INS QB

1) What are Symmetric Ciphers? Explain Caesar cipher

Ans: Symmetric Encryption / Cipher 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.

A symmetric encryption scheme has five ingredients:

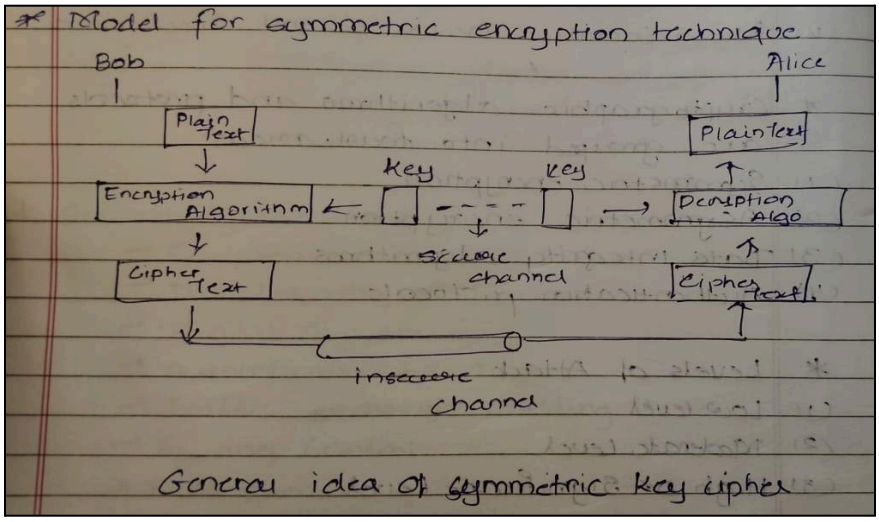
• **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

• **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

• **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

• **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext



Caesar Cipher

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

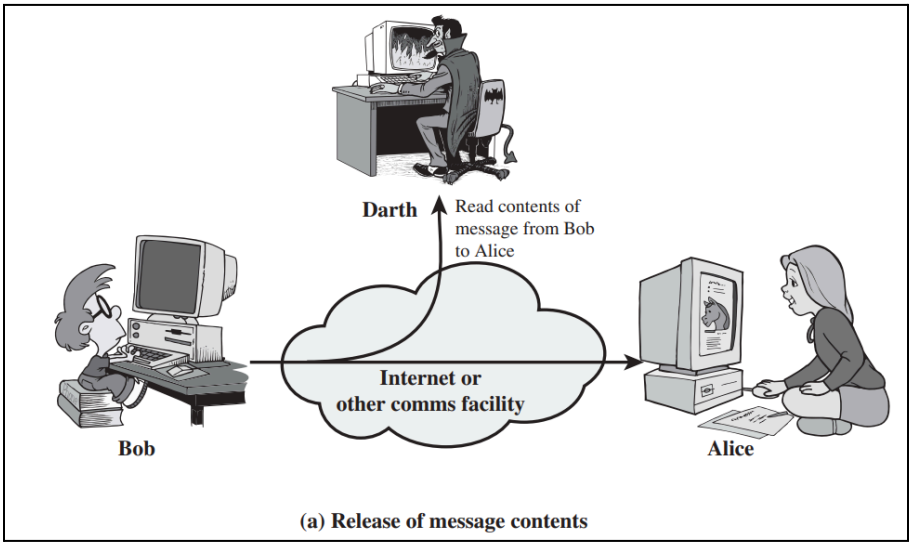
plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

2) What are the various types of Passive attacks?

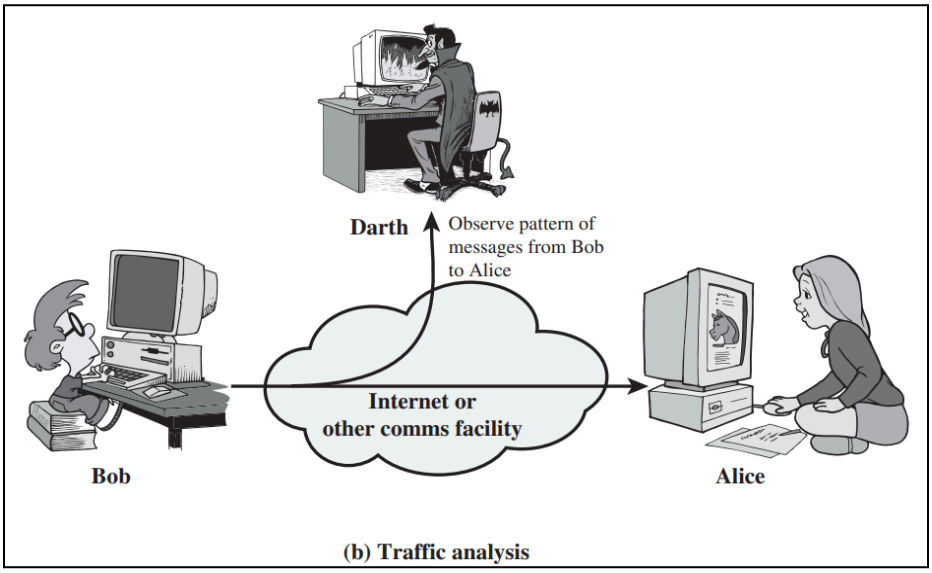
Ans: Two types of passive attacks are the release of message contents and traffic analysis.

1. Release of message contents / Snooping: is easily understood in figure .A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



(a) Release of message contents

2. Traffic analysis : If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place

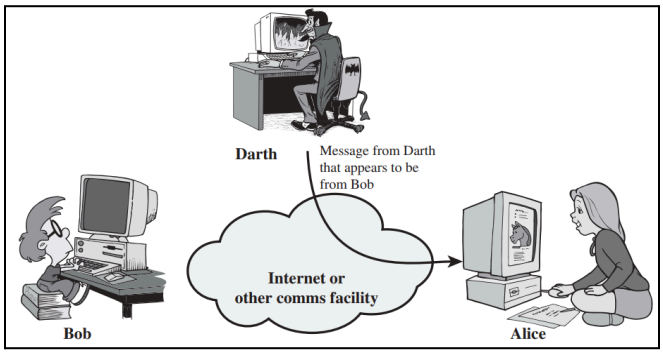


(b) Traffic analysis

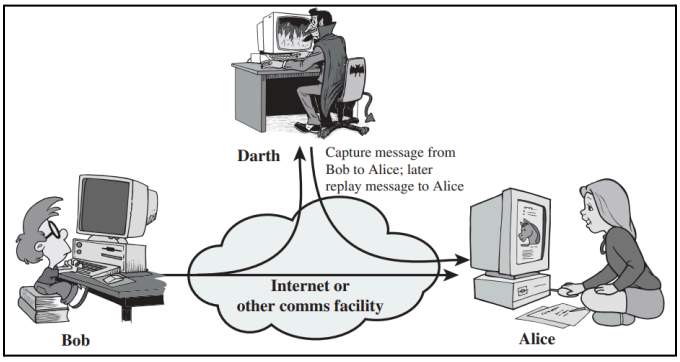
3) Explain any three Active attacks

Ans:

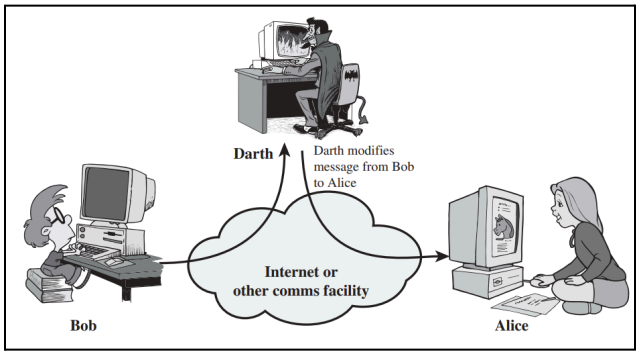
1. Masquerade : It takes place when one entity pretends to be a different entity (Figure 1.3a).A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



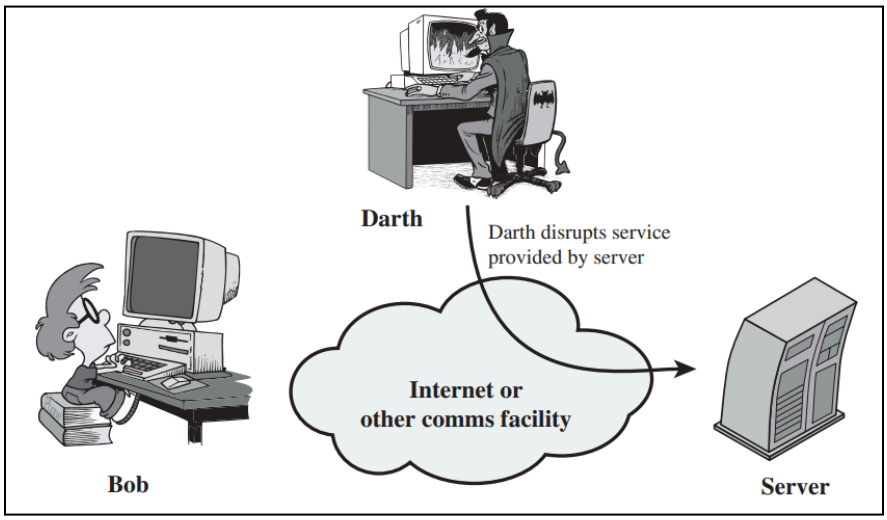
2. Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.



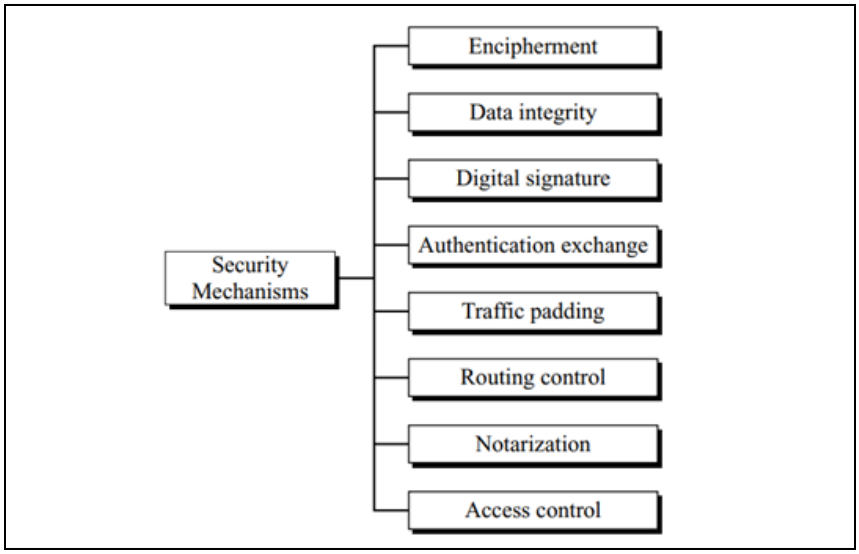
3. Modification of messages: It simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts.



4. Denial of service: The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination .Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



4) What are the security mechanisms to provide security at various levels of OSI model?
Ans:



Encipherment

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today two techniques—cryptography and steganography—are used for enciphering. We will discuss these shortly.

Data Integrity

The **data integrity** mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver receives the data and the checkvalue. He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received. If the two checkvalues are the same, the integrity of data has been preserved.

Digital Signature

A **digital signature** is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

Authentication Exchange

In **authentication exchange,** two entities exchange some messages to prove their identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

Traffic Padding

Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

Routing Control

Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

Notarization

Notarization means selecting a third trusted party to control the communication between two entities. This can be done, for example, to prevent repudiation. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

5) What are the 5 components of a Symmetric cipher model?

Ans:

1. **Plaintext**: The original data that needs to be encrypted or secured.
2. **Encryption Algorithm**: The mathematical procedure used to transform plaintext into ciphertext. This algorithm uses a symmetric key for encryption.
3. **Symmetric Key**: The secret key used for both encryption and decryption. Both the sender and the receiver must possess the same key.

4. **Ciphertext**: The encrypted output generated by applying the encryption algorithm to the plaintext using the symmetric key.
5. **Decryption Algorithm**: The mathematical procedure used to transform ciphertext back into plaintext. This algorithm uses the same symmetric key that was used for encryption.

6) How is encryption done using Playfair cipher?

Ans: Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

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

In this case, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letters I and J count as one letter.

7) Discuss the various methods used in steganography

Ans: Steganograpgy is the technique of hiding a message within another message

Some common techniques are as follows:

1. Character marking: Selected letters of printed or typewritten text are over-written in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

2. Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

3. Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

4. Typewriter correction ribbon: Used between lines typed with a black ribbon, the

results of typing with the correction tape are visible only under a strong light

8) Explain the DES technique

Ans:

- DES stands for Data Encryption Standard. It is a type of symmetric encryption, which means the same key is used for both encrypting and decrypting data.
- DES is a Feistel cipher, which is a specific structure used in many encryption algorithms.
- DES is a block cipher. This means it processes data in fixed-size blocks. Specifically, it works with 64-bit blocks of data.
- It takes 64-bit plaintext (the original data) and uses a 56-bit key to encrypt it, turning it into 64-bit ciphertext (the encrypted data).
- DES uses a 56-bit key for encryption. The process involves 16 rounds of operations to securely encrypt the data.
- There are initial and final permutations, meaning the data is shuffled at the start and end of the encryption process.