SECURITY ATTACKS:

Security attacks are classifieds into two:

- ***Passive attacks and***
- ***Active attacks.***

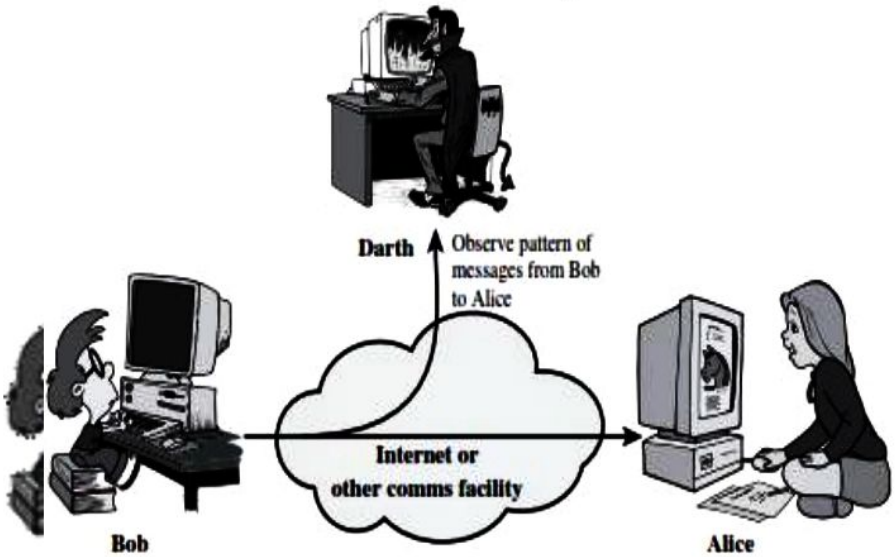
A passive attack attempts to learn or make use of information from the system but does not affect system resources.

An active attack attempts to alter system resources or affect their operation.

Passive Attacks:

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

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



(b) Traffic analysis

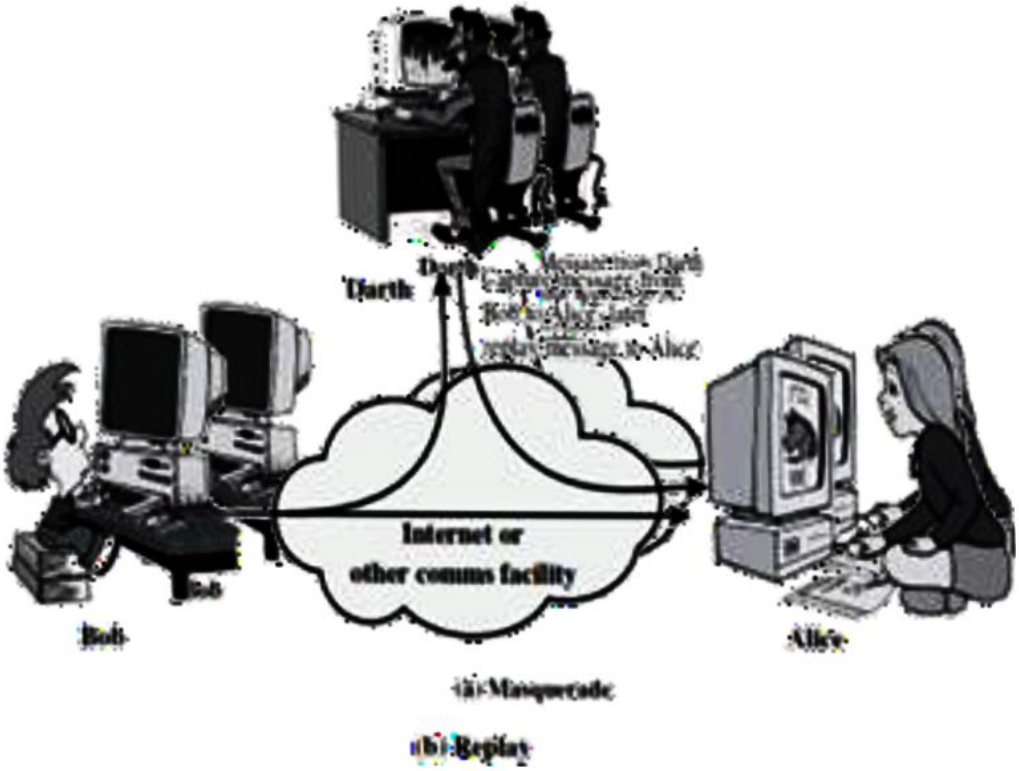
Release of message contents: The **release of message contents is easily understood.** A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

TRAFFIC ANALYSIS:

- Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, evenif theycaptured the message, couldnot extract the informationfrom the message.
- The common technique for masking contents is encryption.
- 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 communicationthat was taking place.
- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
- Typically, the message traffic is sent and receivedin an apparentlynormal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usuallyby means of encryption.
- Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into **four** categories: **masquerade, replay, modification of messages, and denial of service**.

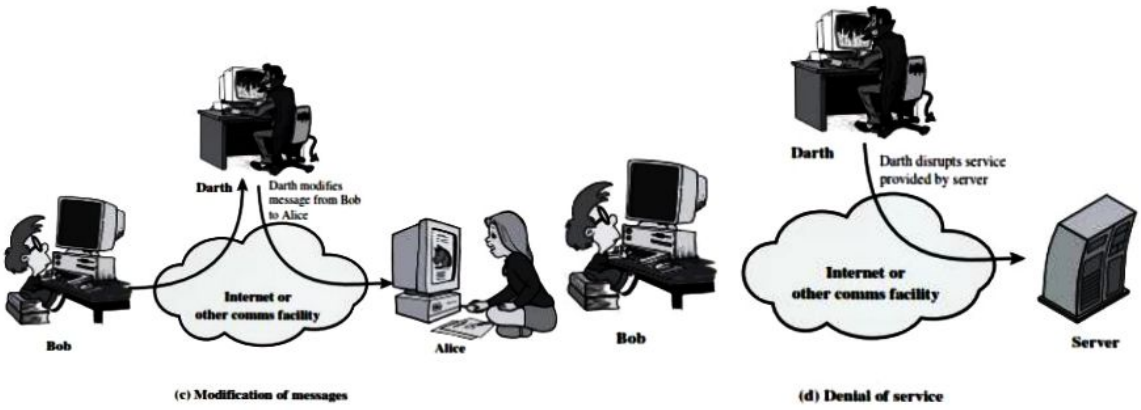
A masquerade attack is an attack that uses a fake identity, to gain unauthorized access to personal computer information through legitimate access identification. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



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

Modification of messages simply means that some portion of a valid 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."*



The **denial of service prevents 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.

SECURITY SERVICES:

- Security service means a processing or communicationservice that is provided by a system to give a specific kind of protection to system resources.
- X.800 divides these services into
  - **AUTHENTICATION**
  - **ACCESS CONTROL**
  - **DATA CONFIDENTIALITY**
  - **DATA INTEGRITY**
  - **NONREPUDIATION**
  - **AVAIL**

ABILITY

AUTHENTICATION:

The authentication service is concerned with assuring that a communication is authentic. In the case of a **single message**, its function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an **ongoing interaction**, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures

that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interferedwith in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Two specific authentication services are defined

- Peer entity authentication
- Data origin authentication

Peer entity authentication: Provides for the corroboration of the identity of a peer entities involved in communication. It is used for providing authentication at the time of connection establishment and during the process of data transmission.

Data origin authentication: Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supportsapplications like electronic mail, where there are no prior interactions between the communicating entities .

ACCESS CONTROL:

The prevention of unauthorized use of a resources. Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailoredto the individual.

DATA CONFIDENTIALITY:

Confidentiality is the protection of transmitted data from passive attacks. The protection of data from unauthorized disclosure.

Types of confidentiality:

- **Connection Confidentiality:** The protection of all user data on a connection.
- **Connectionless Confidentiality:** The protection of all user data in a single data block
- **Selective-Field Confidentiality:** The confidentiality of selected fields within the user data on a connection or in a single data block.
- **Traffic-Flow Confidentiality:** The protection of the information that might be derived from observation of traffic flows.

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

Types of integrity

- **Connection Integrity with Recovery**: Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery** as above, but provides only detection without recovery.
- **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferredover a connectionand takesthe formof determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- **Connectionless Integrity** Provides for the

- **Selective-Field Connectionless Integrity** Provides for the integrityof selected fields withina single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION:

It is assurance that someone cannotdenysomething. It is a method of guaranteeingmessage transmission between parties. Provides protection againstdenial by one of the entities involved in a communication of having participated in all or part of the communication.

- **Nonrepudiation, Origin: Proof** that the message was sent by the specified party.
- **Nonrepudiation, Destination:** Proof that the message was received by the specified party.

SECURITY MECHANISMS:

Security mechanism are categorized into two types. They are,

- **SPECIFIC SECURITY MECHANISMS**
- **PERVASIVE**

SECURITY MECHANISMS

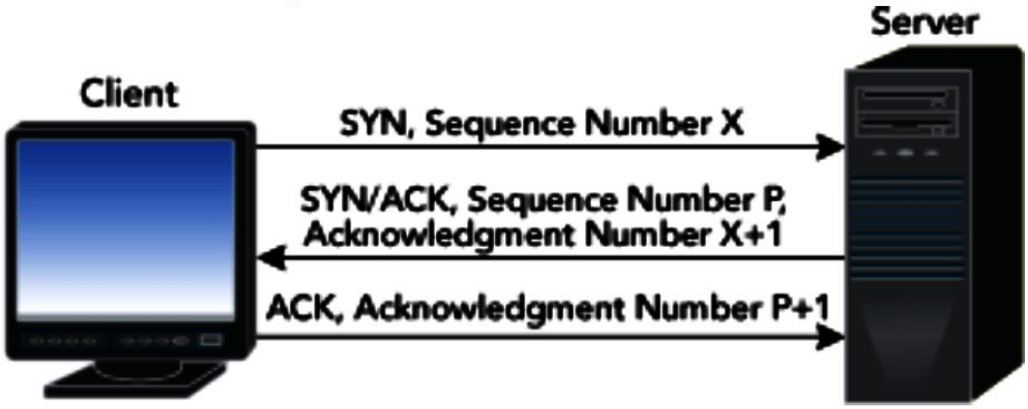
SPECIFIC SECURITY MECHANISMS:

These mechanisms are incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

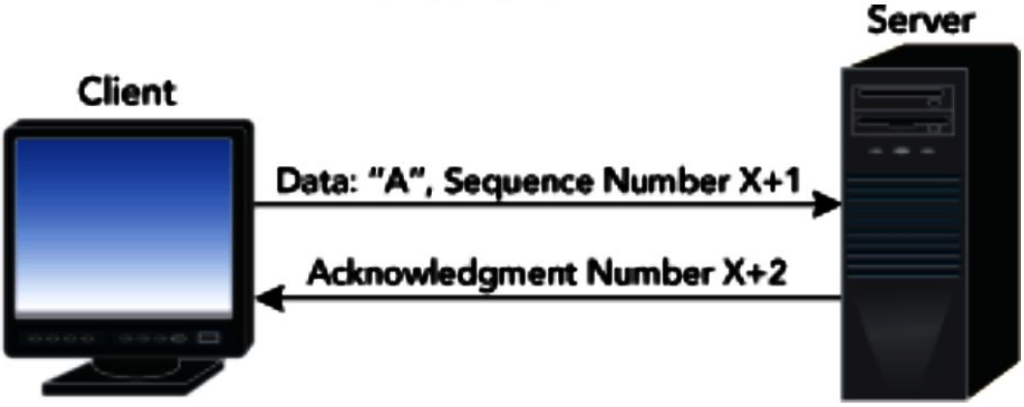
- **Encipherment:** It refers to the processof applying mathematical algorithmsto transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and encryption keys.
- **Digital Signature:** Data appended to, or a cryptographic transformation of, a data unit must preserve the integrity of the data and prevents it from any unauthorized access.
- **Access Control:** A variety of mechanisms that enforce access rights to resources.
- **Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Authentication Exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic Padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control:** Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization:** The use of a trusted third party to assure certain properties of a data exchange.

TCP session hijacking:

TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. In order to guarantee that packets are delivered in the right order, TCP uses acknowledgement (ACK) packets and sequence numbers to create a "full duplex reliable stream connection between two end points," with the end points referring to the communicating hosts. The connection between the client and the server begins with a three-way handshake.



Figure(a): TCP Three-Way Handshake



For now, observe what happens to these sequence numbers when the client starts sending data to the server (see **Figure (b)**). In order to keep the example simple, the client sends the character A in a single packet to the server.

Figure(b) Sending Data over TCP

TCP Session hijacking is when a hacker takes over a TCP session between two machines. Since most authentications only occur at the start of a TCP session, this allows the hacker to gain access to a machine.

A popular method is using source-routed IP packets. This allows a hacker at point A on the network to participate in a conversation between B and C by encouraging the IP packets to pass through its machine. If source-routing is turned Off, the hacker can use “blind" hijacking see figure (c), whereby it guesses the responses of the two machines. Thus, the hacker can send a command, but can never see the However, a common command would be to set a password allowing access from somewhere else on the net. A hacker can also be "inline" between B and C using a sniffing program to watch the conversation. This is known as a "**man-in-the-middle attack**".

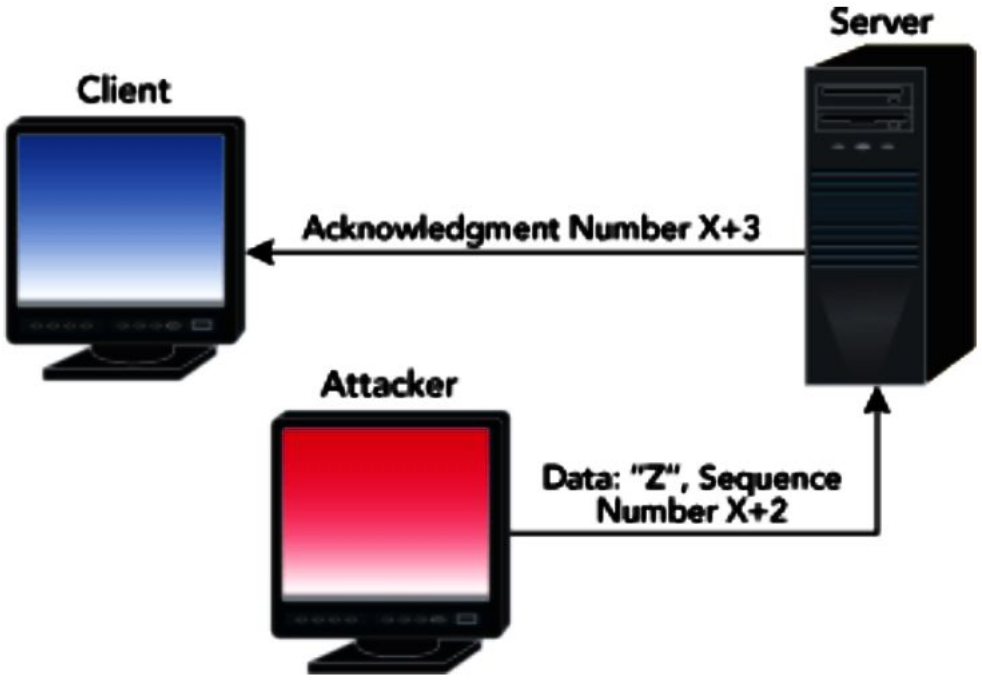
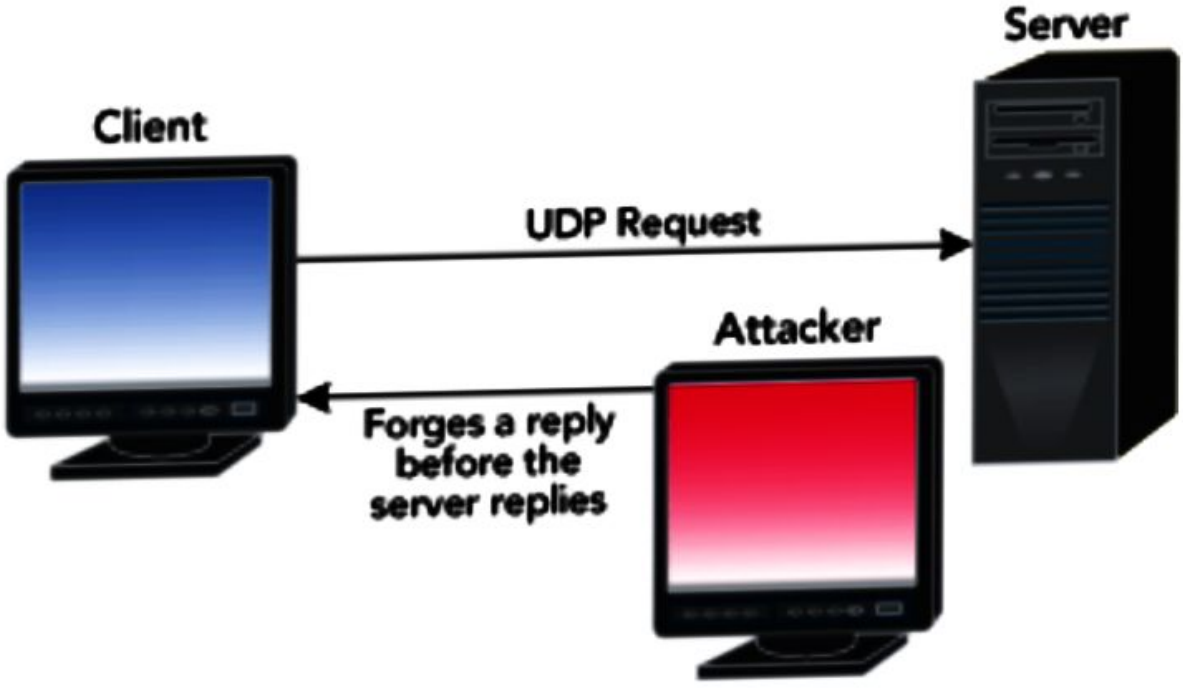


Figure (c) Blind hijacking

A common component of such an attack is to execute a denial-of-service attack against one end-point to stop it from responding. This attack can be either against the machine to force it to crash, or against the network connectionto force heavy packet loss. TCP session hijacking is a much more complex and difficult attack.

UDP Hijacking:

UDP which stands for User Datagram Protocol is defined as a connectionless protocol. It offers a direct way to send and receive datagram's over an IP network. UDP doesn't use sequence numbers like TCP. It is mainly used for broadcasting messages across the network or for doing DNS queries. Hijacking a session over a User Datagram Protocol (UDP) is exactly the same as over TCP, except that UDP attackers do not have to worry about the overhead of managingsequence numbers and other TCP mechanisms. Since UDP is connectionless, injecting data into a session without being detected is extremely easy.



SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has five ingredients (Figure 2.1):

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

- **Encryption algorithm:** The encryption algorithm performs various substitu-tions 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.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The

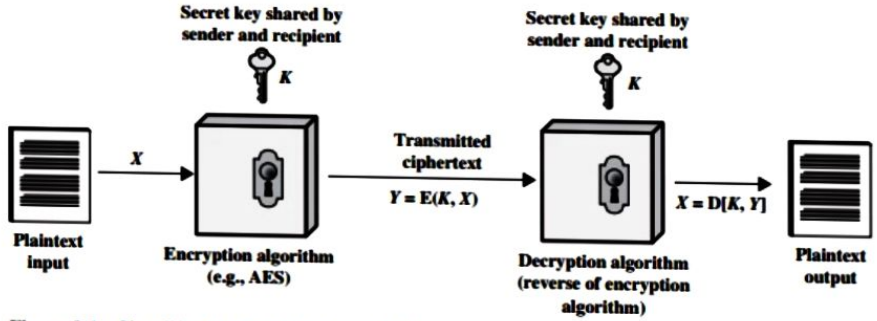


Figure 2.1 Simplified Model of Symmetric Encryption

opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

We assume that it is impractical to decrypt a message on the basis of the ciphertext *plus* knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret. This feature of symmetric encryption is what makes it feasible for widespread use. The fact that the algorithm need not be kept secret means that manufacturers can and have developed low-cost chip implementations of data encryption algorithms. These chips are widely available and incorporated into a number of products. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

What is Phishing?

A phishing attack is a type of cybersecurity threat that targets users directly through email, text or direct messages. During one of these scams, a cybercriminal will pose as a trusted contact to steal data from an unsuspecting user such as login information, account numbers and credit card information.

While there are several types of phishing, the main purpose behind all of them is it to steal sensitive information or transfer malware. Here are three of the most common phishing attempts.

Spear Phishing

While many phishing attempts use spam-like tactics to reach thousands of emails at once, **spear phishing** attacks target specific individuals within an organization. Hackers customize their emails with the target's name, title, work phone number and other information to trick the recipient into believing that the sender somehow knows them personally or professionally.

Whaling

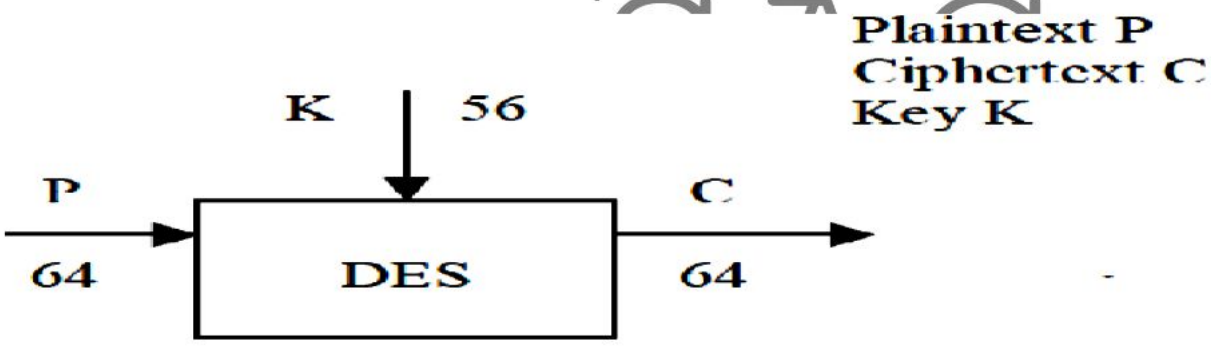
Whaling is a type of spear phishing that targets CEOs and other high-level executives. These are high-value targets since they often have unrestricted access to sensitive corporate data.

BEC (Business Email Compromise)

BEC attacks are designed to impersonate senior executives and trick employees, customers or vendors into wiring payments for goods or services to alternate bank accounts. According to the FBI's 2019 Internet Crime Report, **BEC scams were the most damaging** and effective type of cybercrime in 2019.

Data Encryption Standard:

- DES is a Symmetric-key algorithm for the encryption of electronic data.
- DES originated at IBM in 1977 & was adopted by the U.S Department of Defence. Now it is under the NIST (National Institute of Standard & Technology)
- Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key
- DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations.



Inner workings of DES:

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure (known as a Feistel network).

THE STRENGTH OF DES:

The Use of 56-Bit Keys:

- With a key length of 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16}. A brute-force attack appears impractical. Assuming that, on average, half the key space has to be searched, a single machine performing one DES encryption per microsecond would take more than a thousand years to break the cipher. Diffie and Hellman postulated that the technology existed to build a parallel machine with 1 millionencryptiondevices, eachof which could perform one encryption per microsecond. This would bring the average search time down to about 10 hours.

The Nature of the DES Algorithm:

- Possibilities of cryptanalysis is done by finding the characteristics of DES algorithm.
- Learning of S-Box logic is complex.
- Weakness of the S-boxes not been discovered.

Timing Attacks:

- A timing attack is one in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertexts.
- A timing attack exploitsthe fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.
- DES appears to be fairly resistant to a successful timing attack.

ADVANCED ENCRYPTION STANDARD(AES):

- The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001.
- AES is a block cipher intended to replace DES for commercial applications.
- It uses a 128-bit block size and a key size of 128, 192, or 256 bits.
- AES does not use a Feistel structure. Instead, each full round consists of four separate functions: byte substitution, permutation, arithmetic operations over a finite field, and XOR with a key.

Rijndael was designed to have the following characteristics:

- Resistance against all known attacks
- Speed and code compactness on a wide range of platforms
- Design simplicity

AES parameters:

Key size(words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round Key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

Inner Workings of a Round

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

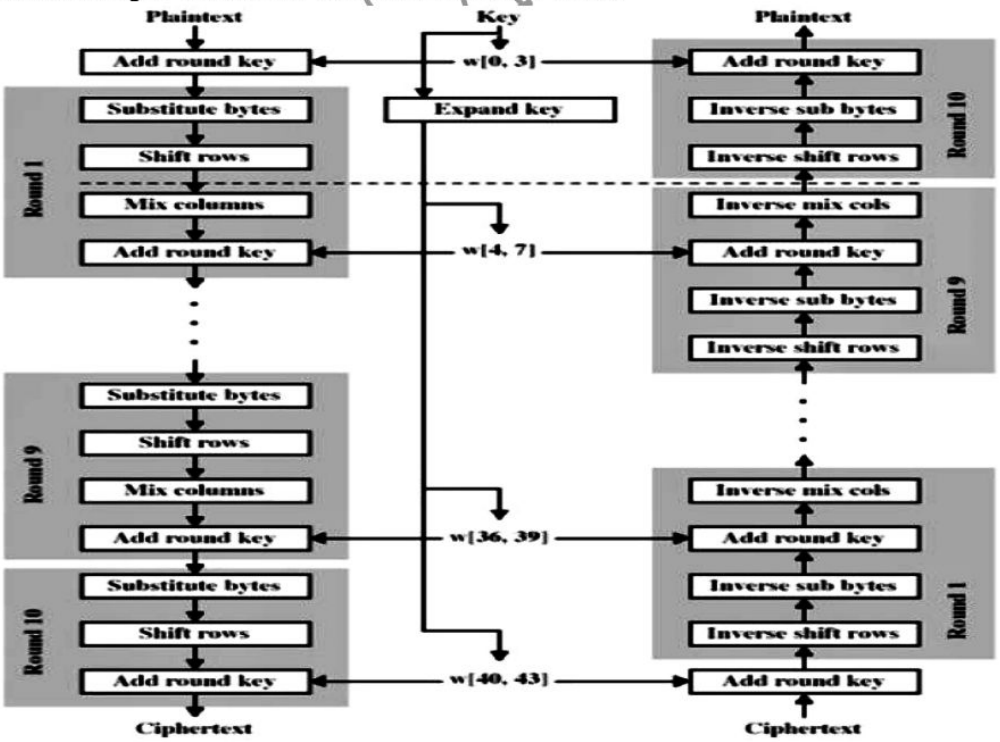


FIGURE:7.1 overall structure of the AES algorithm