of a lot of authorized users. Then, the attacker uses these authorized users at the same time to send requests to the system. Now, thousands (or even more) of requests at the same time are sent to the system and the system cannot recognize the source of attack as there is each request from a different user, and all the users are authorized. So, the attacker is using the authorized users as victims too. The primary victim is the system, and the secondary victims are the authorized users. The authorized users are called Zombie PCs.

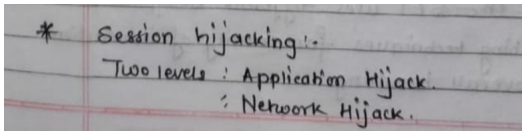
Web Browser Attack:

- Users can see and interact with content on a web page, including text, graphics, video, music, games, and other materials, using a software program called a web browser.
- Internet Explorer, Mozilla Firefox, Opera, and Safari are the most widely used web browsers at the moment. Add-ons and plugins are programs that increase the capabilities of browsers.

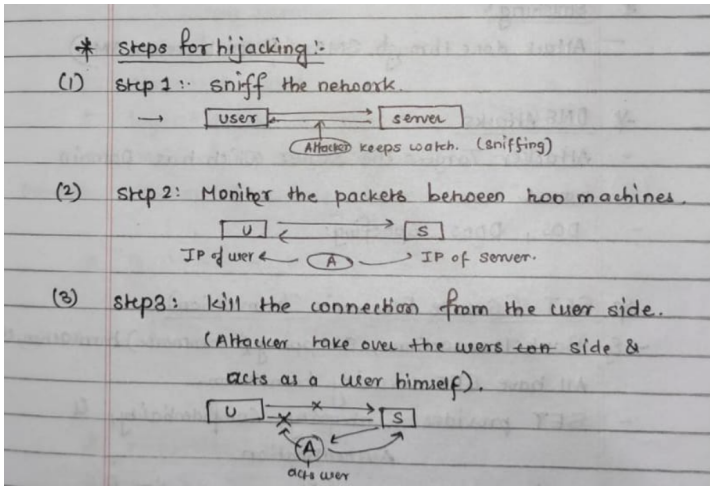
- Web browsers are susceptible to attack or exploitation, much like other software, if the proper security patches aren't installed.
- If the browser plug-ins are not fully patched, a fully patched web browser may still be open to attack or exploit. It's crucial to keep in mind that plug-ins may not always get updated when the browser does.
- Historically, malicious websites were the source of browser-based attacks. However, attackers have recently been successful in breaching a significant number of reliable websites in order to disseminate dangerous payloads to unwary users as a result of weak security coding in web apps or flaws in the software that supports websites.
- Hackers add scripts without altering the look of the website. These scripts could surreptitiously reroute your browser to another website without your knowledge.
- It's possible that your computer will download malicious software as a result of this redirect to another website. These programs are typically made to provide remote access to your computer by the attacker and to collect personal data, frequently in the form of credit card and banking information as well as other information that can be used to commit identity theft.

4. Define Session Hijacking with all hacking steps.

Ans)
Session hijacking is a type of attack where an attacker tries to take control of a legitimate user's session in order to gain unauthorized access to sensitive information or perform malicious activities. The attacker can intercept and manipulate the communication between the user and the server, and use this to take over the user's session.



Application hijacking, also known as app hijacking, is a type of cyber attack where an attacker gains unauthorized access to an application by exploiting vulnerabilities in the application or the underlying system. The attacker may use this access to steal sensitive data, modify or delete files, or execute malicious code on the compromised device.
Network Hijacking is a type of organizational hijacking that involves the unauthorized use of groups of IP addresses, known as ranges. Network hijacking includes IP hijacking or Route Hijacking.



In the above figure, it can be seen that the attacker captures the victim's session ID to gain access to the server by using some packet sniffers.

Session hijacking example: Aditya is sitting in a coffee shop sipping a latte and checking his bank balance. A hijacker at the next table uses "session sniffing", one of the techniques to grab the session cookie, take over the session, and access his bank account.

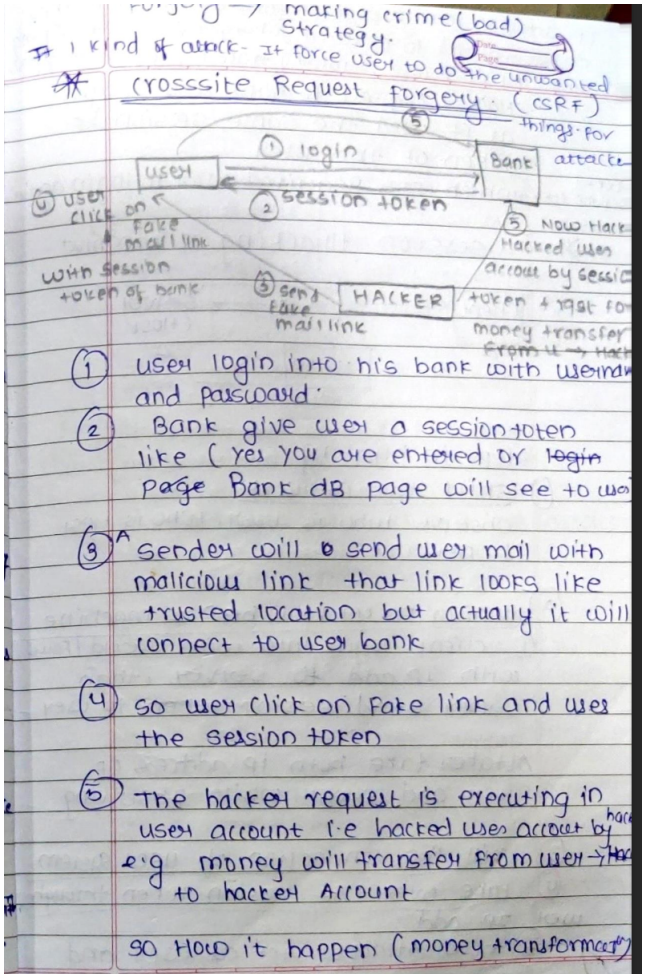
9. What is meant by CrossSite Request Forgery.
Ans)

- Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.
- With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.
- If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

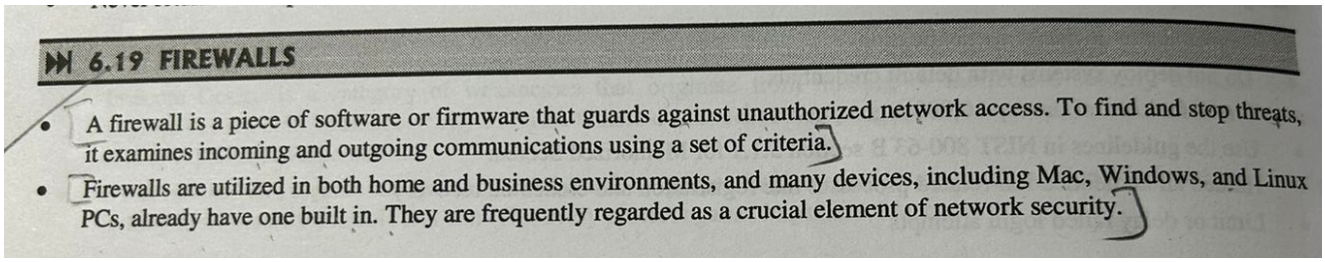
For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.

☞ **Preventing CSRF Vulnerabilities**

- Security experts propose many CSRF prevention mechanisms. This includes, for example, using a referer header, using the HttpOnly flag, sending an X-Requested-With custom header using jQuery, and more.

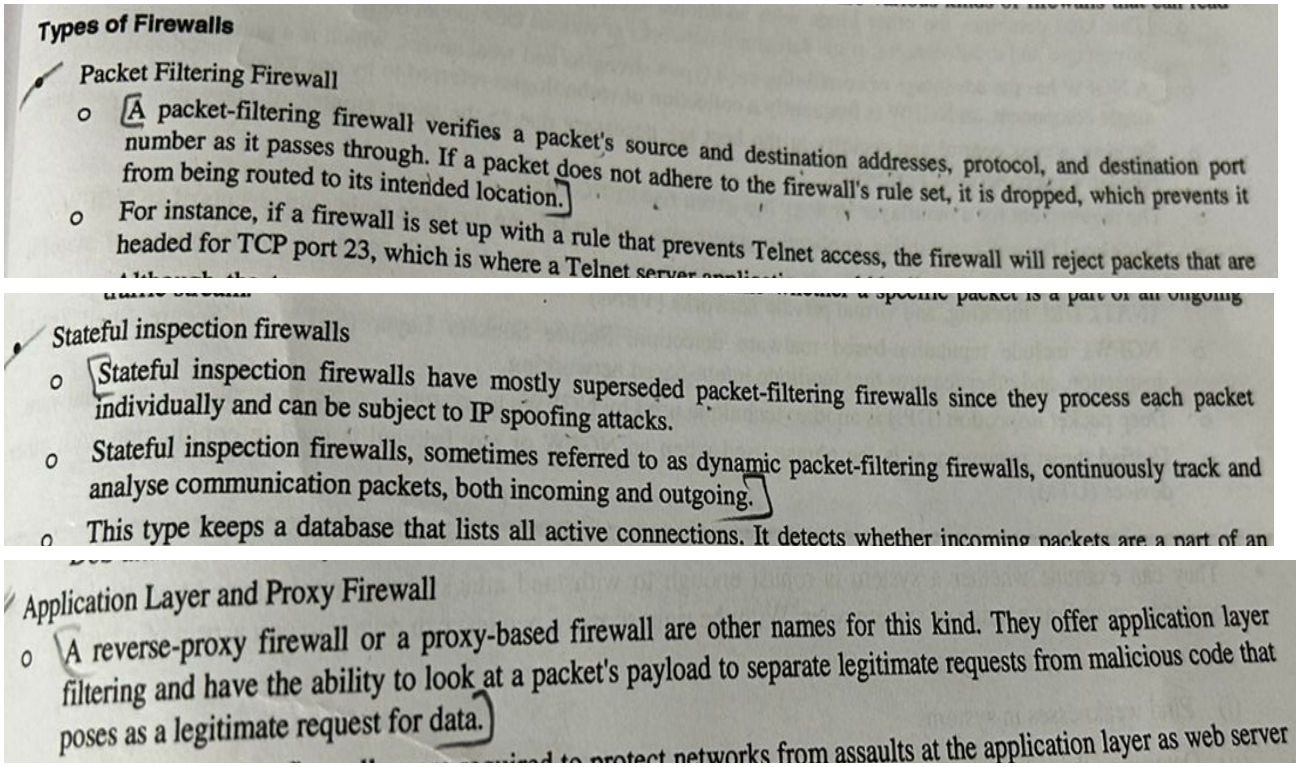


10. Define Firewall and its types.
Ans)



6.19 FIREWALLS

- A firewall is a piece of software or firmware that guards against unauthorized network access. To find and stop threats, it examines incoming and outgoing communications using a set of criteria.
- Firewalls are utilized in both home and business environments, and many devices, including Mac, Windows, and Linux PCs, already have one built in. They are frequently regarded as a crucial element of network security.



Types of Firewalls

Packet Filtering Firewall

- A packet-filtering firewall verifies a packet's source and destination addresses, protocol, and destination port number as it passes through. If a packet does not adhere to the firewall's rule set, it is dropped, which prevents it from being routed to its intended location.
- For instance, if a firewall is set up with a rule that prevents Telnet access, the firewall will reject packets that are headed for TCP port 23, which is where a Telnet server

Stateful inspection firewalls

- Stateful inspection firewalls have mostly superseded packet-filtering firewalls since they process each packet individually and can be subject to IP spoofing attacks.
- Stateful inspection firewalls, sometimes referred to as dynamic packet-filtering firewalls, continuously track and analyse communication packets, both incoming and outgoing.
- This type keeps a database that lists all active connections. It detects whether incoming packets are a part of an

Application Layer and Proxy Firewall

- A reverse-proxy firewall or a proxy-based firewall are other names for this kind. They offer application layer filtering and have the ability to look at a packet's payload to separate legitimate requests from malicious code that poses as a legitimate request for data.

protect networks from assaults at the application layer as web server

15. The message" The meeting is Delayed "is to be Securely communicated to the receiver. Apply the knowledge of SSH and show the steps to communicating this message.

Ans) To securely communicate the message "The meeting is delayed" using SSH, you can follow these steps:

1. Open a terminal on your local computer and type the following command:

ssh user@remotehost
Replace "user" with the username on the remote host and "remote host" with the hostname or IP address of the remote host.

1. Enter your password when prompted. This will establish a secure SSH connection to the remote host.
2. Type the following command to send the message:

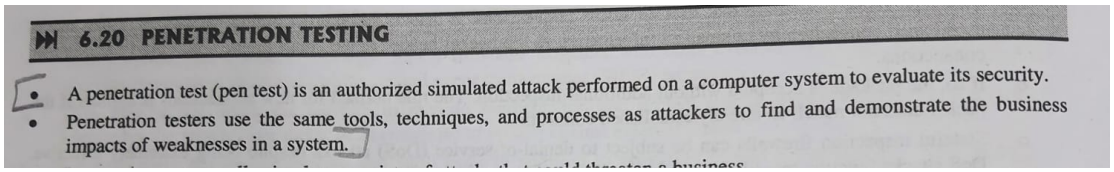
echo "The meeting is delayed" | ssh user@remotehost 'cat > message.txt'
This will send the message "The meeting is delayed" to the remote host and save it to a file named "message.txt".

1. Close the SSH connection by typing:

exit
This will close the SSH connection and return you to your local terminal.

By using SSH, the message is encrypted and transmitted securely over the network, preventing unauthorized access or interception of the message.

16. Explain how data is protected during and after Penetration Testing. Illustrate its Phases and Methods.
Ans)



6.20 PENETRATION TESTING

- A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security.
- Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.

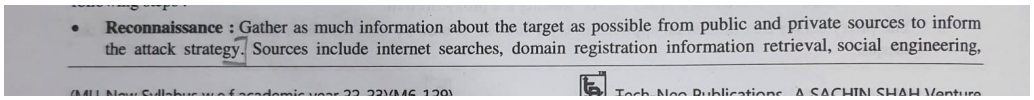
To protect the data during and after penetration testing, various measures can be taken.
During Penetration Testing:

1. Non-Disclosure Agreements (NDAs): An NDA can be signed between the penetration testing team and the organization to ensure that all sensitive information and data found during testing remains confidential.
2. Scope Limitation: The scope of the testing can be limited to certain systems, networks, or applications to ensure that only authorized areas are being tested and that sensitive data is not exposed.
3. Use of Test Data: The penetration testing team can use test data that is representative of the actual data to ensure that real data is not exposed or modified during the testing process.
4. Data Encryption: Data encryption can be used during testing to ensure that sensitive data remains protected while it is being used by the penetration testing team.

After Penetration Testing:

1. Data Deletion: All data used during testing should be securely deleted and removed from the testing environment to ensure that it is not accessible to unauthorized users.
2. Reporting and Remediation: The penetration testing team should provide a report that includes all vulnerabilities found during testing and recommendations for remediation. The organization should then take steps to address the identified vulnerabilities.

PHASES:



- **Reconnaissance :** Gather as much information about the target as possible from public and private sources to inform the attack strategy. Sources include internet searches, domain registration information retrieval, social engineering,

target's attack surface and possible vulnerabilities. Reconnaissance can vary with the scope and objectives of the pen test; it can be as simple as making a phone call to walk through the functionality of a system.

- **Scanning :** Pen testers use tools to examine the target website or system for weaknesses, including open services, application security issues, and open-source vulnerabilities. Pen testers use a variety of tools based on what they find during reconnaissance and during the test.
- **Gaining access :** Attacker motivations can include stealing, changing, or deleting data; moving funds; or simply damaging a company's reputation. To perform each test case, pen testers determine the best tools and techniques to gain access to the system, whether through a weakness such as SQL injection or through malware, social engineering, or something else.
- **Maintaining access :** Once pen testers gain access to the target, their simulated attack must stay connected long enough to accomplish their goals of exfiltrating data, modifying it, or abusing functionality. It's about demonstrating the potential impact.

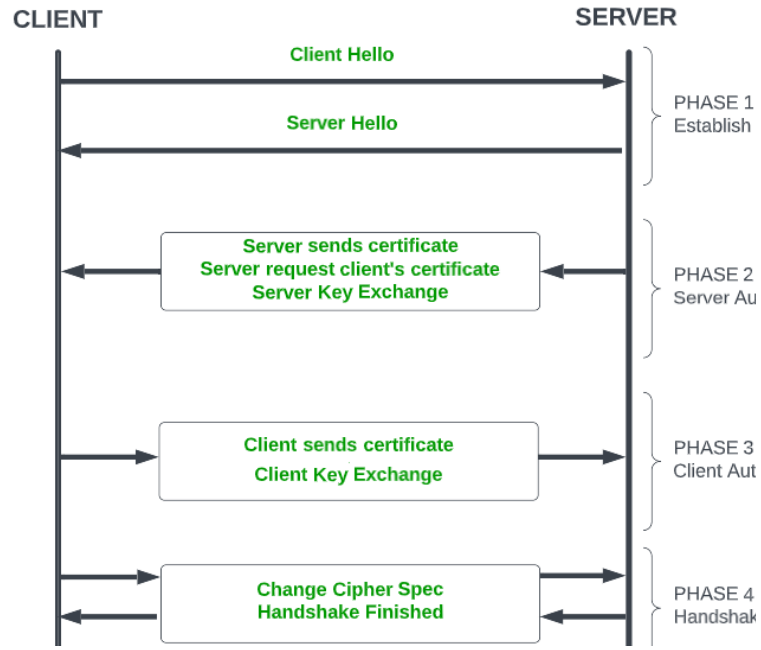
6.20.2 Penetration Testing Methods

Following are the different methods of penetration testing :

1. **External testing :** External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access to and extract valuable data.
2. **Internal testing :** In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.
3. **Blind testing :** In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.
4. **Double-blind testing :** In a double-blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defense before an attempted breach.
5. **Targeted testing :** In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a

19. The message" The meeting is canceled "is to be Securely communicated to the receiver. Apply the knowledge of SSL and show the steps for communicating this message.

Ans)



Secure Socket layer (SSL)

(1) It provide security when 2 user are doing communicatn over on network so SSL give security betn 2 user.

(2) It ensures the Integrity, authenticatn & confidentiality.

(3) It lies betn Applicatn layer & transport layer of TCP/IP proto.

Appln L
SSL
Transport L

TCP/IP ⇒ 4 lay
OSI → 7 layer

protocol Stack of SSL.

SSL Handshake protocol	SSL change cipher sec	SSL alert protocol	http
SSL Record protocol			
TCP			
IP			

SSL Record protocol ⇒ 2 services.
(1) confidentiality of data ⇒ done by encrypt no 3rd party can involved.
(2) Msg Integrity ⇒ done by MAC.

working

Data — Application layer data
F1 F2 F3 ... — Fragmentatn (2^{14})
lossless compression — data compressn
100
100 | MAC — MAC Addition
110 → 100110
PT — Encryptn
SSL Header | CT — Add SSL Header.

(1) A data presen on Appln layer &
(2) data divided into no of Fragmen and process called Fragmentatn. Based on size of data it's divide into no of Frg
(3) each Fragmen size = 2^{14} byte blocks
(4) once it divided into no of fragmen each fragmen will follow same process.
(5) take F1 and do data compression (dc) dc ⇒ Reduce the size of data i.e F1
2 type dc ⇒ lossy c & lossless c.
lossy com ⇒ some data loss will happen ⇒ loss of data happen.
lossless dc ⇒ Data loss will not happen size of data will loss or compress

(6) After finding lossless data by comp calculate MAC code
Once get MAC code Append (add) MAC data at the end of lossless c. data.
e.g lossless c. data = 100
MAC data = 110
so. 100110

(7) In MAC Addit part you will get Msg Integrity

(8) Before encryptn we call data as PT Encryptn is used for confidentiality

(9) After Applying En on PT we get CT
(10) Once get CT → Add SSL Header at the begining (starting) of CT

working.

(1) connectn (wire or wireless) establishmen with server.
(2) key exchange from server to Client ⇒ for checking Client is authorized or not
(3) key exchange from Client to server ⇒ whether server is auth or not
(4) Handshake done from server. ensure you are authorized person
e.g if you want to login into gmail account.
1st step (1) GO to google enter gmail
(2) server ask for psswd
(3) Client enter psswd
(4) once write you access the login.

I SSL Handshake protocol

we got Integrity & confidentiality in SSL Record protocol

Ensure ⇒ Here we get Authentication.
⇒ most complicated part in SSL
⇒ It do key exchange btn Client/server

II SSL change cipher protocol

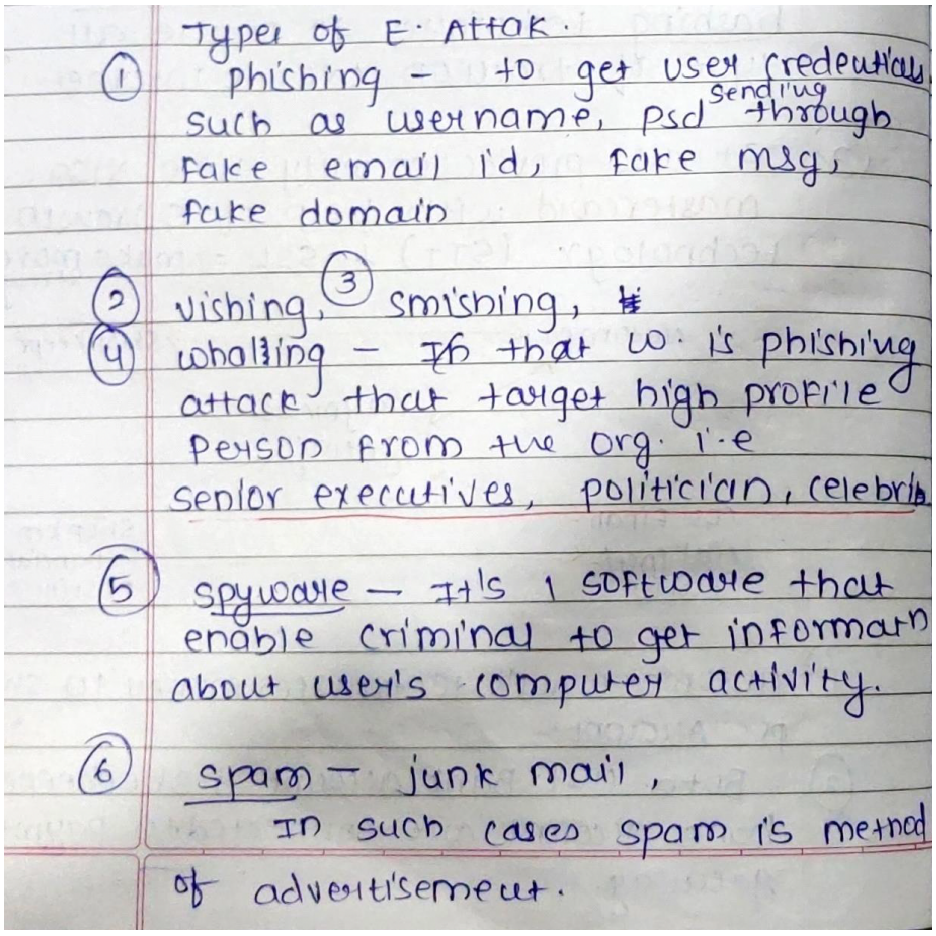
- size = 1byte → Single byte
- It copies the pending state into current state.

III SSL Alert protocol

(1) whatever alert Related to SSL those alert sent to Client.
(2) It has 2 bytes size

20. How Email Attacks can be done by an attacker in Web Security. Illustrate its types with examples.

Ans) Email is a universal service used by over a billion people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations. Below are some of the most common types of Attacks:



Email Spoofing: Email spoofing involves sending emails that appear to come from a trusted source, but actually come from a different sender. This attack can be used to trick users into downloading malware or providing sensitive information. One advantage of this attack is that it can be easily carried out using basic technical skills, without the need for sophisticated social engineering techniques. However, it can be easily detected if users are aware of the legitimate source of the email.

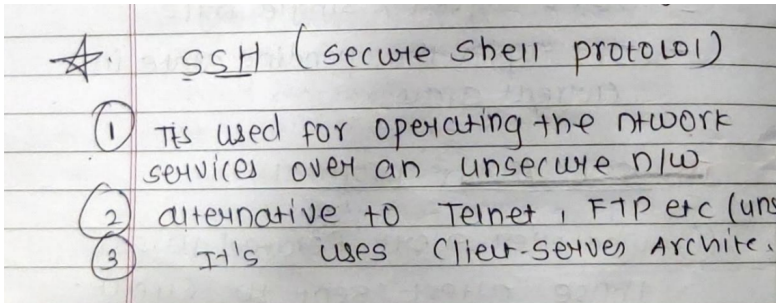
Spear Phishing: Spear phishing is a targeted version of phishing that involves sending customized emails to a specific individual or group of individuals. These emails are designed to look like they come from a trusted source and are personalized to increase the likelihood of the victim falling for the attack. One advantage of this attack is that it can be highly effective, as the attacker has done research on the victim to make the email seem more legitimate. However, it requires more effort and resources than a generic phishing attack.

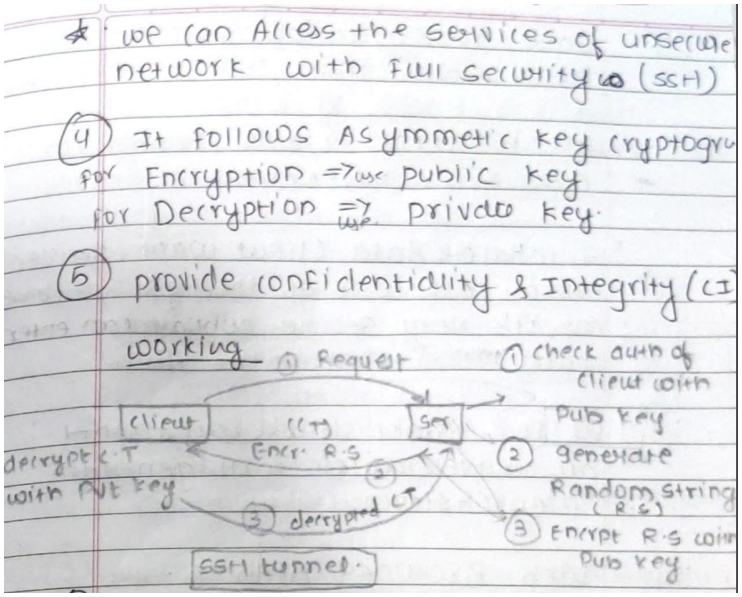
How to Protect Yourself from Email Attacks

- Be cautious when opening emails from unknown sources.
- Look for signs of phishing, such as spelling errors, suspicious links or attachments, and requests for personal information.
- Use strong passwords and two-factor authentication to protect your email account.
- Keep your computer and software up-to-date with the latest security patches.
- Use antivirus and anti-malware software to detect and prevent email attacks.

EXTRA:

Q.SSH theory:





Q.Clickjacking

Ans)