What is Security?

- **Security** is a continuous process of protecting an object from attack.

Eg: person , organization like business, computer system or file, Distributed computer system.

- **Security** means preventing unauthorized access, use, alteration, and theft or physical damage to these resources.

Objectives

Objective of this chapter has:

1) To define three security goals.
2) To define security attacks that threaten security goals.
3) To define security services & how they are related to three security goals.
4) To define security mechanism to provide security services.

Basic terms

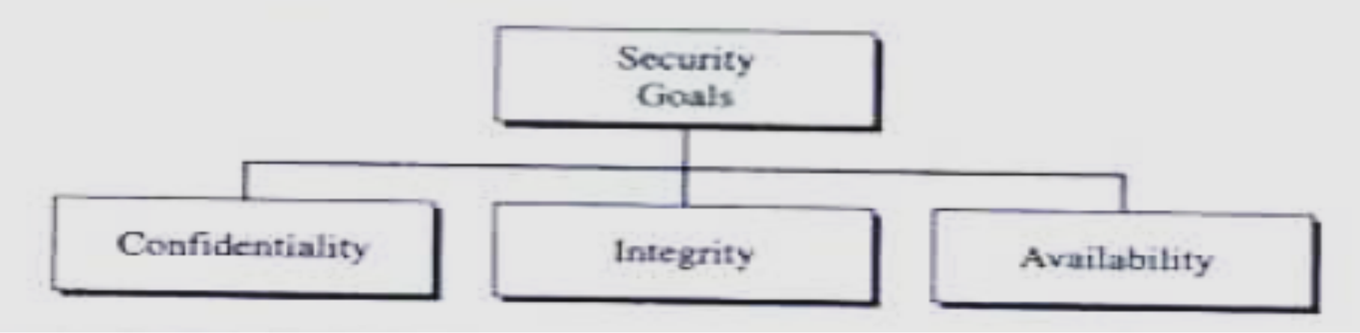
- **Unauthorized access** – An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.
- **Hacker** – Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.
- **Threat** – Is an action or event that might compromise the security.
- **Vulnerability** – It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.
- **Attack** – Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.
- **Antivirus or Antimalware** – Is a software that operates on different OS which is used to prevent from malicious software.
- **Social Engineering** – Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.
- **Virus** – It is a malicious software that installs on your computer without your consent for a bad purpose.
- **Firewall** – It is a software or hardware which is used to filter network traffic based on rules.

Security Goals

- Security defined the three elements:

1) **confidentiality**-: To prevent unauthorized disclosure of information to third parties.
2) **Integrity**-: To prevent unauthorized modification of resources.
3) **Availability**-: To prevent unauthorized withholding of system resources from those who need them when they need them. (means resource should be available to authorized parties at all times)

fig : Security Goals

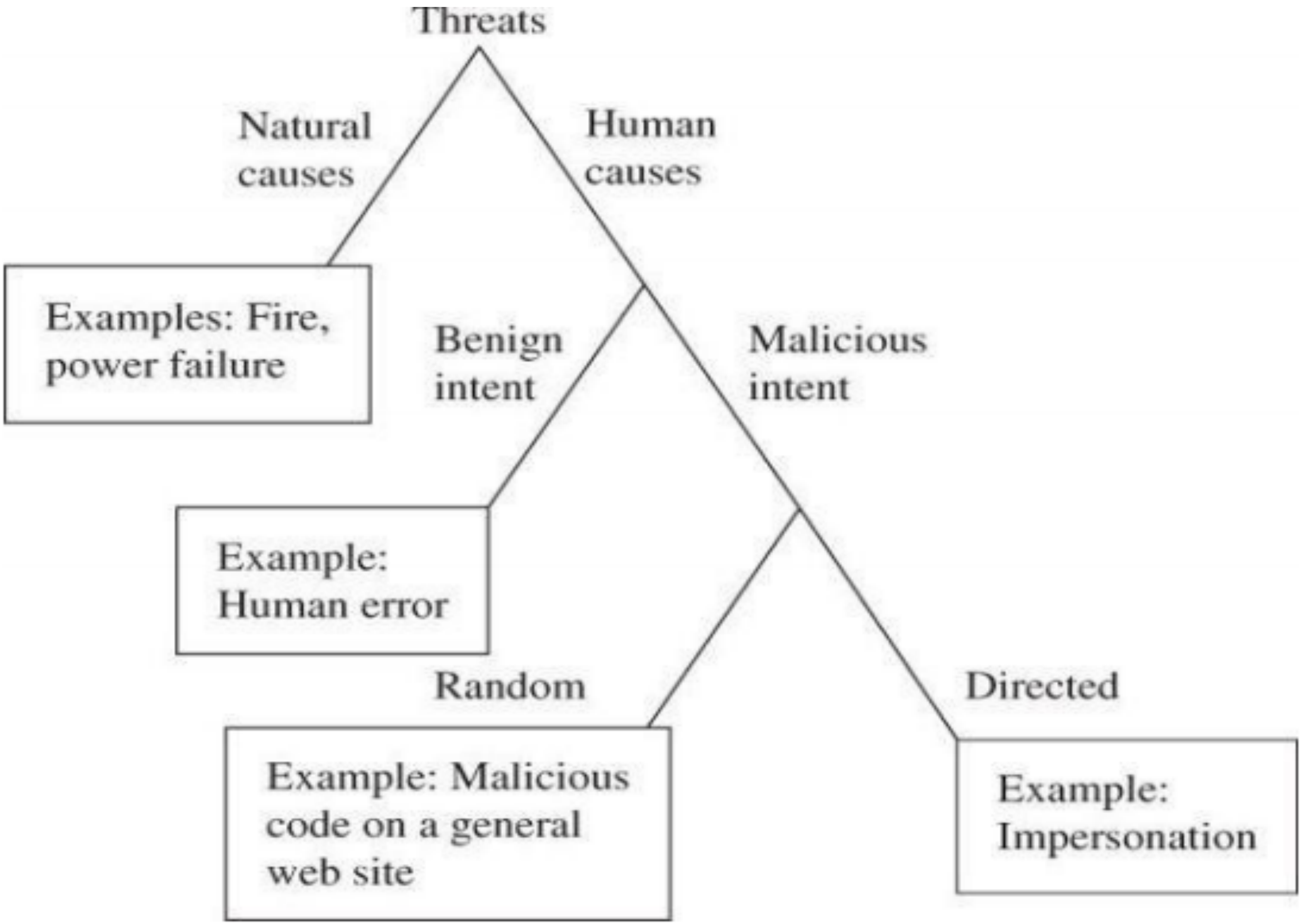


- Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability).

The Vulnerability–Threat–Control Paradigm

- A vulnerability is a weakness in the system, for example, procedures, design, or implementation, that might be exploited to cause loss or harm.
- For example, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

- A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.
- A control is an action, device, procedure, or technique that removes or reduces a vulnerability
- A threat is blocked by control of a vulnerability.


Threats

Natural causes

Examples: Fire, power failure

Human causes

Benign intent

Example: Human error

Malicious intent

Random

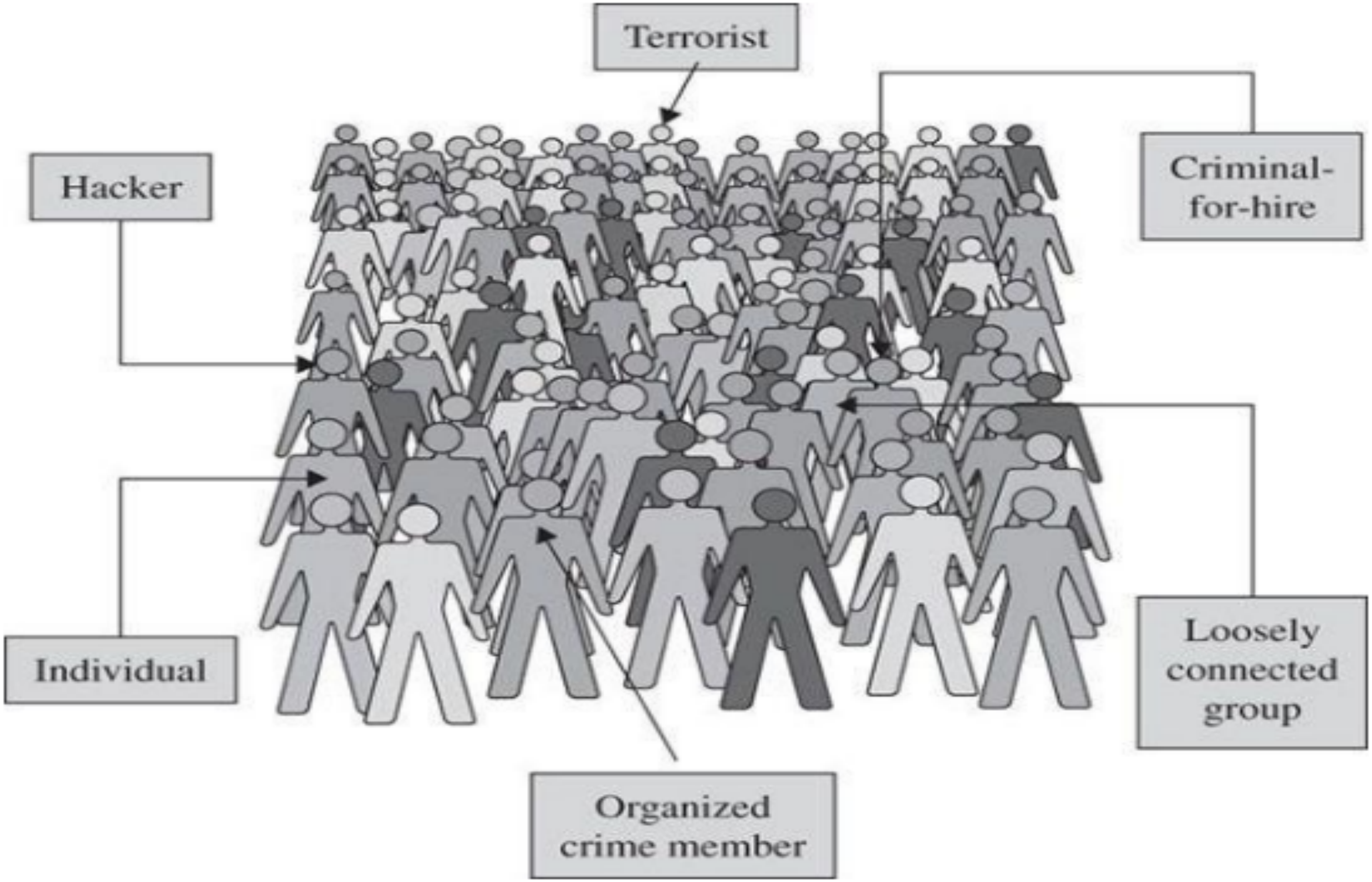
Example: Malicious code on a general web site

Directed

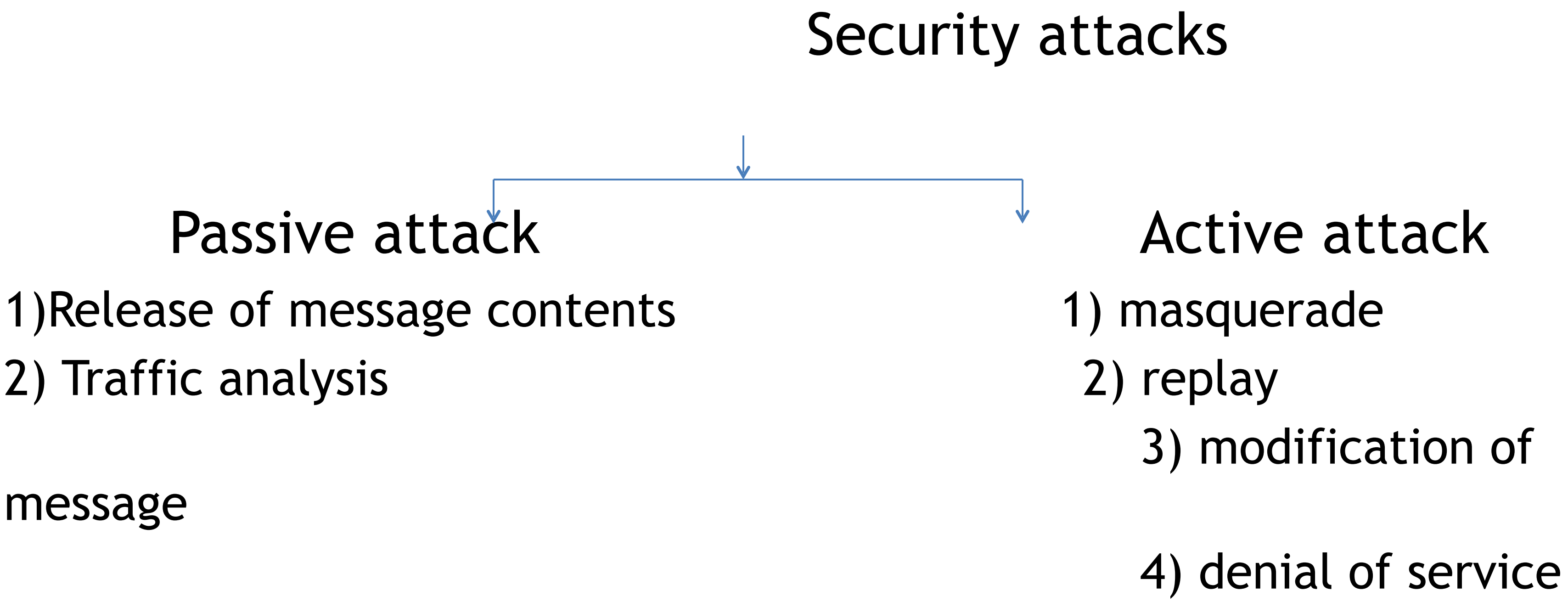
Example: Impersonation

Impersonation::an act of pretending to be another person for the purpose of fraud.

Computer criminals



Security Attacks



Security attacks

Passive attack

1)Release of message contents

2) Traffic analysis

Active attack

1) masquerade

2) replay

3) modification of

message

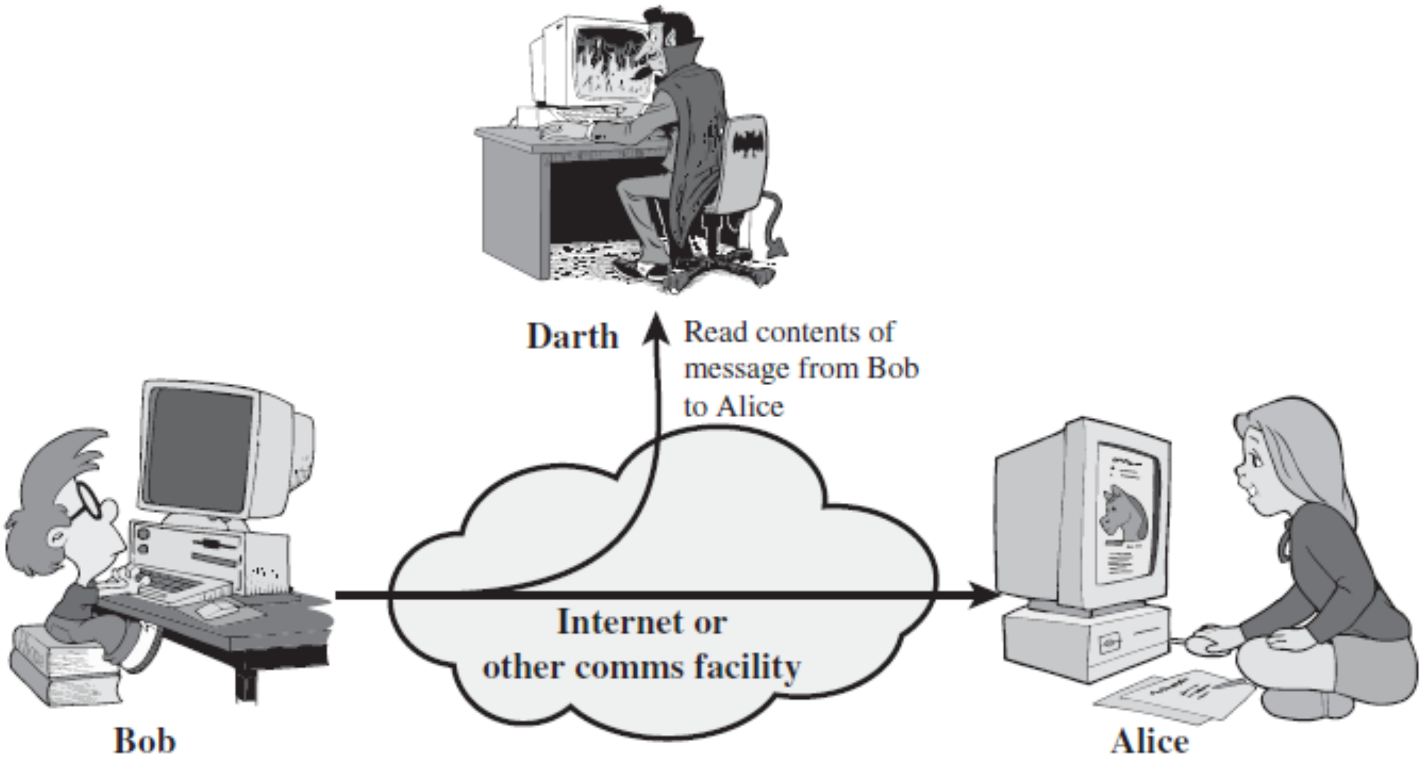
4) denial of service

Passive Attack

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

Types of Passive Attack :

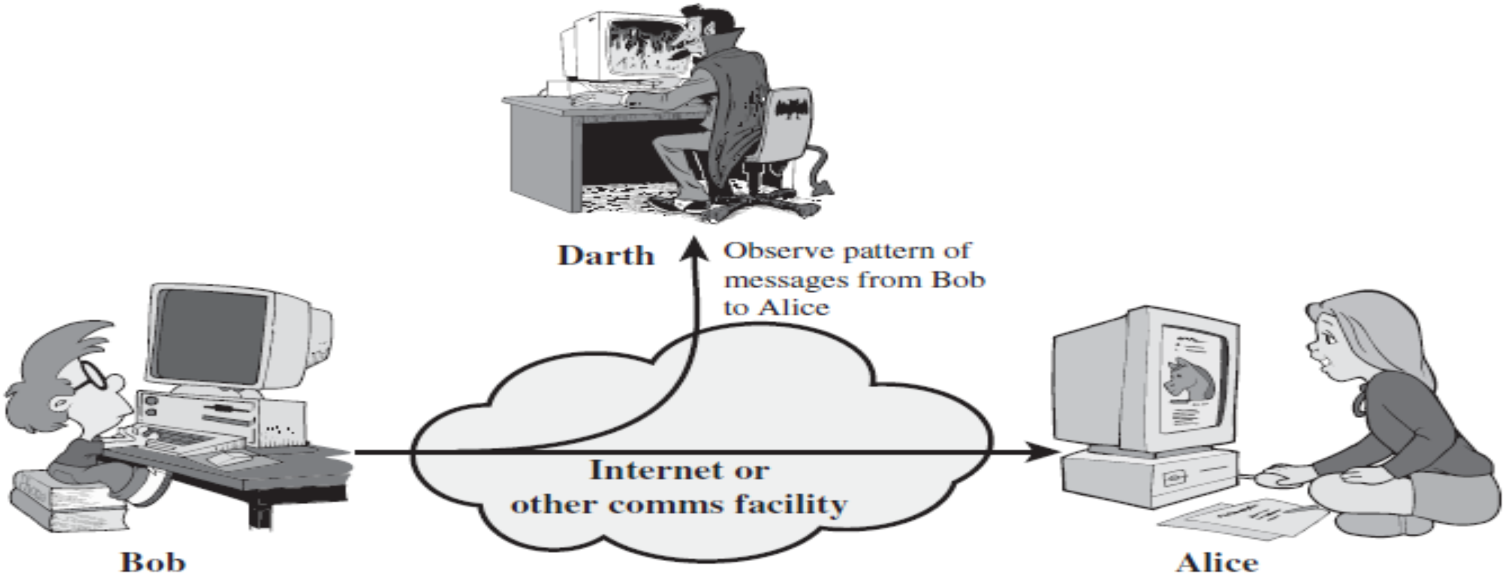
1) Release of message -: a telephone conversation, an electronic mail message, transferred files may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmission.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

- Traffic analysis: eg wireshark

2) Traffic Analysis-: we had a way of masking the contents of message or other information traffic so that opponents could not extract the information from the message.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

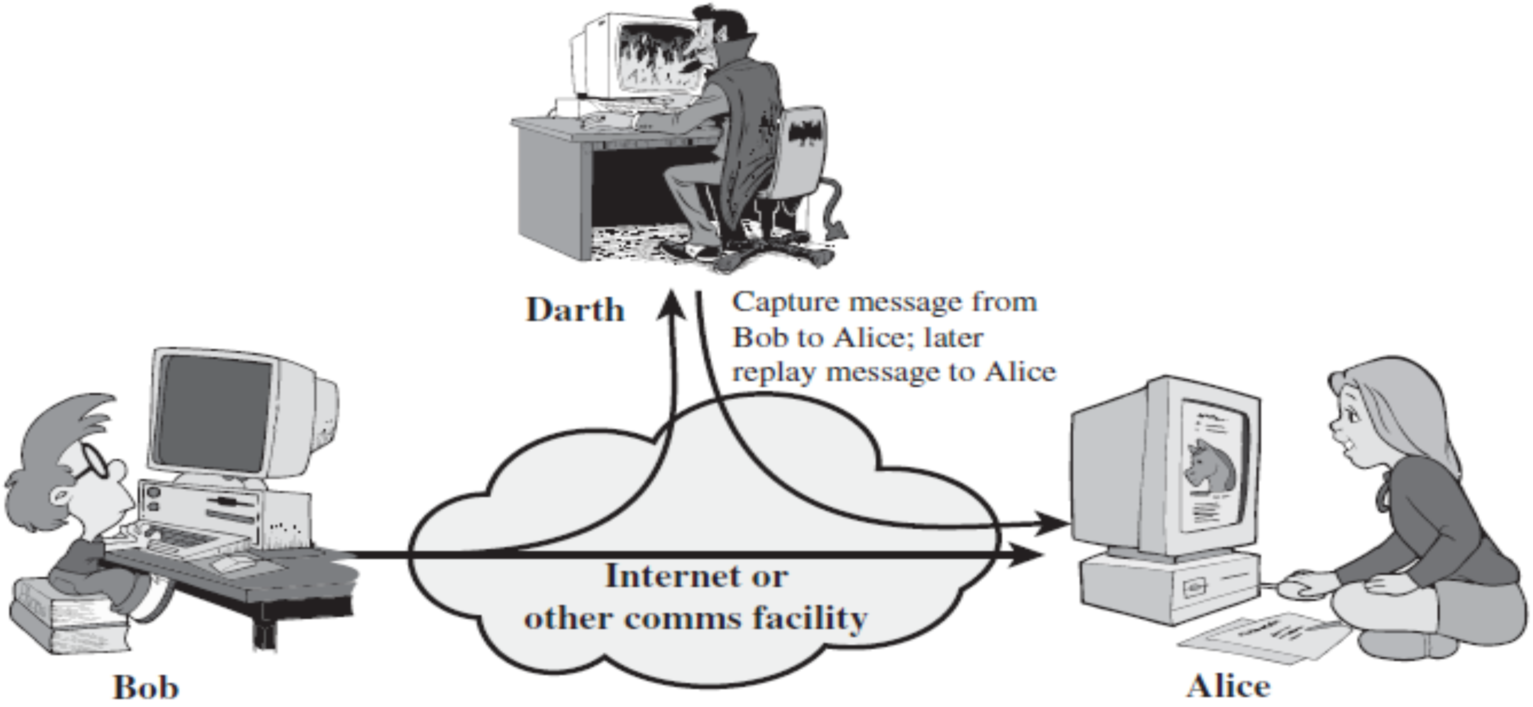
- Passive attacks are very difficult to detect.
- Neither the sender nor receiver is aware that a third party has read the message or observed the traffic pattern.
- It is feasible to prevent the success of these attack. Usually by means of encryption.
- Emphasis in dealing with passive attack is on prevention rather than detection.

Active Attacks-:

- Active Attack-: an active attack attempts to alter system resources or affect their operation

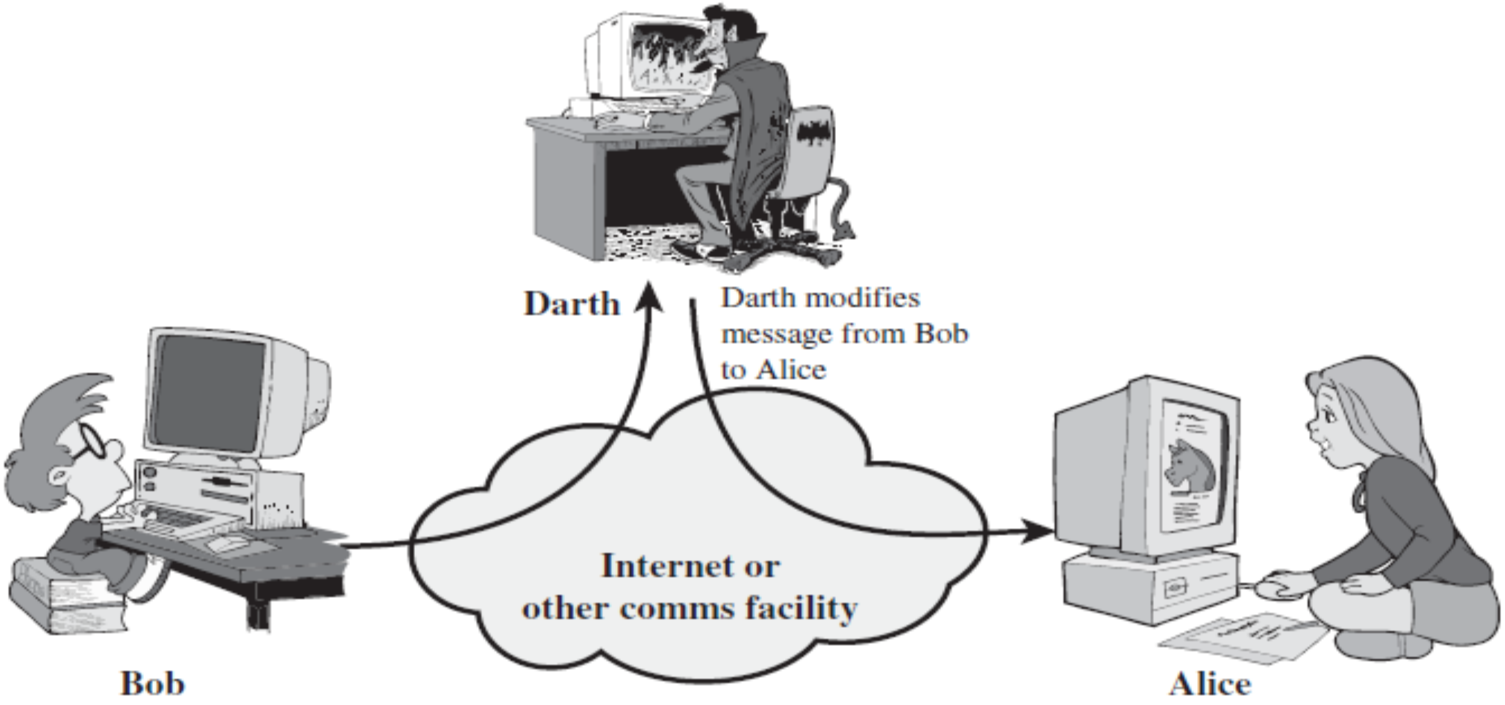
1. A masquerade-: takes place when one entity pretends to be a different entity.

2. Replay-: The attacker obtains a copy of massage sent by a user & later tries to replay it.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

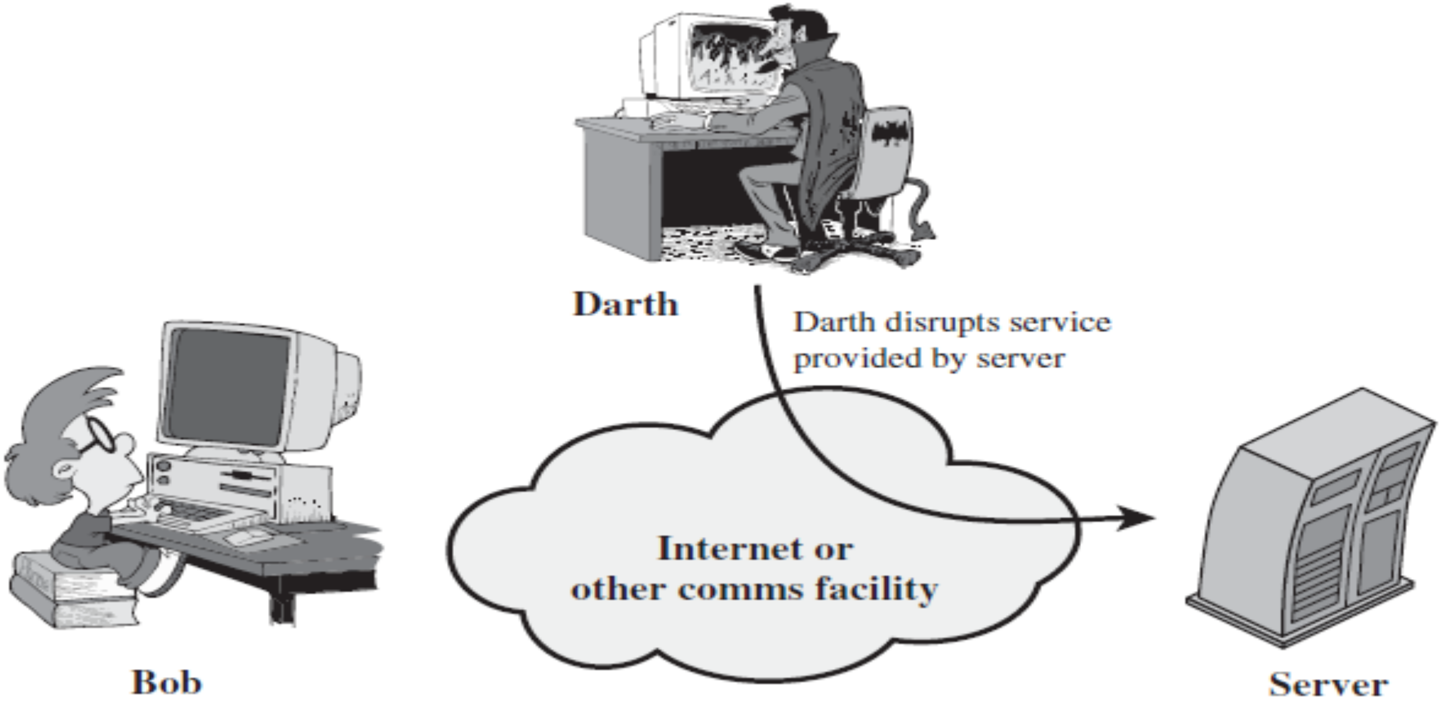
(b) Replay

3. Modification of Messages-: Means that some portion of a legitimate message is altered or that messages are delayed or recorded to produce an unauthorized effect.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

4. The Denial of Service-: Makes an attempt to prevent legitimate users from accessing some services, which they are eligible for.


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

5. Repudiation-: this type of attack is different from others because it is performed by one of the two parties in the communication the sender or receiver.

- the sender of the message might later deny that she has sent the message or the receiver of the message might later deny that he has received message.

Fig : Attacks with relation to security goals

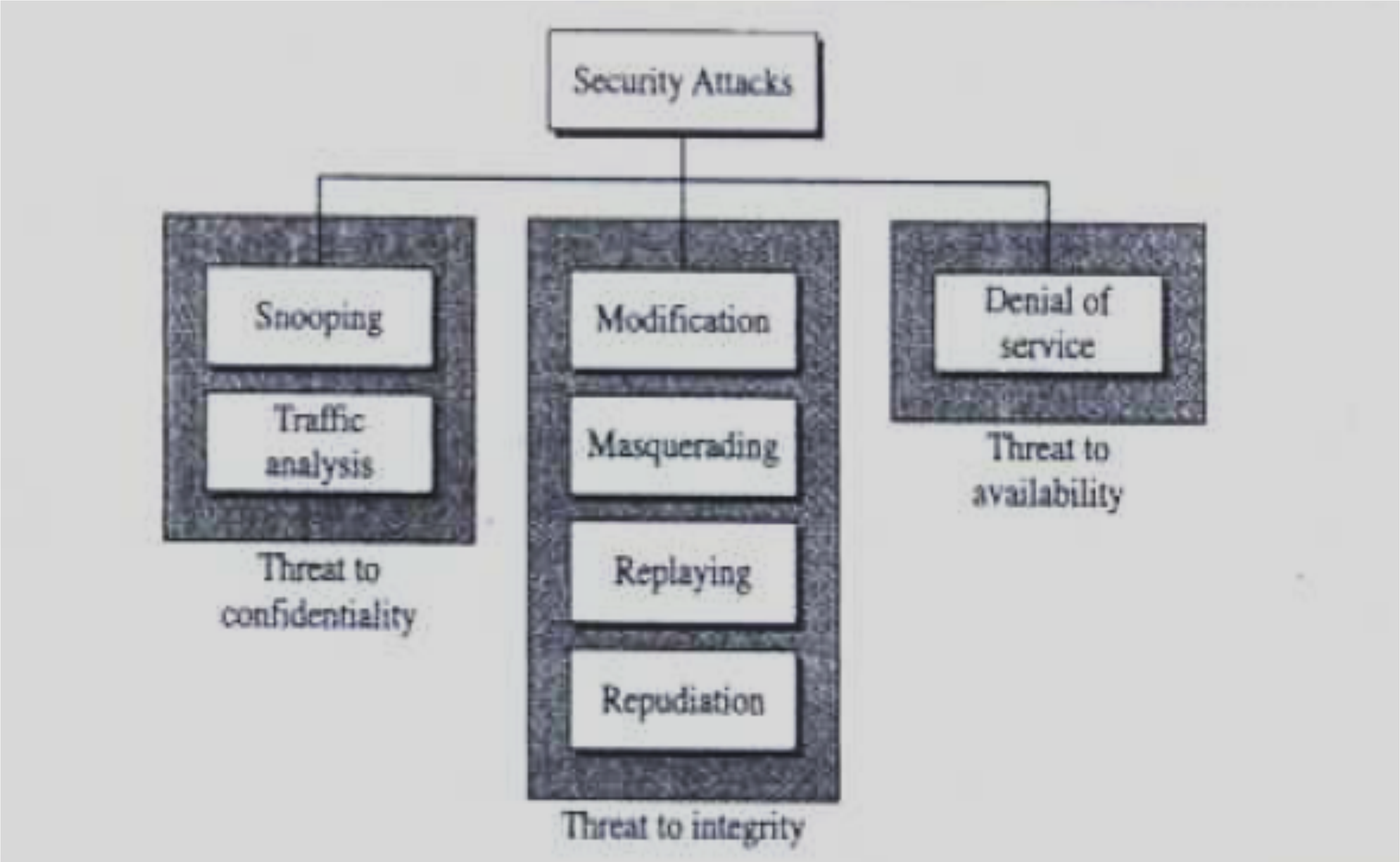
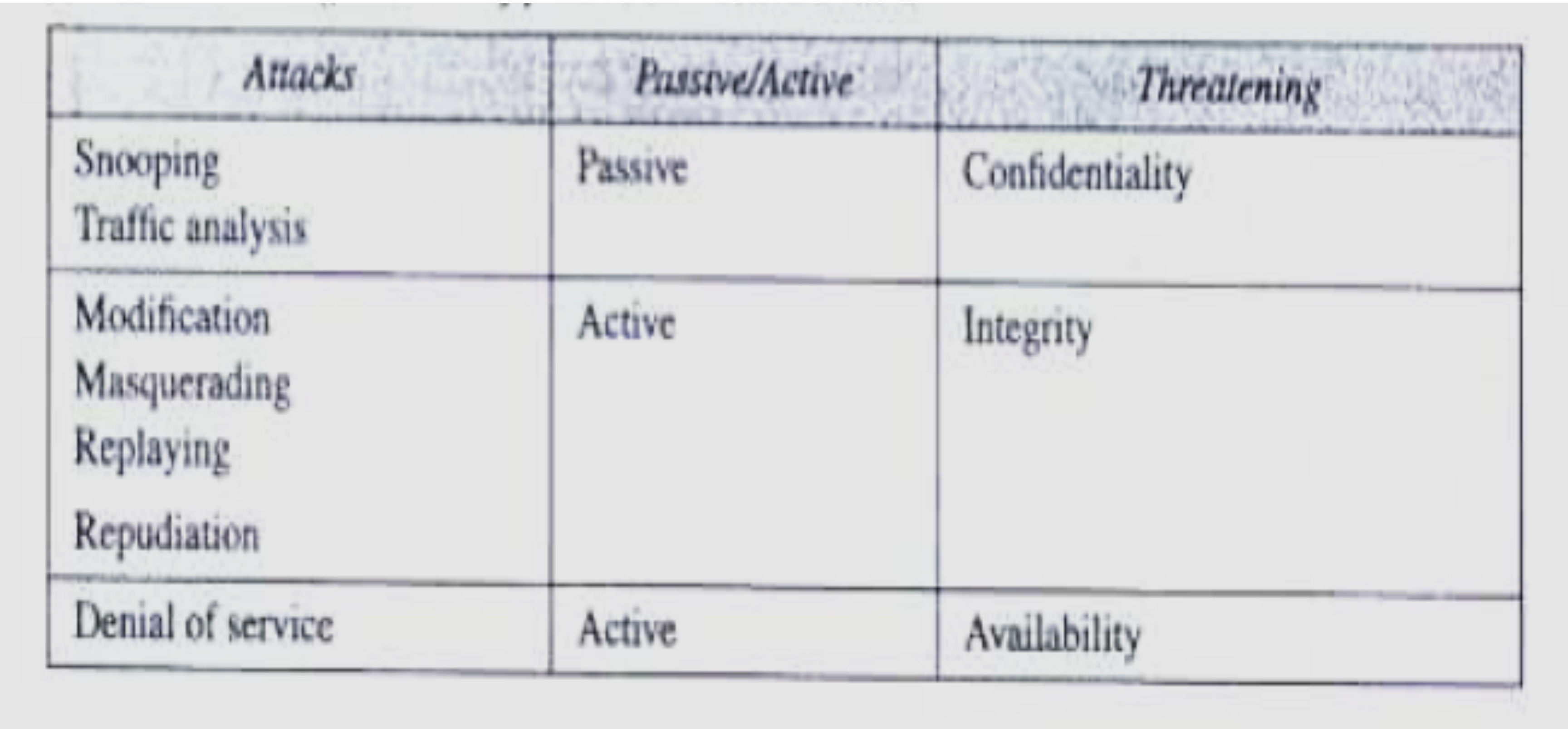


Fig : Classification of Passive & Active attack



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Security Services

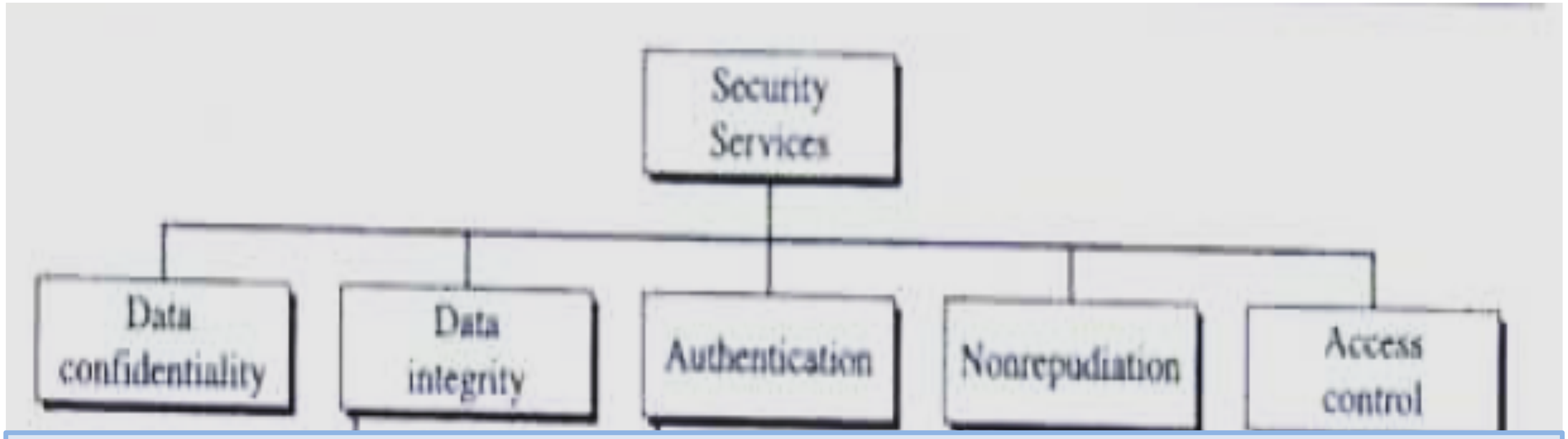
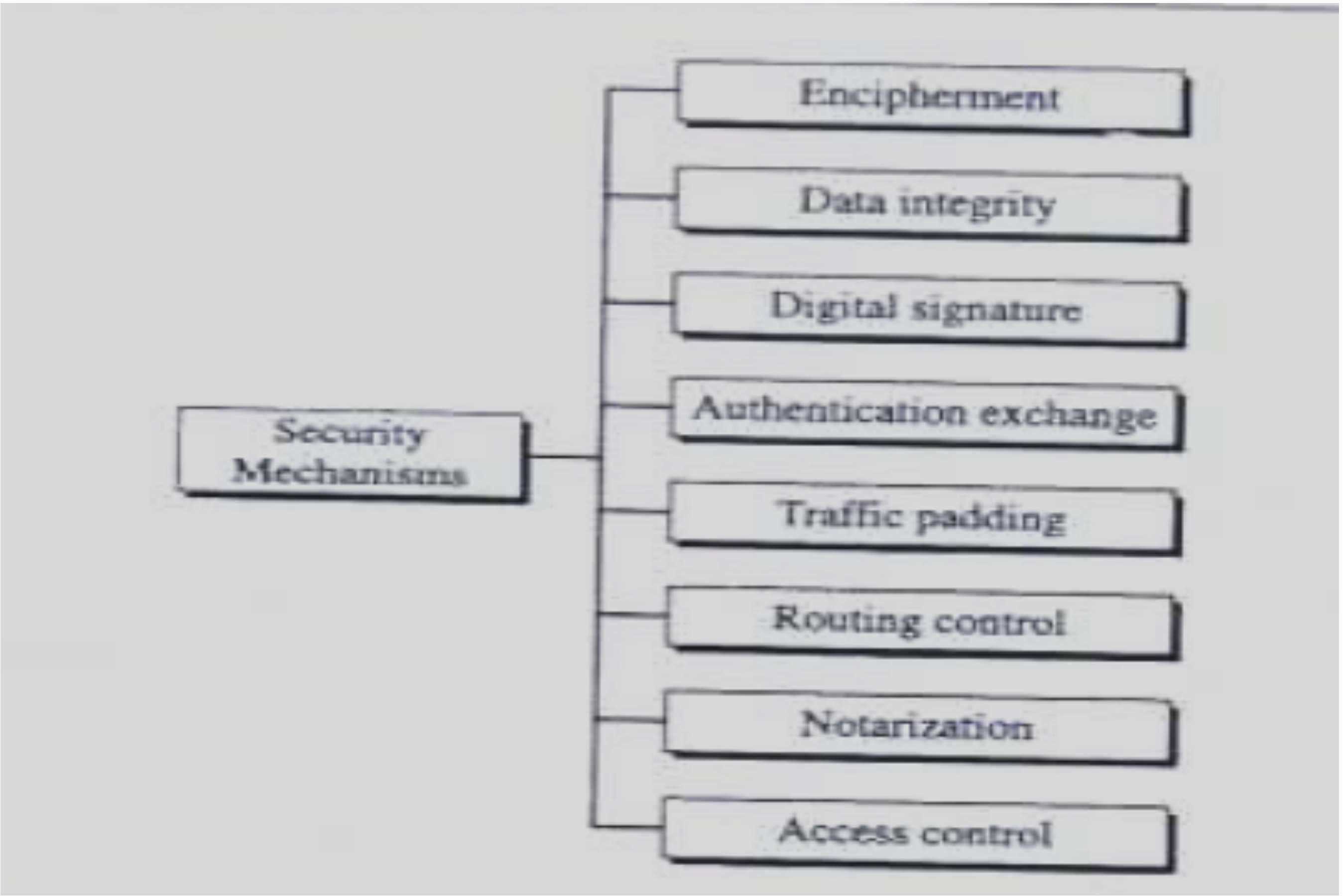


Fig-: Security Services

Fig : Security Mechanism



Security Mechanism

1. Encipherment-: hiding or covering data can provide confidentiality. Two technique used for encipherment is cryptography, stegenography

(Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Steganography requires two files: one is the message which has to be hidden, the other is the cover file which is used to hide the date/message.)

(In **cryptography**, one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key.)

2. Data Integrity-:added short check value, the receiver receives the data and the check value, he creates a new check value from received data and compares the newly created check value with the one received. If two check value are same that means integrity of data has been preserved.
3. Digital Signature-: DS is a mean by which the sender can electronically sign the data and receiver can electronically verify the signature.
4. Authentication Exchange-: Two entities exchange some message to provide their identity to each other.

5. Traffic Padding-: Inserting some bit of data into the data traffic to avoid the adversary's attempt to use the traffic analysis.

6. Routing control-: Selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping.

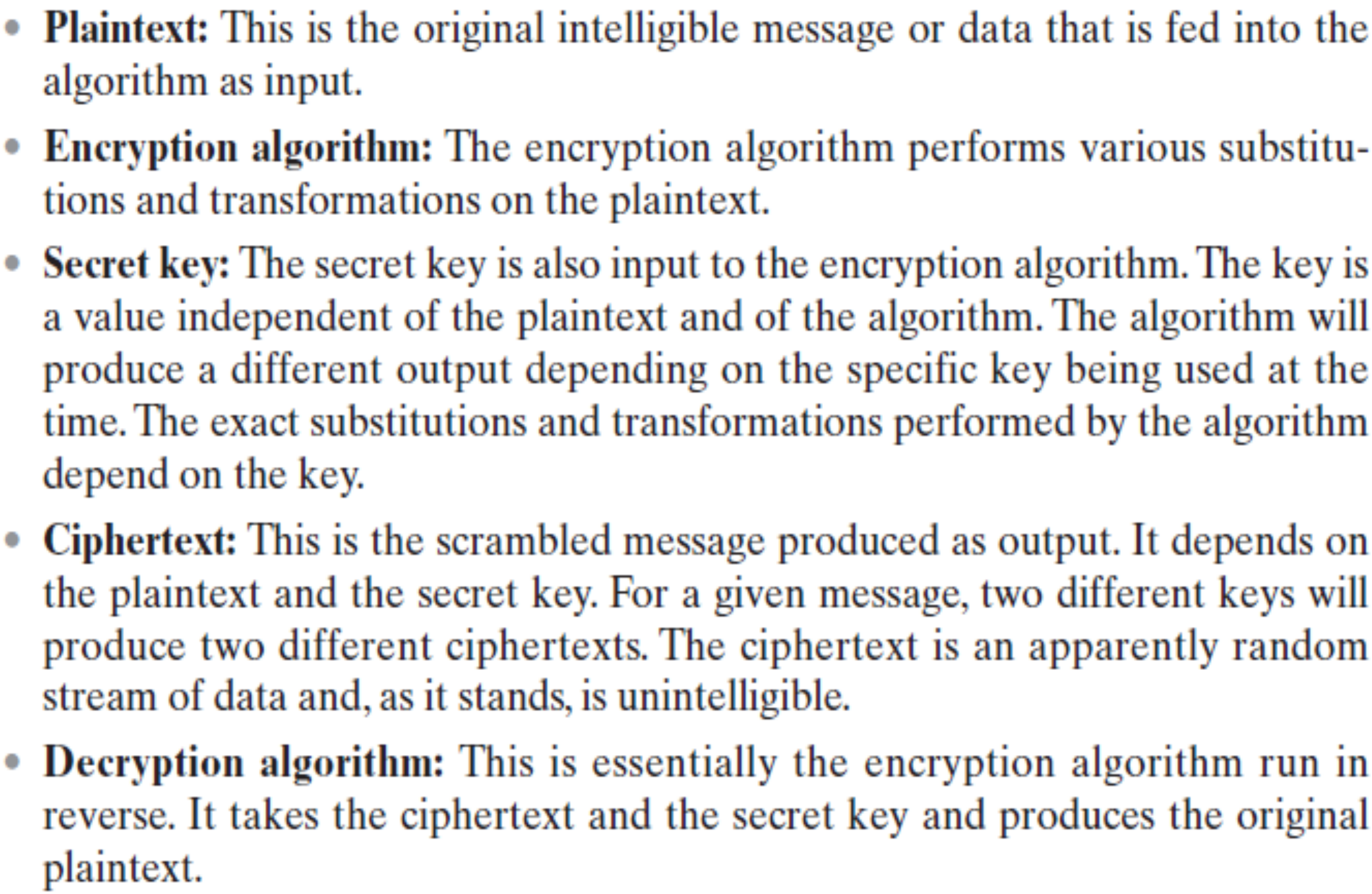
7. Notarization-: means selecting a third trusted party to control the communication between two entities.

8. Access control-: access control use methods to prove that a user has access right to the data or resources owned by a system. Eg-: passwords & PINs

General model for Symmetric Encryption

- Symmetric Encryption is a form of cryptography in which encryption & decryption are performed using the same key.
- It is also known as **conventional encryption** or **single key encryption or** **private key cryptosystem.**

Symmetric cipher model



- **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.

Symmetric key encipherment uses a single key for both encryption & decryption. In addition the encryption & decryption algorithms are inverse of each other.

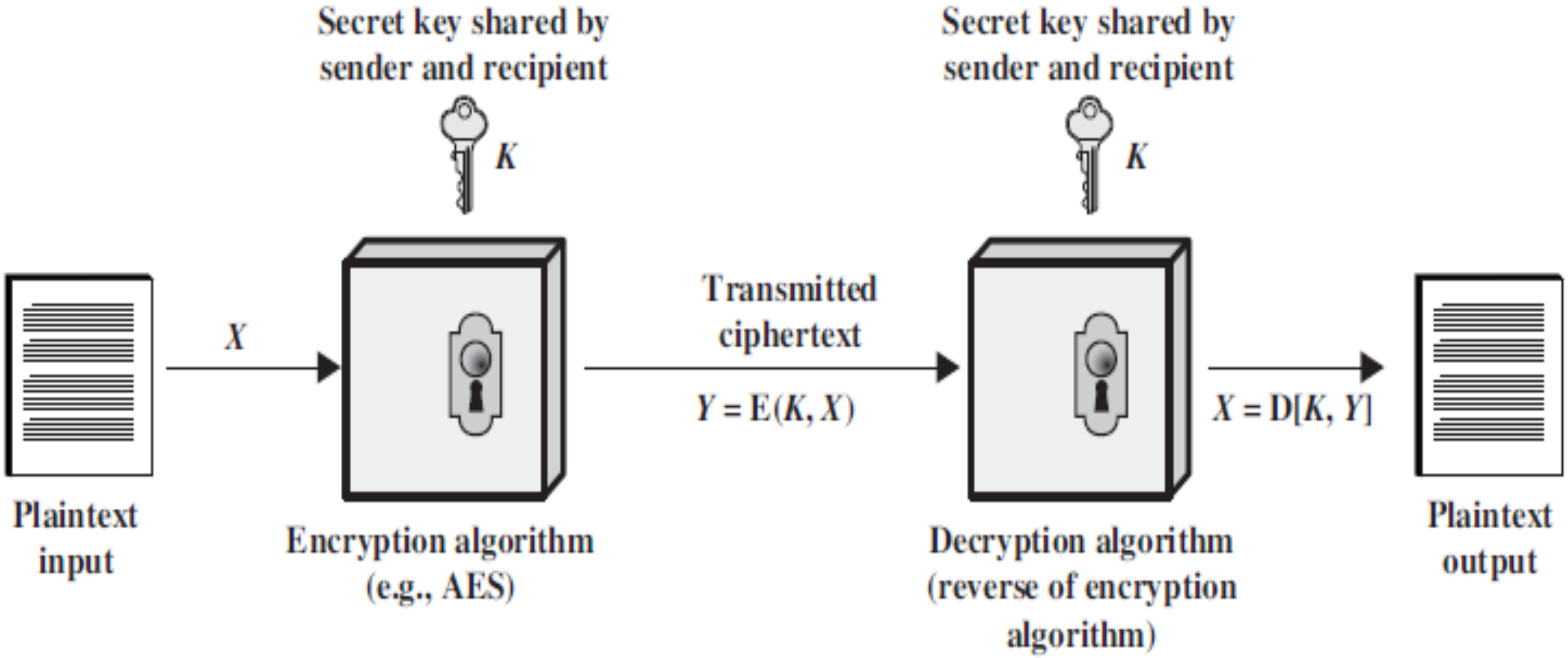
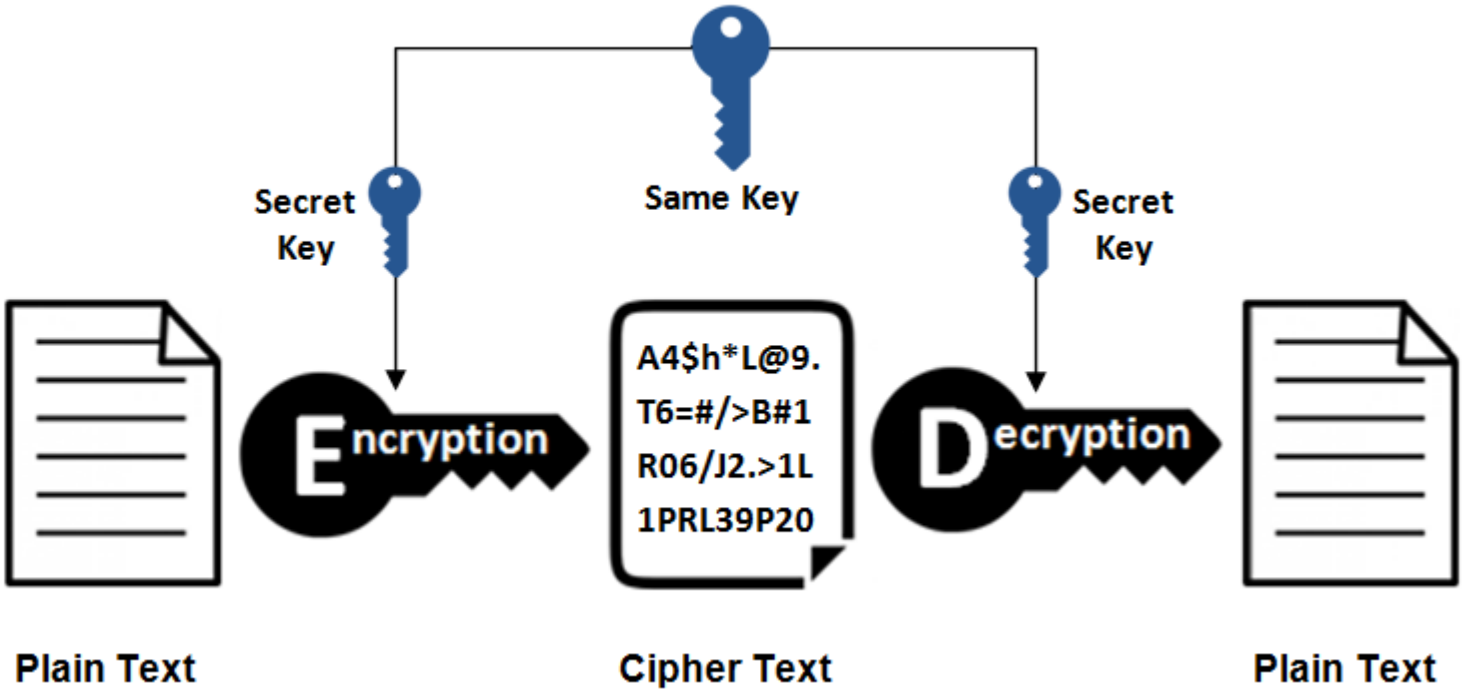

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

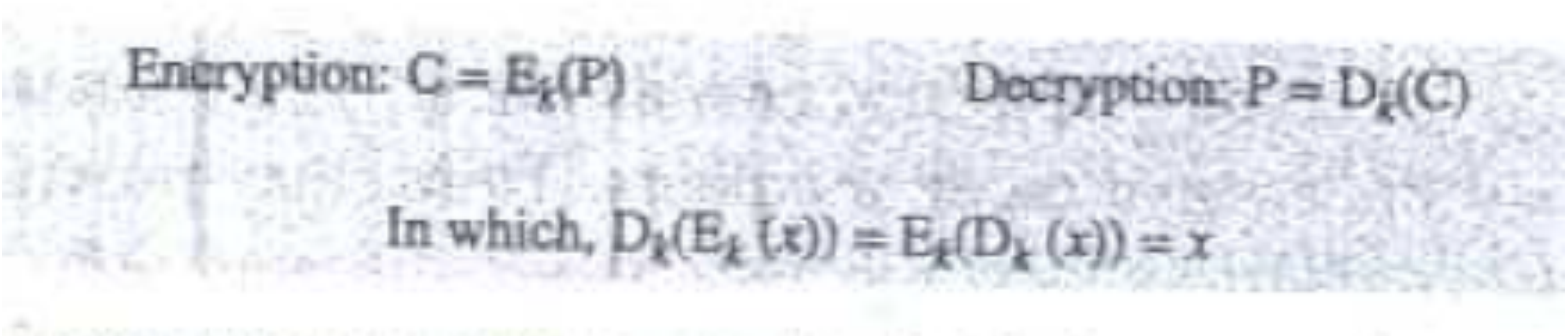
Symmetric Encryption



Requirements for secure use of conventional encryption

- We need a strong encryption algorithm so that the opponent should be unable to decrypt CT or discover the key.
- Sender and receiver must have obtained copies of the secret key in a secure fashion & must keep the key secure.

- If p is the plain text, c is the cipher text, k is the key, the encryption alg$E_k(x)$thm creates the cipher text from the plain text . Decr$D_k(x)$ption algorithm creates the plain text from cipher text.
- We assume that $E_k(x)$ $D_k(x)$ are inverse of each other. They cancel the effect of

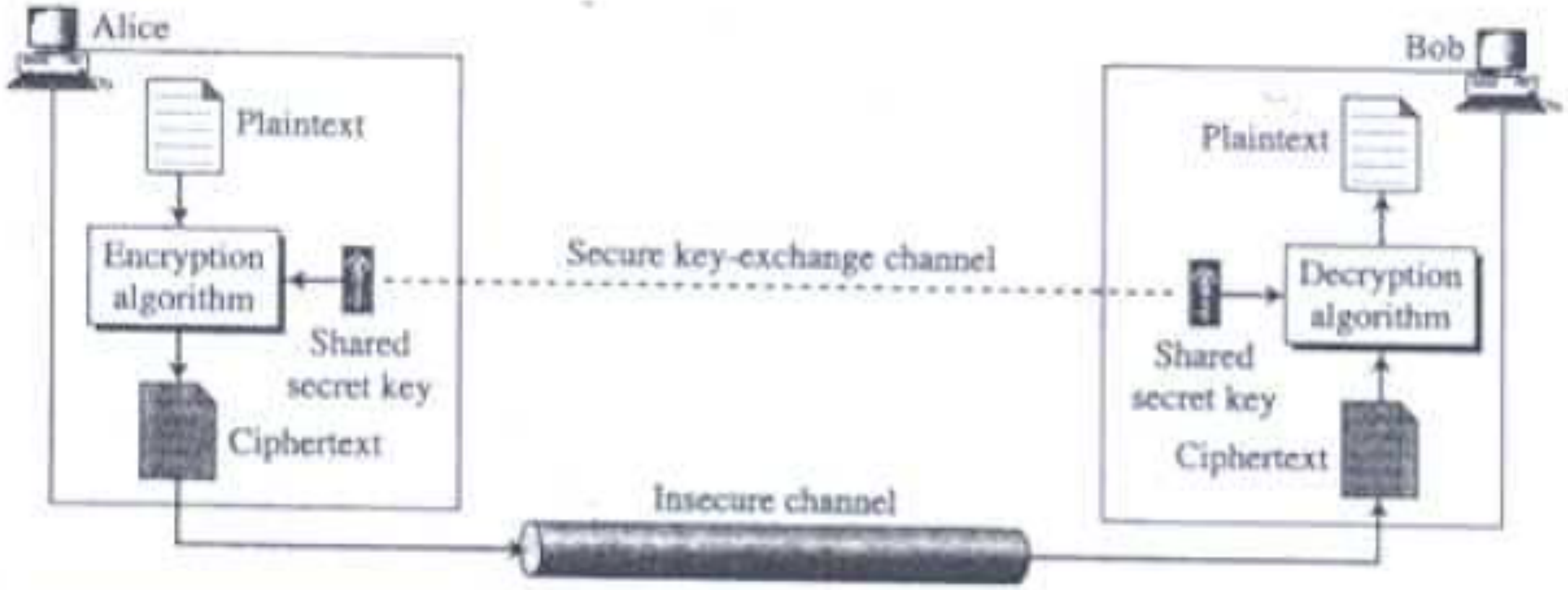


Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

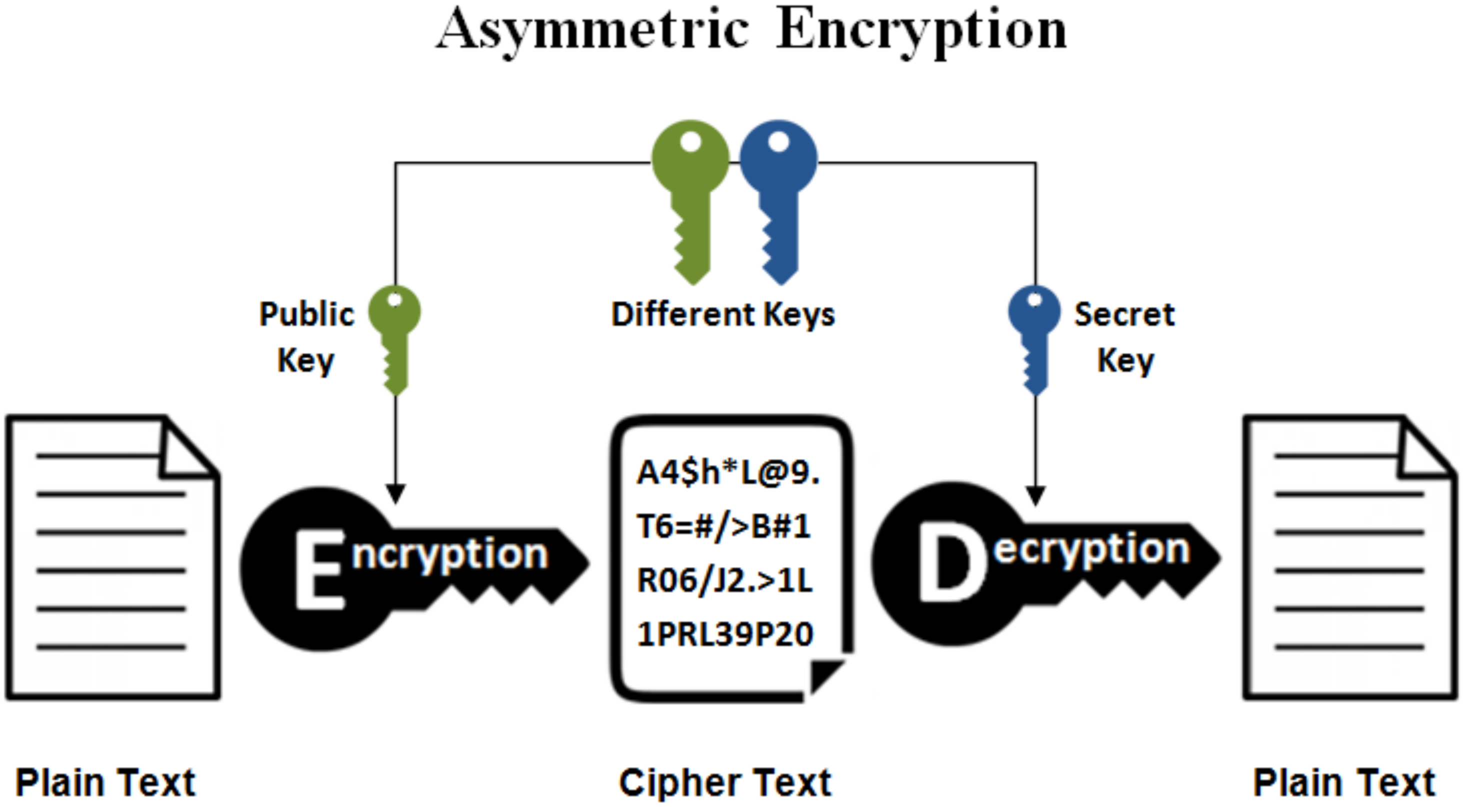
The plain text created by bob is same as the one originated by alice.

Figure 3.1 *General idea of symmetric-key cipher*



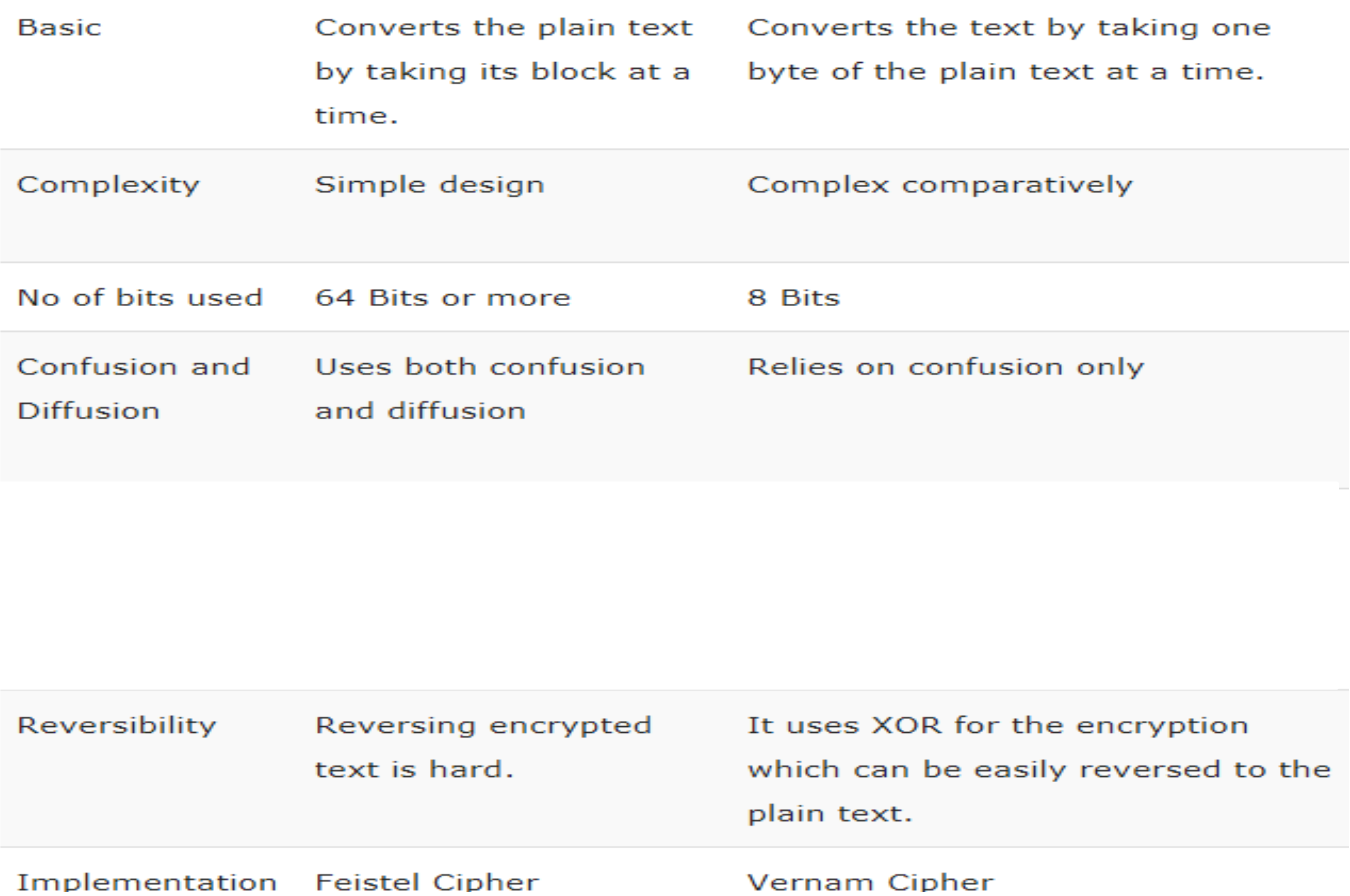
Deffie Hellman key exchange algo

ASYMMETRIC ENCRYPTION



- A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.
- A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.
- Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes RSA, etc

RSA ALGO



	Block cipher	stream cipher
Basic	Converts the plain text by taking its block at a time.	Converts the text by taking one byte of the plain text at a time.
Complexity	Simple design	Complex comparatively
No of bits used	64 Bits or more	8 Bits
Confusion and Diffusion	Uses both confusion and diffusion	Relies on confusion only
Reversibility	Reversing encrypted text is hard.	It uses XOR for the encryption which can be easily reversed to the plain text.
Implementation	Feistel Cipher	Vernam Cipher

Shannon introduced confusion and diffusion

- Diffusion-: the idea of diffusion is to hide the relationship between the CT & PT. this will frustrate the adversary who uses CT statics to find the PT.
- Diffusion implies that each symbol (character or bit) in the CT is dependent on some or all symbols in the PT.
- In other word if a single symbol in the plaintext is changed , several or all symbols in the cipher text will also be change

Confusion-:

- The idea of confusion is to hide the relationship between the CT & the key.
- This will frustrate the adversary who tries to use the CT to find the key. In other words if a single bit in the key is changed most or all bits in CT will also be changed.

confusion and diffusion

- The terms confusion and diffusion are the properties for making a secure cipher. Both Confusion and diffusion are used to prevent the original message.
- Confusion is used for creating clueless ciphertext while diffusion is used for increasing the redundancy of the plaintext over the major part of the ciphertext to make it obscure.

Tools Used to Encrypt Documents

- **Axcrypt** – It is one of the best opensource encryption file softwares. It can be used in Windows OS, Mac OS and Linux as well. This software can be downloaded from – http://www.axantum.com/AxCrypt/Downloads.aspx
- **GnuPG** – This is an opensource software again and it can be integrated with other softwares too (like email). It can be downloaded from – https://www.gnupg.org/download/index.html
- **Windows BitLocker** – It is a Windows integrated tool and its main functions is to secure and encrypt all the hard disk volumes.
- **FileVault** – It is a Mac OS integrated tool and it secures as well as encrypts all the hard disk volume.

cryptanalysis

- Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them.

- For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it; cryptanalysts also target secure hashing, digital signatures and other cryptographic algorithms.

- Cryptosystem:

➢ A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**.

➢ Typically, a **cryptosystem** consists of three algorithms: one for key generation, one for encryption, and one for decryption.

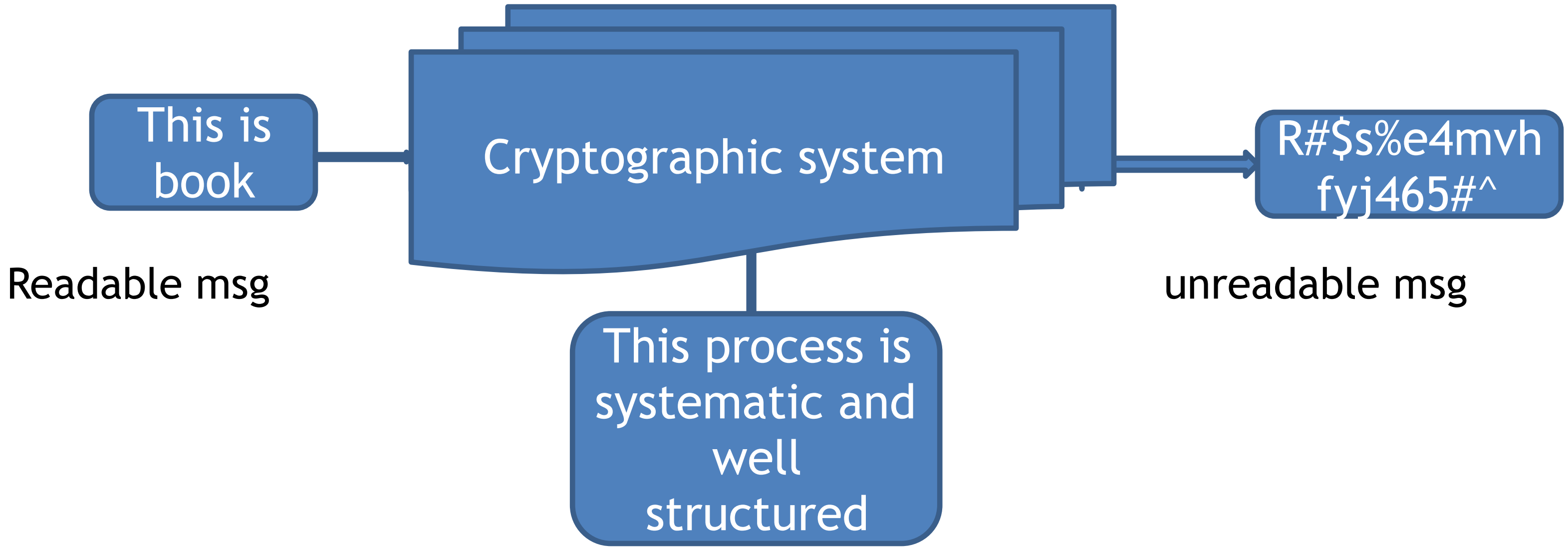
- Types of Cryptosystems
- Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –
- Symmetric Key Encryption
- Asymmetric Key Encryption

Difference Between Cryptanalysis & cryptography

cryptography	Cryptanalysis
The art and science of keeping massage secure is cryptography	The art and science of breaking cipher is cryptanalysis
It creates the secret code	It breaks the secret code

Cryptography

Cryptography is the art & science of achieving security by encoding massage to make them non-readable.



This is book

Readable msg

Cryptographic system

R#$s%e4mvh fyj465#^

unreadable msg

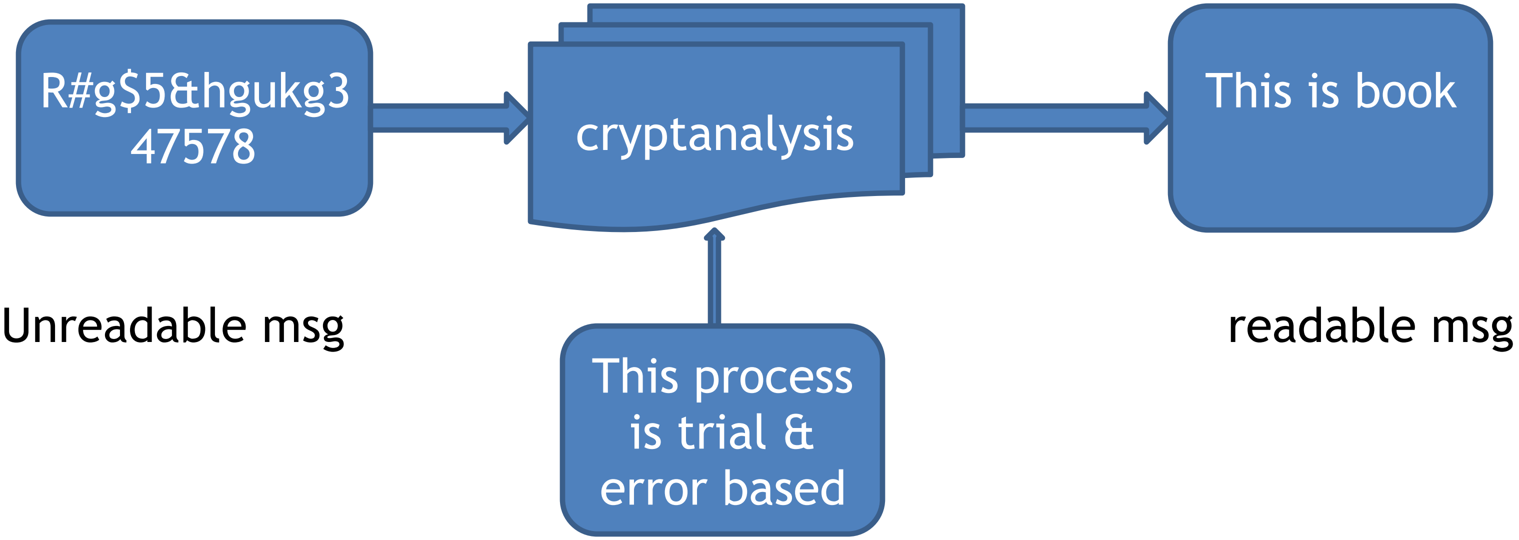
This process is systematic and well structured

Fig: cryptographic system

cryptanalysis

- Cryptanalysis is the technique of decoding massage from a nonreadable format back to readable format without knowing how they were initially converted from readable format to non readable format.

In other word it is like breaking code



R#g$5&hgukg3 47578

cryptanalysis

This is book

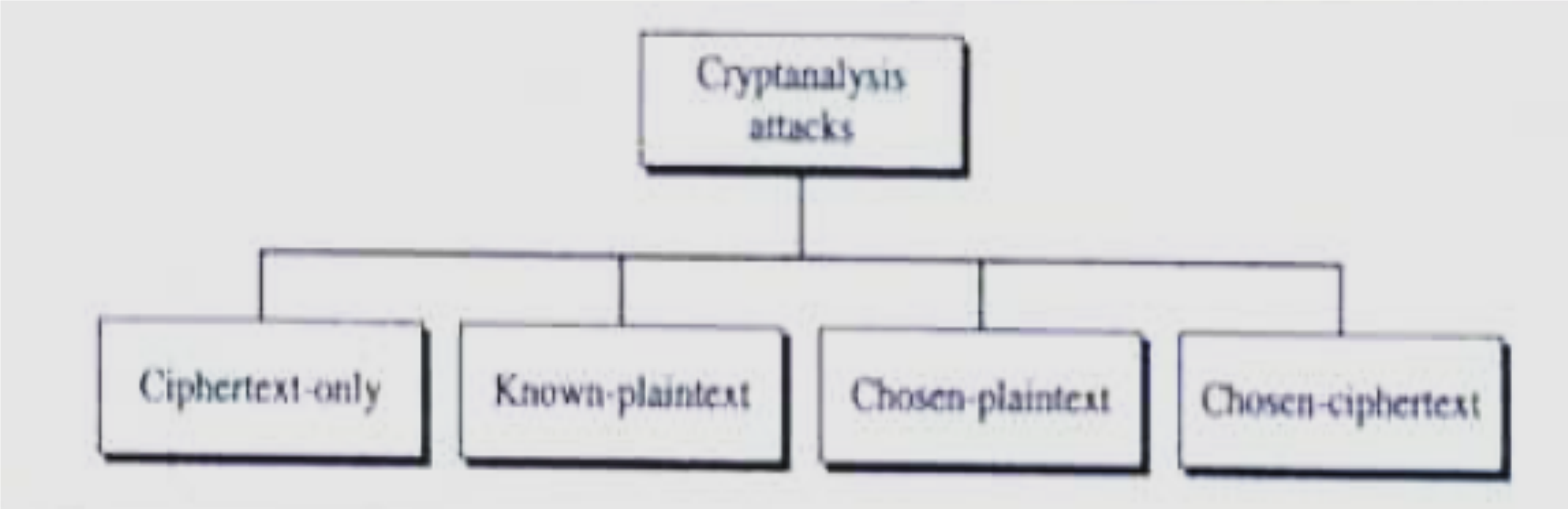
Unreadable msg

readable msg

This process is trial & error based

Cryptographic Attacks

- The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.
- Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as *broken* or *compromised*.
- Based on the methodology used, attacks on cryptosystems are categorized as follows –


Cryptanalysis attacks
Ciphertext-only
Known-plaintext
Chosen-plaintext
Chosen-ciphertext

- **Ciphertext Only Attacks (COA)** − In this method, the attacker has access to a set of ciphertext(s).
- He does not have access to corresponding plaintext.
- COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext.
- Occasionally, the encryption key can be determined from this attack.
- Modern cryptosystems are guarded against ciphertext-only attacks.

Various method can be used under cipher text only attack

A) Brute force attack-: in brute force method or exhaustive key search method the attacker eve tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained to present this type of attack. The no. of possible key must be very large. If the key is 8 bits long, then the number of possible keys is 2^8 = 256. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

B) Statistical attack -: the cryptanalysis can benefit from same inherent characteristic of the plaintext language to launch a statistical attack.

EXAMPL-: We know that the letter E is the most frequently used letter in english text. The cryptanalyst finds the mostly used character in the cipher text & assume that the corresponding plain text character is E. After finding a few pairs, the analyst can find the key & use it to decrypt the massage to prevent type of attack the cipher should hide the characteristic of the language.

- **Known Plaintext Attack (KPA)** – In a *known plaintext attack*, the analyst may have access to some or all of the plaintext of the ciphertext; the analyst's goal in this case is to discover the key used to encrypt the message and decrypt the message. Once the key is discovered, an attacker can decrypt all messages that had been encrypted using that key. Linear cryptanalysis is a type of known plaintext attack

- **Chosen Plaintext Attack (CPA)** − In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is *differential cryptanalysis* applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.
- The analyst can encrypt the chosen plaintext with the targeted algorithm to derive information about the key.

4. Chosen chipertext attack

- A **chosen-ciphertext attack (CCA)** is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

- **Dictionary Attack** – This attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

- Man in the middle
- Side channel attack , etc