NRCM
your roots to success...

NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana State, India

Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

DEPARTMENT OF CSE -CYBER SECURITY

NETWORK SECURITY AND CRYPTOGRAPHY (NSC) - 23CY501

III B. Tech I Semester (NR23)

Prepared by

Mr. K. SRINIVASA RAO
Assit. Prof.

UNIT-1

UNIT - I

Security Concepts:

- Introduction,
- The need for security,
- Security approaches,
- Principles of security,
- Types of Security attacks,
- Security services,
- Security Mechanisms,

A model for Network Security Cryptography Concepts and Techniques / Cryptographic Techniques:

- Introduction,
- Plain Text And Cipher Text,
- Substitution Techniques,
- Transposition Techniques,
- Encryption And Decryption,
- Symmetric And Asymmetric Key Cryptography,
- Steganography,
- Key Range And Key Size,
- Possible Types Of Attacks.

Security Concepts:

- Introduction,
- The need for security,
- Security approaches,
- Principles of security,
- Types of Security attacks,
- Security services,
- Security Mechanisms,

SECURITY CONCEPTS

INTRODUCTION

Computer data often **travels** from **one computer to another**, **leaving** the safety of its **protected physical surroundings**. Once the data is out of hand, people with **bad intention could modify** or **forge your data**, either for amusement or for their own benefit. **Cryptography** can **reformat** and **transform our data**, making it safer on its trip between computers. The technology is based on the essentials of **secret codes**, **augmented** by **modern mathematics** that **protects our data in powerful ways**.

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Need Information Security

Because there are threats : **Threats and Threat Categories**

Threats

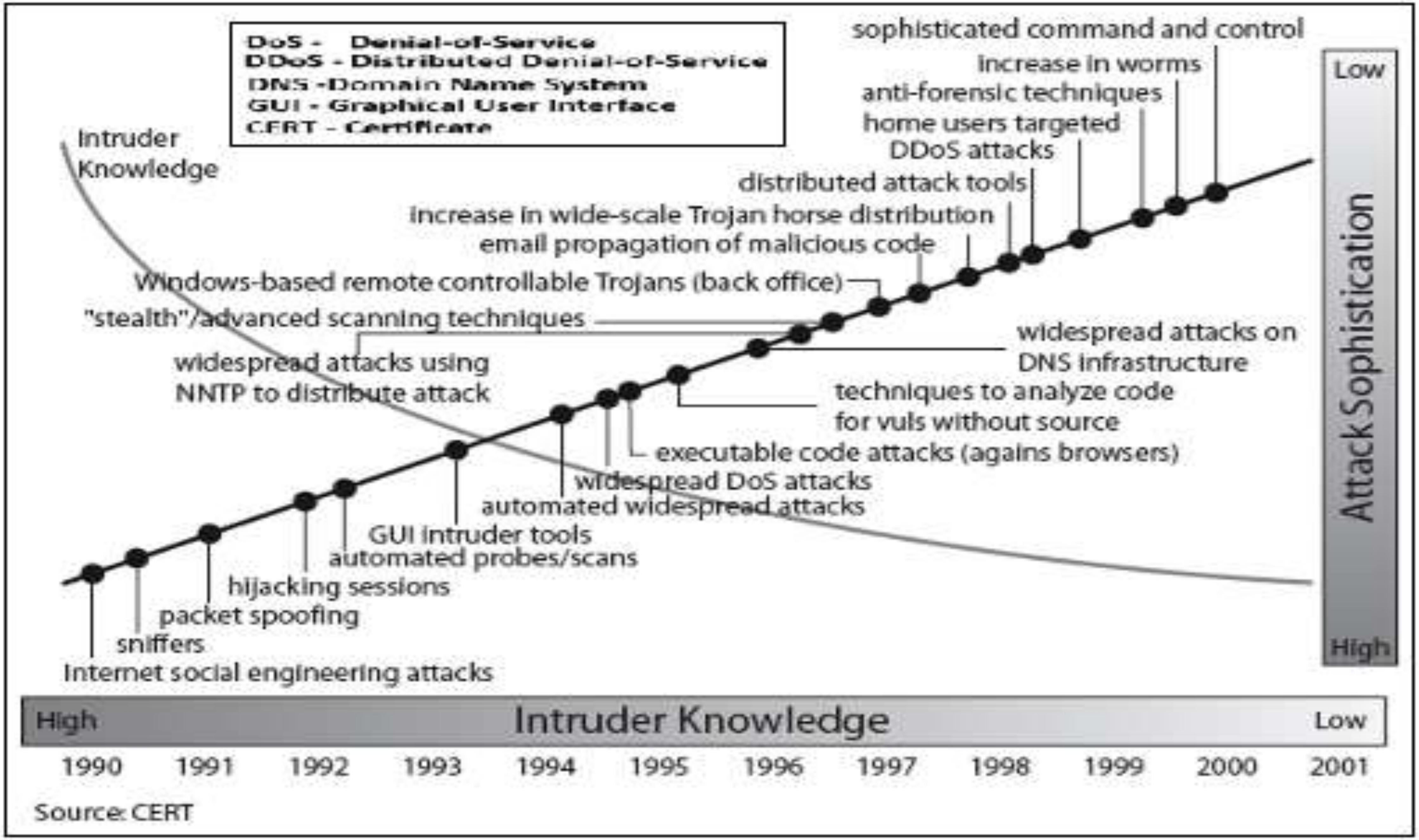
A threat is an object, person, or other entity that represents a constant danger to an asset

The **2007 CSI (Computer Security Institute)** survey

- 494 computer security practitioners
- 29% reported to law enforcement
- 1/5 suffered _targeted attack‘
- Most prevalent security problem
- 46% suffered security incidents
- Average annual loss $350,424
- The source of the greatest financial losses?
- Insider abuse of network access
- Email

Threat Categories

• Acts of human error or failure • Compromises to intellectual property • Deliberate acts of espionage or trespass • Deliberate acts of information extortion • Deliberate acts of sabotage or vandalism • Deliberate acts of theft • Deliberate software attack • Forces of nature • Deviations in quality of service • Technical hardware failures or errors • Technical software failures or errors • Technological obsolesce


DoS - Denial-of-Service
DDoS - Distributed Denial-of-Service
DNS -Domain Name System
GUI - Graphical User Interface
CERT - Certificate
Intruder Knowledge
sophisticated command and control
increase in worms
anti-forensic techniques
home users targeted
DDoS attacks
distributed attack tools
increase in wide-scale Trojan horse distribution
email propagation of malicious code
Windows-based remote controllable Trojans (back office)
"stealth"/advanced scanning techniques
widespread attacks on DNS infrastructure
widespread attacks using NNTP to distribute attack
techniques to analyze code for vuls without source
executable code attacks (agains browsers)
widespread DoS attacks
automated widespread attacks
GUI intruder tools
automated probes/scans
hijacking sessions
packet spoofing
sniffers
Internet social engineering attacks
Low
Attack Sophistication
High
High
Intruder Knowledge
Low
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001

Source: CERT

THE NEED FOR SECURITY

Network Security measures are needed to protect data during their transmission.

Following are the examples of security violations:

User A transmits a sensitive information file to User B. The Unauthorized User C is able to monitor the transmission and capture a copy of the file during its transmission.

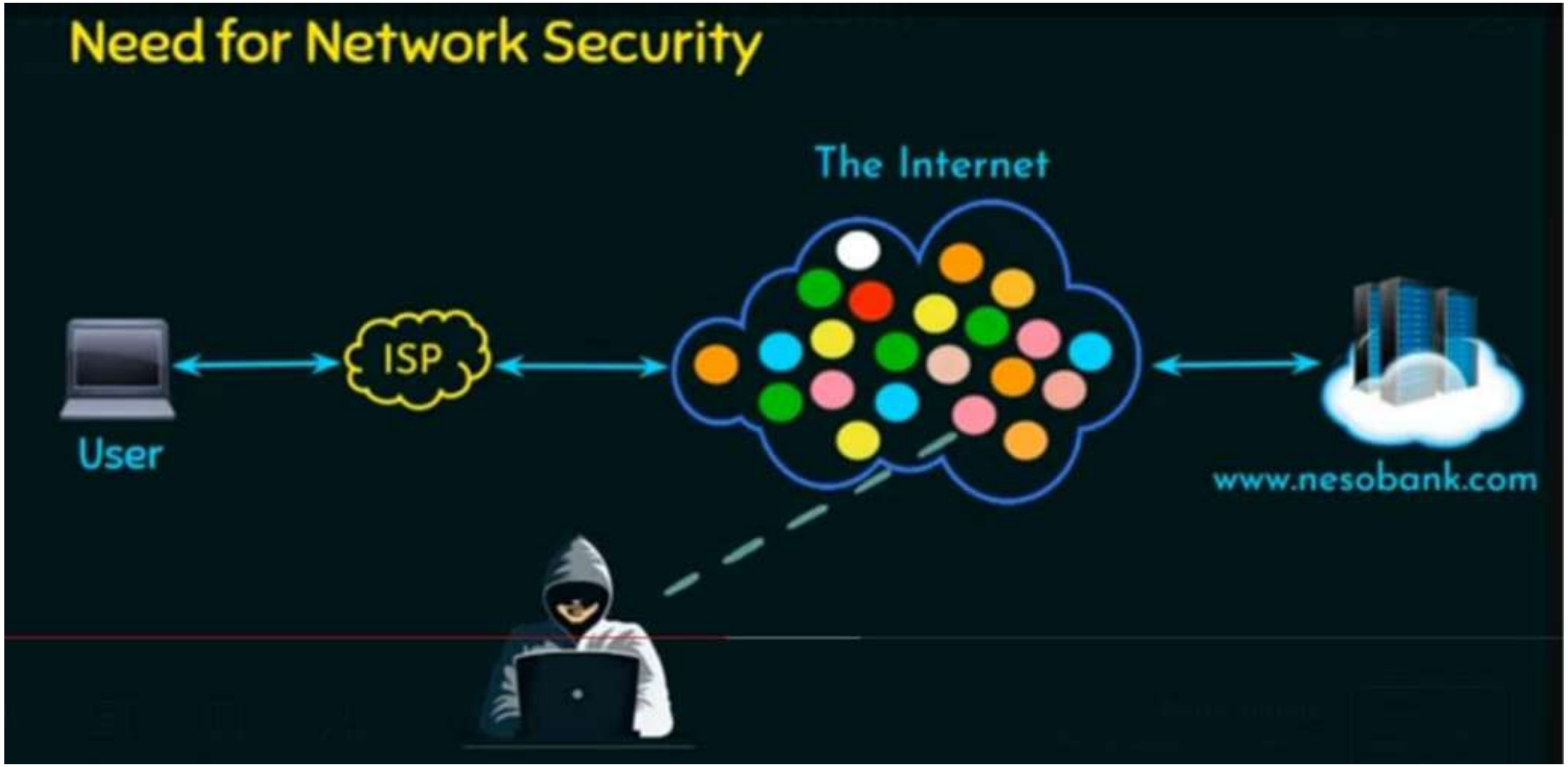
A message is sent from a **customer** to a **stock broker** with instructions for various transactions, subsequently the investments lose value and the customer denies sending the message.

While transmitting the message between **two users**, **the unauthorized user intercepts the message**, **alters its contents to add or delete entries, and then forwards the message to destination user**.

THE NEED FOR SECURITY

Security provider privacy for your data means no other party can view your data.

Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization.



ISP (Internet Service Provider) was **Telenet**

OSI Security Architecture

The **International Telecommunication Union Telecommunication (ITU-T)** recommendation X.800, Security Architecture for OSI, defines such a **Systematic approach**.

The OSI Security architecture is useful to manager as a way of organizing the task of providing **Security**.

It mainly focuses on **Security attacker**, **Mechanisms** and **Services.**

1).Security attack: Any action that compromises the security of information owned by an organization.

2).Security mechanism: A process that is designed to detect, prevent or recover from a security attack.

3) Security Service: A processing or communication service that enhances the security of the data processing Systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

DEFINITIONS

- **Computer Security** - Generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - Measures to protect data during their transmission
- **Internet Security** - Measures to protect data during their transmission over a collection of interconnected networks
- our focus is on Internet Security.
- which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information

Security Approaches

An organization can take several approaches to implement its security model. The **various approaches** are

1.No Security : In this simplest case, the approach could be a decision to implement no security at all

2.Security through obscurity: In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long as there are many ways an attacker can come to know about it.

3.Host Security: In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is there. That it cannot scale well. The complexity and diversity of modern organizations makes the task even harder.

4.Network Security: Host Security is tough to achieve as organization grow is become more diverse. In this, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

PRINCIPLES OF SECURITY / ASPECTS OF SECURITY

➢ consider **3 aspects of information security**:

● **Security Attack**

● **Security Mechanism**

● **Security Service**

● Security Attack

Security: **F**reedom from danger : safety

Defination of Security Attack:

Any form of malicious or actions taken to harm the security of information system components

Types of Security attacks

There are **four general categories of attacks** / **Types of Security attacks**:

1) Interruption: An Asset of the system is destroyed or becomes unavailable. This is a threat to availability.

Eg: cutting of **communication line**

2) Interception : An unauthorized party gain access to an asset. This is a threat to Secrecy.

Eg: wiretapping to capture **data in a network**.

3) Modification : An Unauthorized party not only gains access but tampers with an asset. This is a threat to integrity.

Eg: changing values in a **data file**

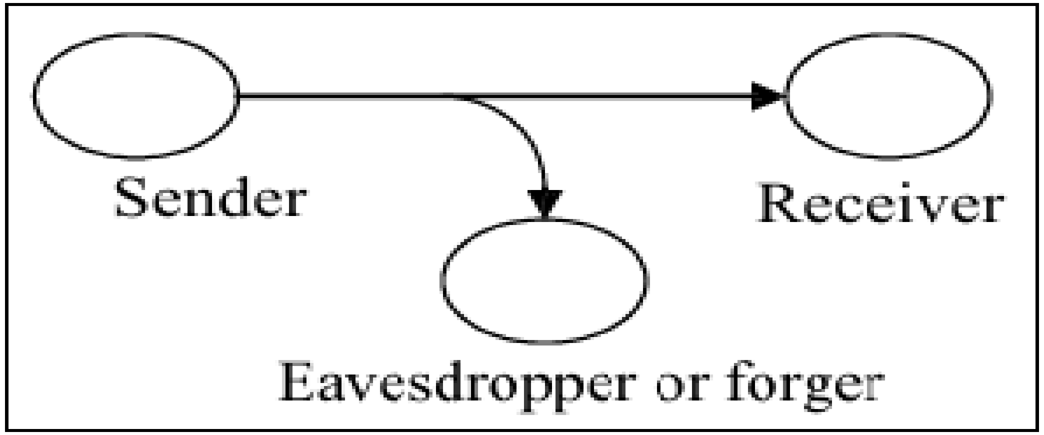
4) **Fabrication:** This is also a threat to integrity. An unauthorized party inserts counter fit objects into the System.

Eg: Addition of **records to a file**

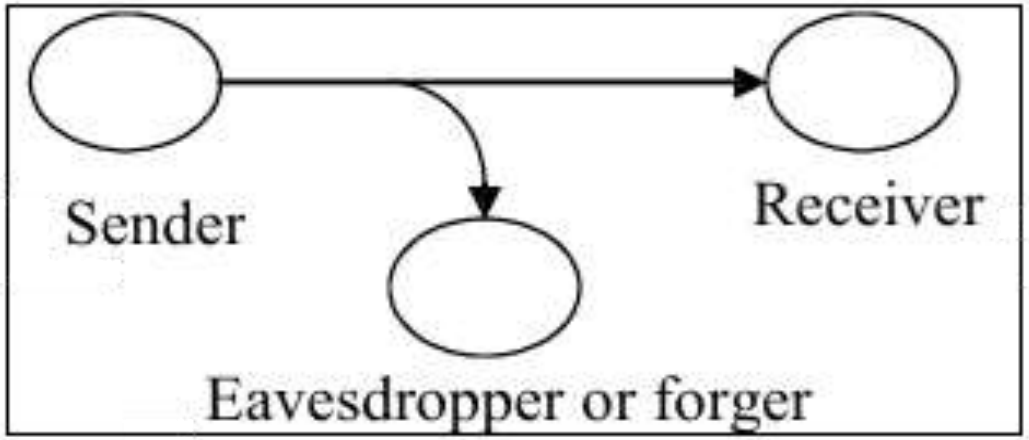
SECURITY ATTACKS: There are **four general categories** of attack which are listed below.

1.Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

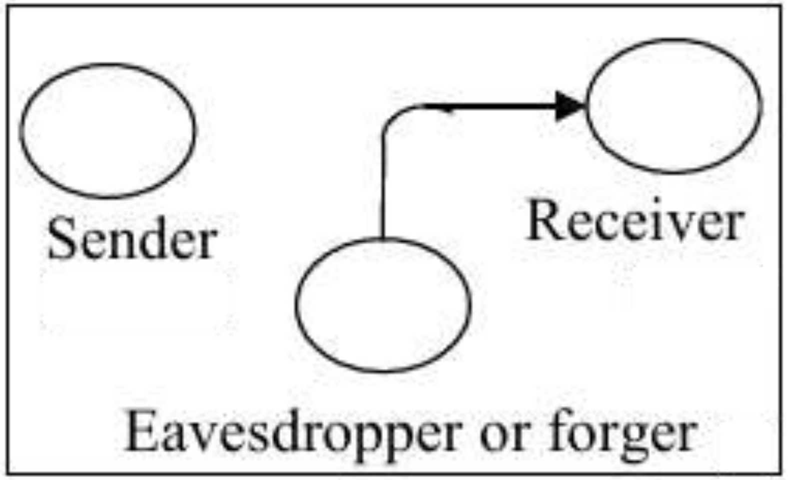
2.Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer.e.g., wire tapping to capture data in the network, illicit copying of files



3.Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



4.Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.



CRYPTOGRAPHIC ATTACKS

Attack: Any action that compromises the security of information owned by an organization.

Security attacks are of **two types**: **A).Passive, B).Active attacks.**

A). Passive attacks:

Two types of passive attacks are:

1.Release of message contents

2.Traffic analysis

B).Active attacks:

Four types of Active attacks are:

1).Masquerade

2).Replay

3).Modification of messages

4).Denial of service

- ➢ any action that compromises the security of information owned by an organization
- ➢ information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- ➢ often threat & attack used to mean same thing
- ➢ have a wide range of attacks
- ➢ can focus of generic types of attacks

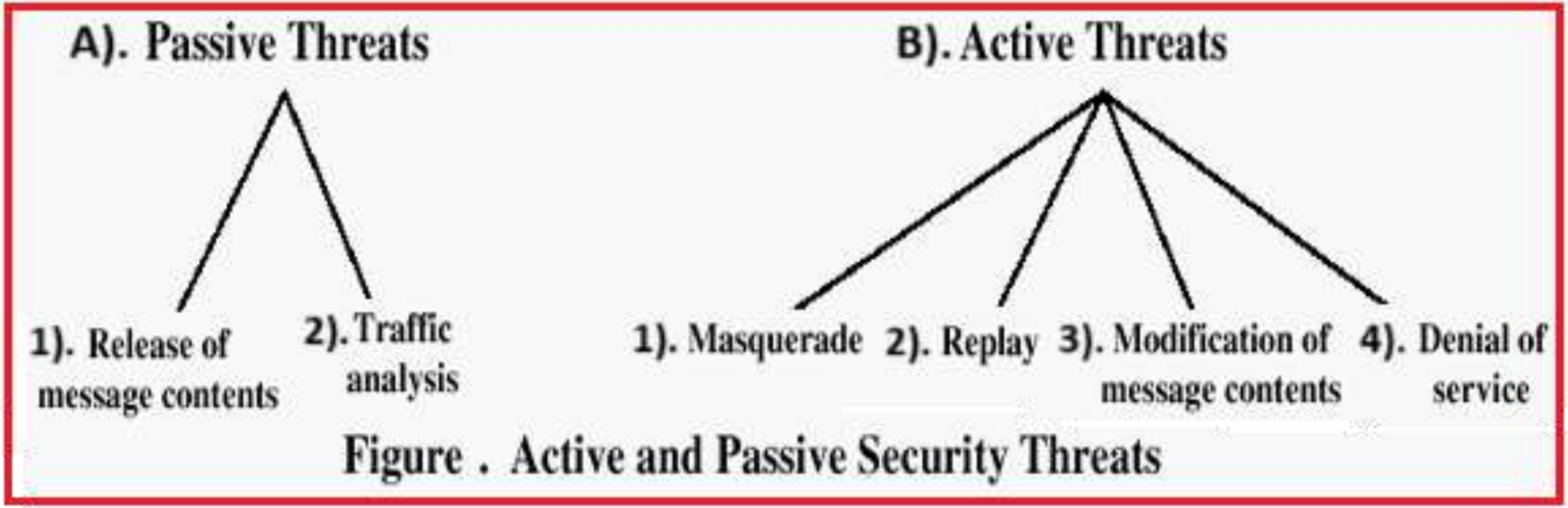
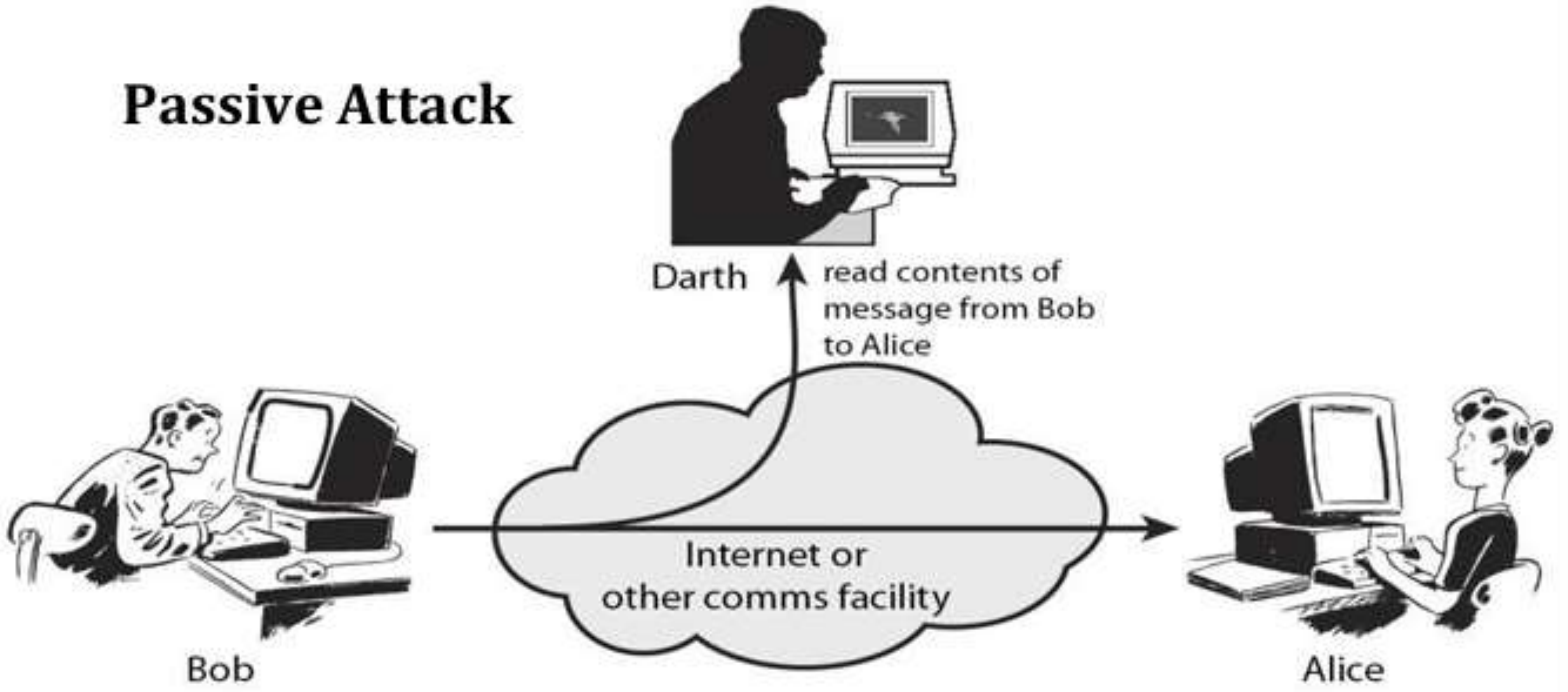


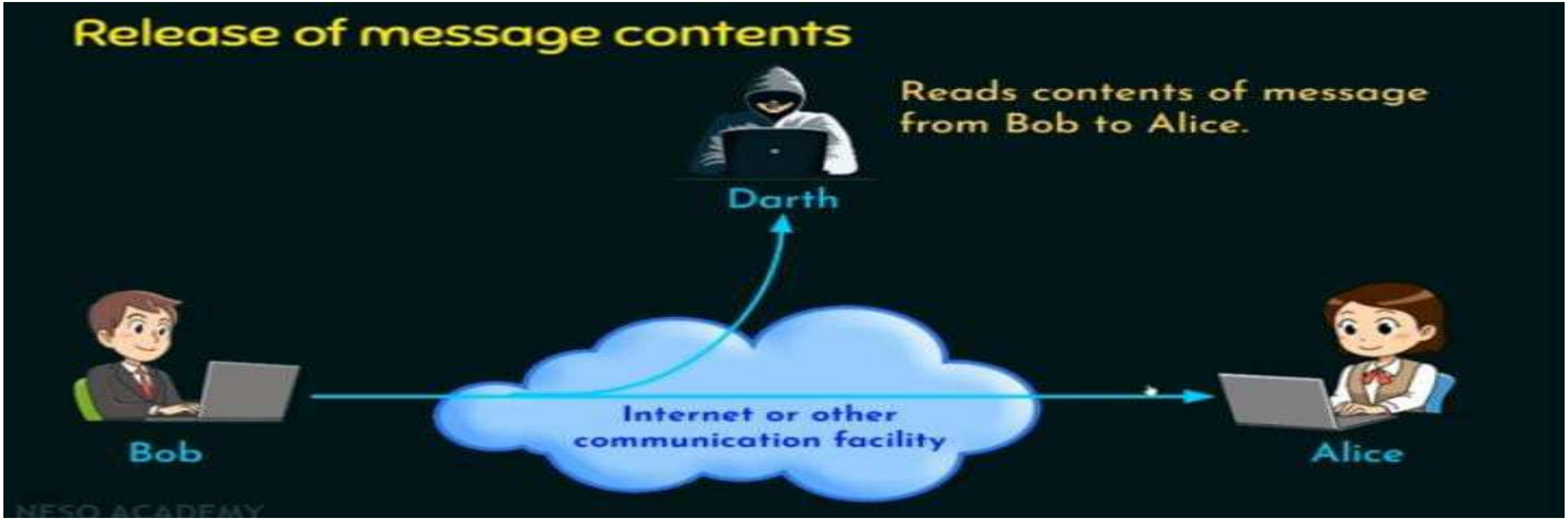
Figure . Active and Passive Security Threats

A). Passive attacks


Passive Attack
Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

A). Passive attacks

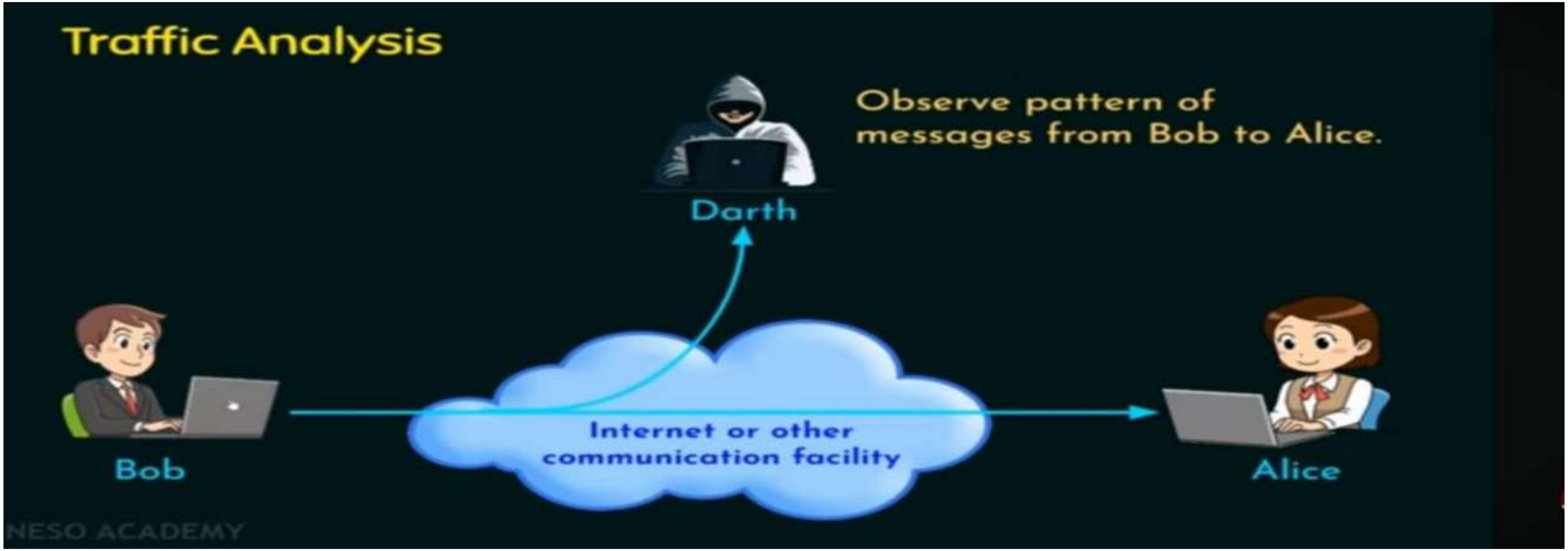
1.Release of message contents:


Release of message contents
Reads contents of message from Bob to Alice.
Darth
Internet or other communication facility
Bob
Alice
NESO ACADEMY

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 content of these transmissions.

2) Traffic analysis

2) Traffic analysis:


Traffic Analysis
Observe pattern of messages from Bob to Alice.
Darth
Internet or other communication facility
Bob
Alice
NESO ACADEMY

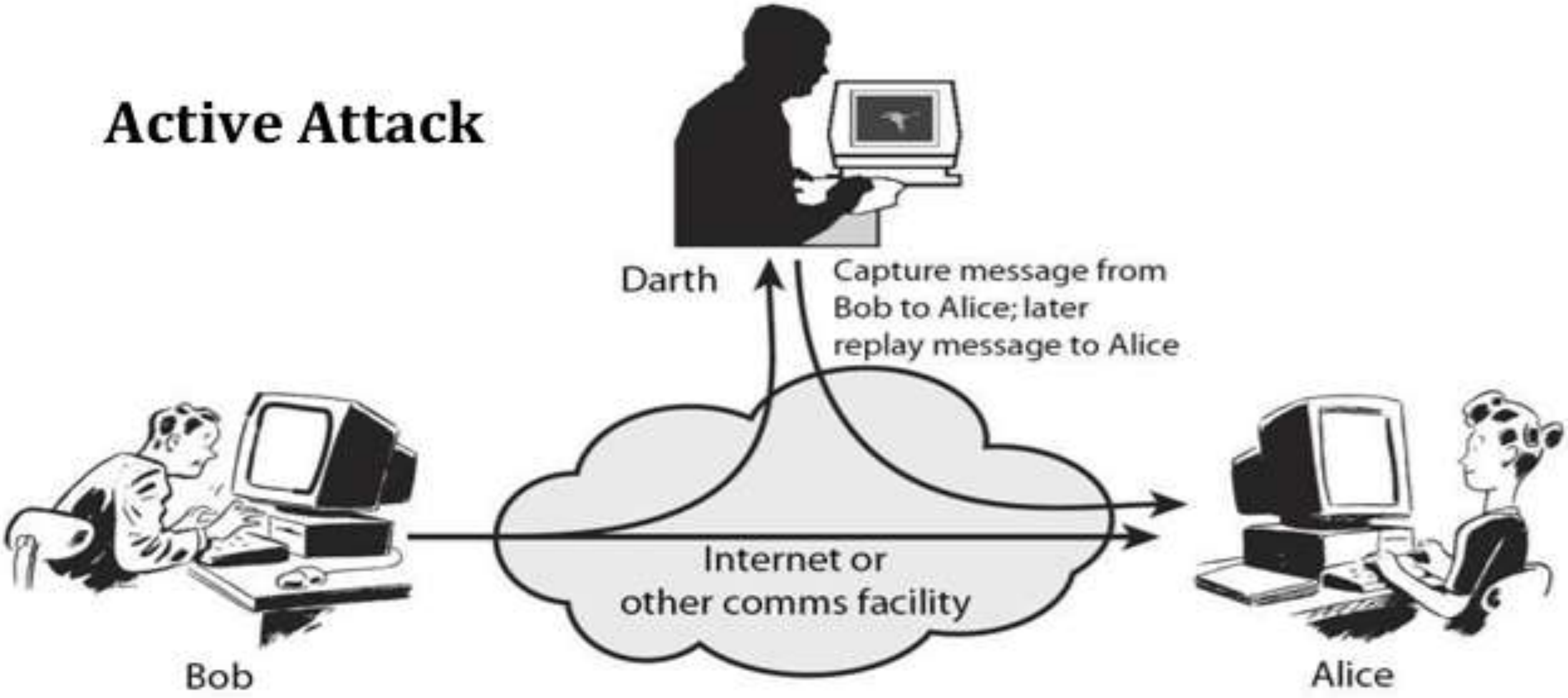
Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking.

B).Active Attacks

These attacks can be classified in to **four categories**:

1).Masquerade – One entity pretends to be a different entity.
2).Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
3).Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
4).Denial of service – Prevents or inhibits the normal use or management of communication facilities.

B).Active Attacks


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

INTERRUPTION An asset of the system is destroyed or becomes unavailable or unusable.

Examples: ➢ **Destruction of some hardware**
➢ **Jamming wireless signals**
➢ **Disabling file management systems**

INTERCEPTION An unauthorized party gains access to an asset. Attack on confidentiality.

Examples:

➢ **Wire tapping to capture data in a network.**
➢ **Illicitly copying data or programs**
➢ **Eavesdropping**

MODIFICATION When an unauthorized party gains access and tampers an asset. Attack is on Integrity.

Examples: ➢ **Changing data file** ➢ **Altering a program and the contents of a message**

FABRICATION An unauthorized party inserts a counterfeit object into the system. Attack on Authenticity. Also called impersonation

Examples: ➢ **Hackers gaining access to a personal email and sending message**
➢ **Insertion of records in data files**
➢ **Insertion of spurious messages in a network**

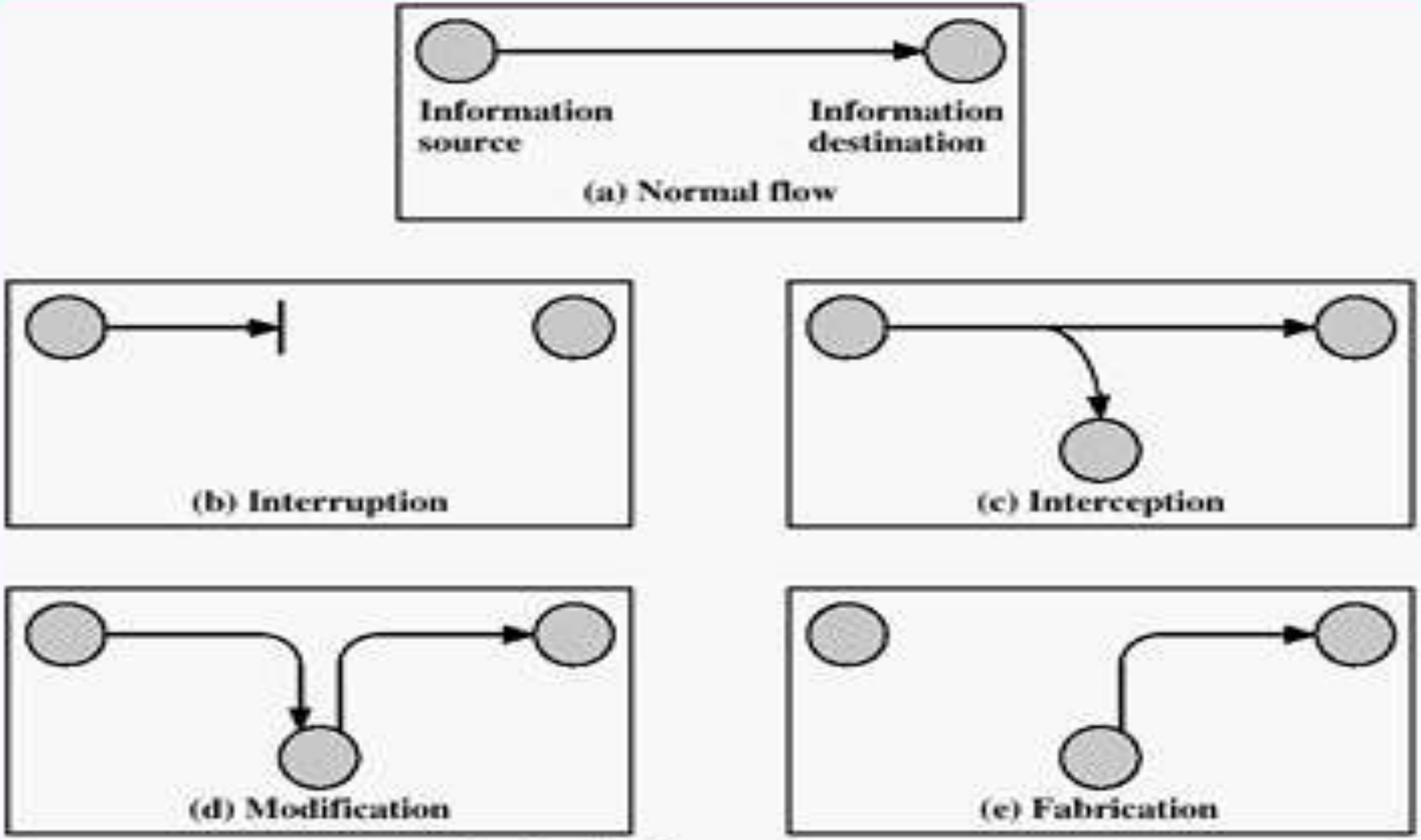


Figure Security Threats

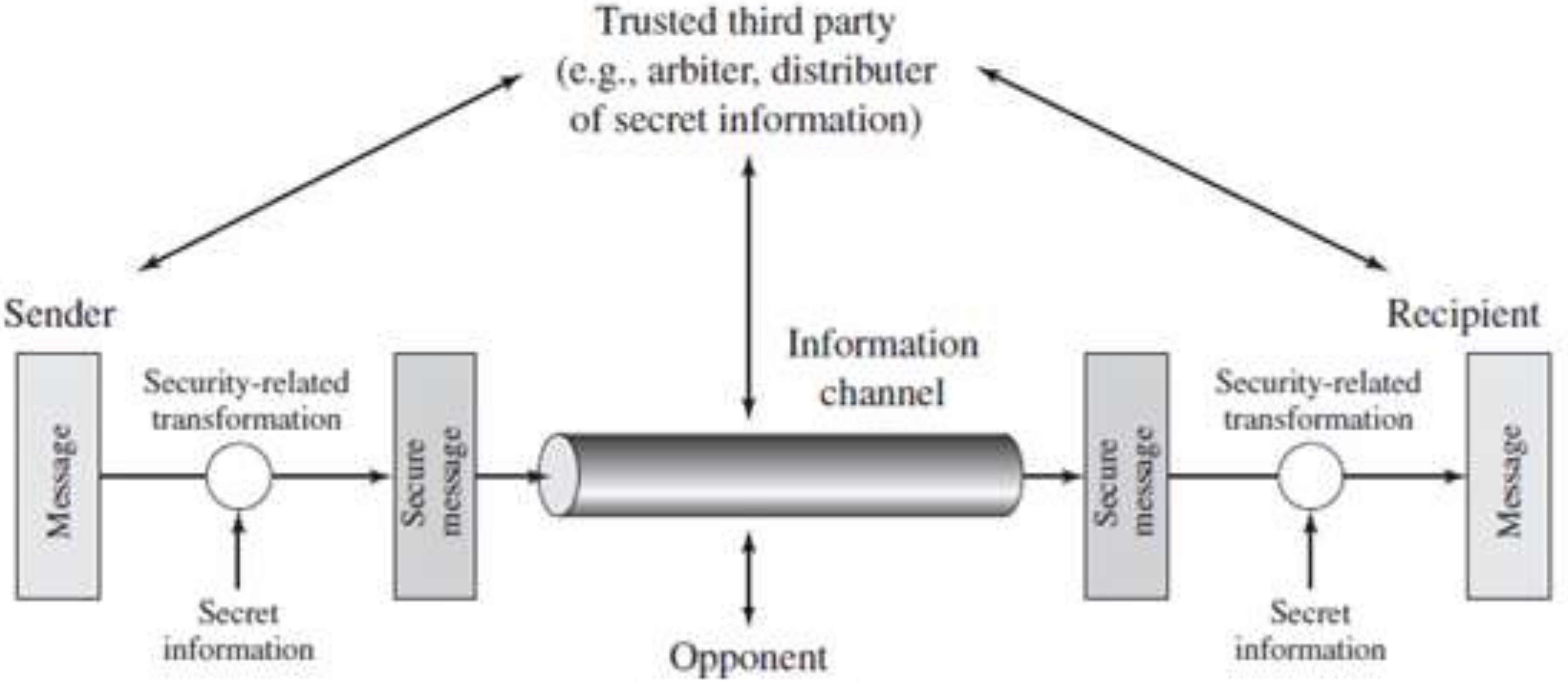
Symmetric and public key algorithms

Encryption/Decryption methods fall into **two categories**:**1).Symmetric key, 2).Public key**

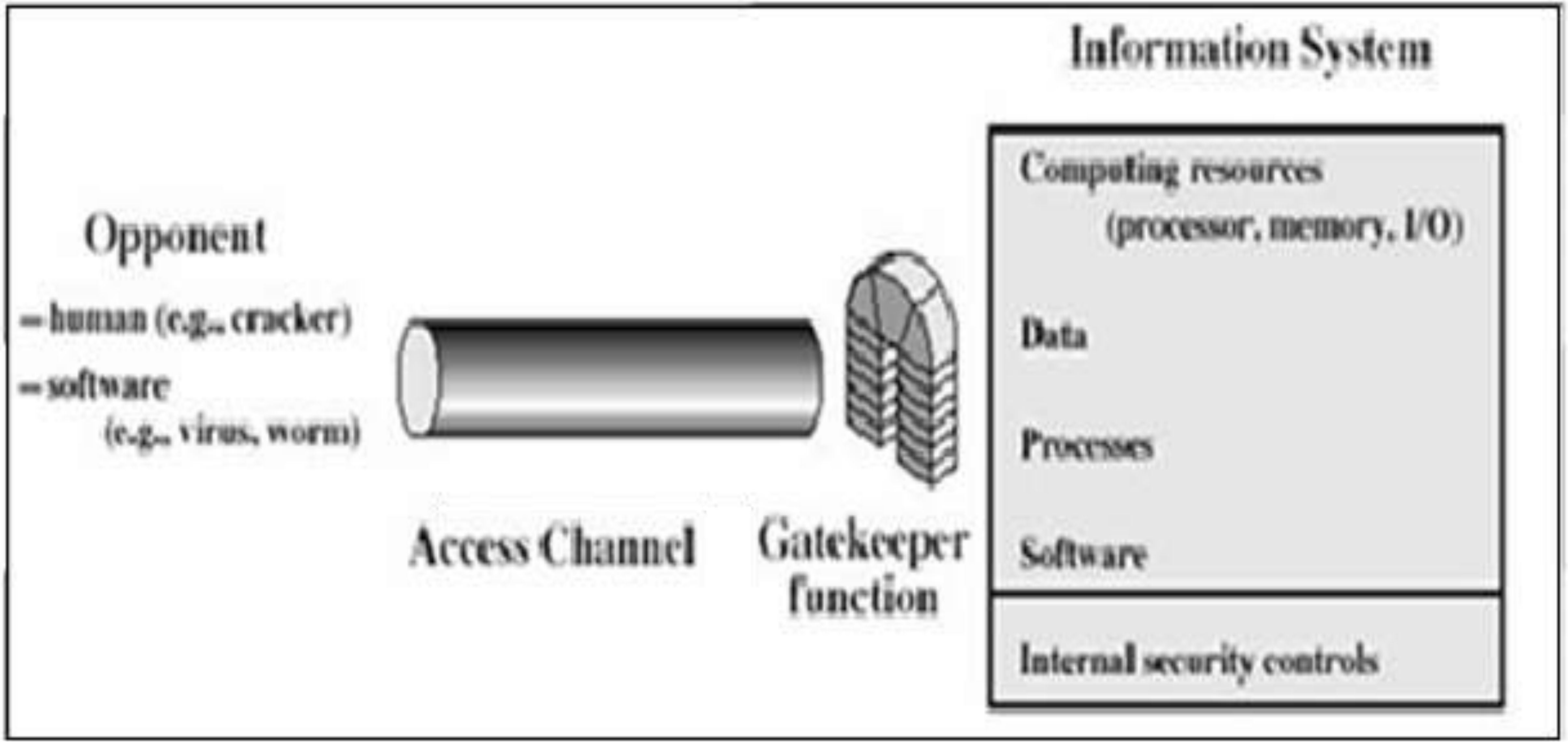
In **symmetric key algorithms**, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

In **public key cryptography, encryption key** is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

A MODEL FOR NETWORK SECURITY



Using this model requires us to:

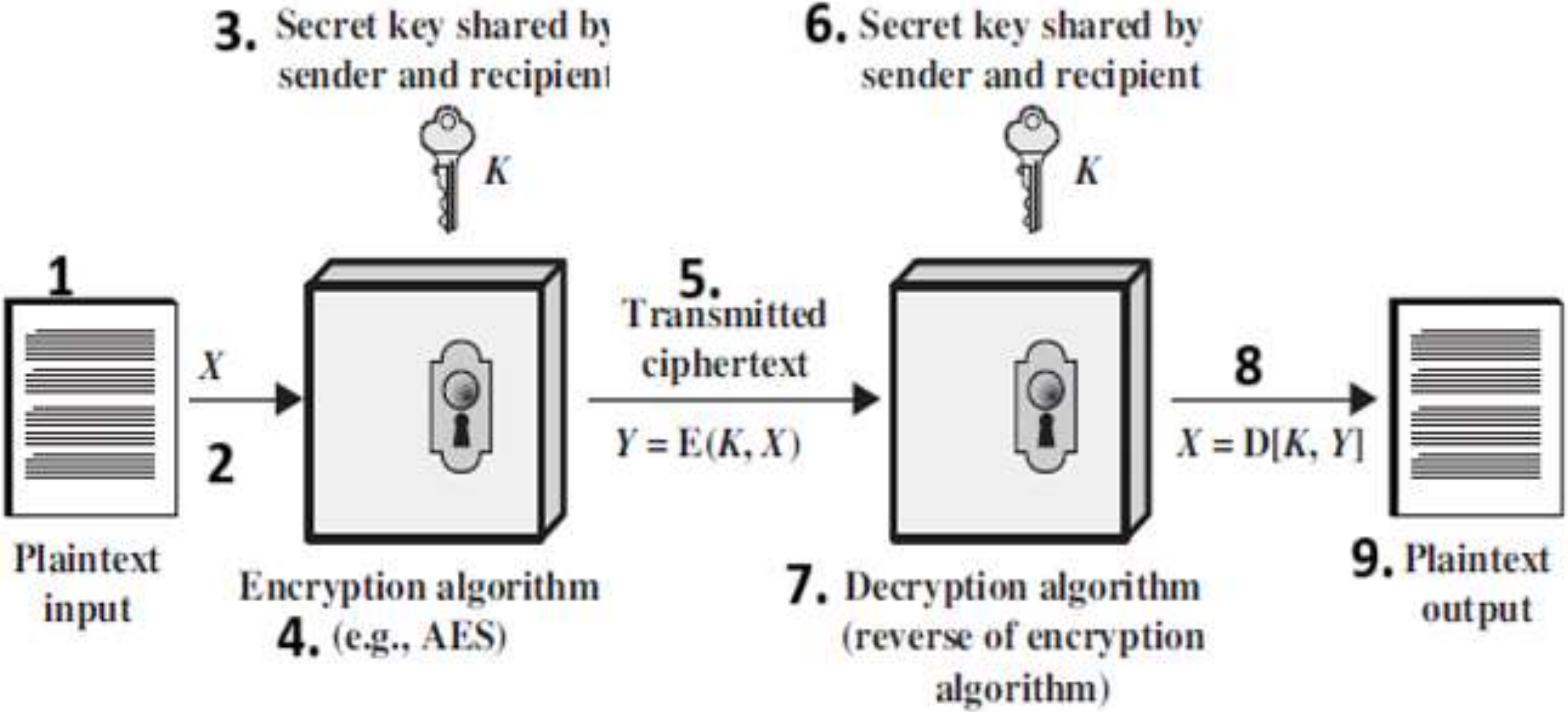


CONVENTIONAL ENCRYPTION

- **Referred conventional / private-key / single-key**
- **Sender and recipient share a common key**

All classical encryption algorithms are private-key was only type prior to invention of public key in 1970‟plaintext - the original message Some basic terminologies used:

- Cipher text - the coded message
- Cipher - algorithm for transforming plaintext to cipher text
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to cipher text
- Decipher (decrypt) - recovering cipher text from plaintext
- Cryptography - study of encryption principles/methods.
- Cryptanalysis (code breaking) - the study of principles/ methods of deciphering cipher text without knowing key
- Cryptology - the field of both cryptography and cryptanalysis


3. Secret key shared by
sender and recipient
K
6. Secret key shared by
sender and recipient
K
1
X
2
Plaintext
input
Encryption algorithm
4. (e.g., AES)
5.
Transmitted
ciphertext
Y = E(K, X)
7. Decryption algorithm
(reverse of encryption
algorithm)
8
X = D[K, Y]
9. Plaintext
output

● Security Mechanism

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are

1.Encipherment, 2.Digital Signature, 3.Access Control.

Specific Security Mechanisms: Provide some of the OSI security services,

❍ **Encipherment,** ❍ **Digital Signature,** ❍ **Access Control,**
❍ **Data Integrity,** ❍ **Authentication Exchange,** ❍ **Traffic Padding,**
❍ **Routing Control, Notarization.**

Pervasive Security Mechanisms: These are not specific to any particular OSI security service or protocol layer.

❍ **Trusted Functionality,** ❍ **Security Level,** ❍ **Event Detection,**
❍ **Security Audit Trail,** ❍ **Security Recovery.**

● Security Service

It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms.

- ❍ **Confidentiality,**
- ❍ **Authentication: • Peer entity authentication,**
- ❍ **Integrity: • Connection-Oriented Integrity Service,**
  • Connectionless-Oriented Integrity Service,
- ❍ **Non-repudiation,**
- ❍ **Access Control,**
- ❍ **Availability**

SECURITY SERVICES

SECURITY SERVICES

The classification of security services are as follows:

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

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

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

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

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

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

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

MODULE-2

A model for Network Security Cryptography Concepts and Techniques / Cryptographic Techniques:

- Introduction,
- Cryptography Concepts and Techniques
- Plain Text And Cipher Text,
- Substitution Techniques,
- Transposition Techniques,
- Encryption And Decryption,
- Symmetric And Asymmetric Key Cryptography,
- Steganography,
- Key Range And Key Size,
- Possible Types Of Attacks.

A model for Network Security Cryptography Concepts and Techniques / Cryptographic Techniques:

Basic Concepts

Cryptography The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

Plaintext The original intelligible message

Cipher text The transformed message

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

Key Some critical information used by the cipher, known only to the sender& receiver ***Encipher (encode)*** The process of converting plaintext to cipher text using a cipher and a key

Decipher (decode) the process of converting cipher text back into plaintext using a cipher and a key

Cryptanalysis The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking

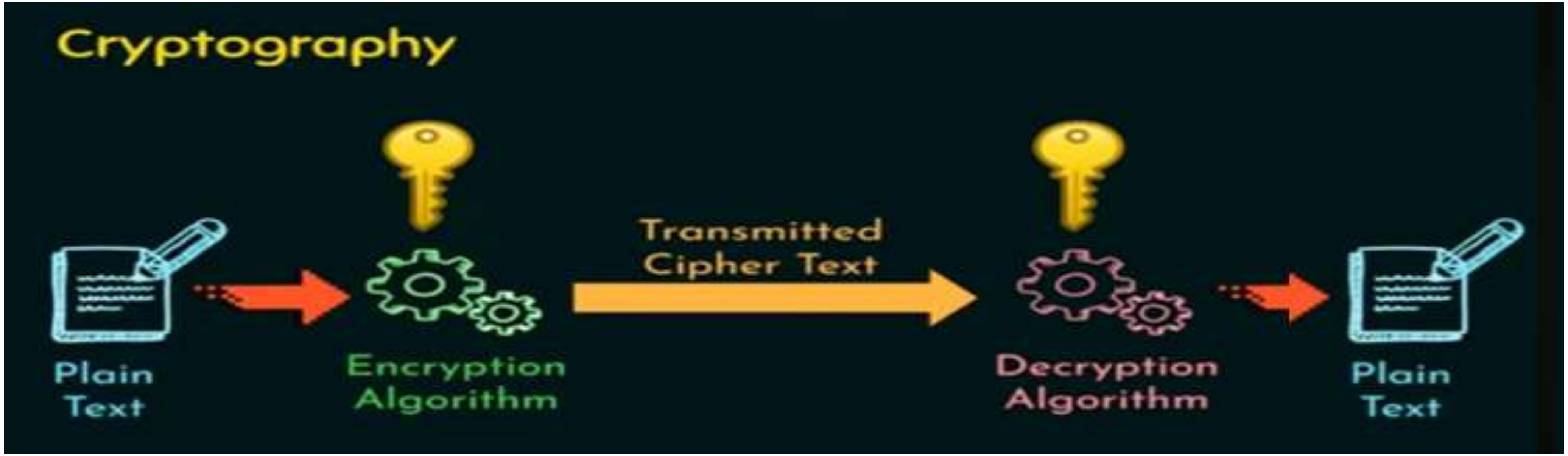
Cryptology Both cryptography and cryptanalysis

Code An algorithm for transforming an intelligible message into an unintelligible one using a code-book.

CRYPTOGRAPHY CONCEPTS and TECHNIQUES

Cryptography: Cryptography means secret writing, **is** the science of converting a message into a coded form that hides the information contained in the message. We encrypt a message before its transmission ,so that can eavesdropper may not get the information contained in the message.

There are many ways of carrying out encryption , These are called cryptography or ciphers.



➢ Plain Text And Cipher Text,

Plain Text: This is the original message or data that is fed into algorithm as input.

Cipher Text: This is the Scrambled message produced as output. It depends on the Plain text and the Secret Key. For a given message, two different keys will produced.

Encryption : The process of converting plain text into Cipher text is Known as encryption.

Decryption : The process of converting cipher text into plain text is known as decryption.

A cryptography system consists of two components

1).A Set of complementary algorithms, encryption algorithm(E) and decryption algorithm(D).

2).Cipher key(K)

Cryptographic Systems are generally classified along three independent dimensions

1),The type of operations used for transforming plain text to cipher text: All encryption algorithms are based on two general principles.

2).Substitution

3).Transposition

i).Substitution: It means replacing a symbol of the plain text with another symbol. Eg: COMPUTER---□ DPNQVUFS

ii) Transposition: It means rearranging the order of appearance of the symbols of the message. Eg: COMPUTER-□ CMUEOPTR

2. **The number of keys used:** If both sender and receiver use the same key, the system is referred to as Symmetric, Single key or Conventional encryption.
If the sender and receiver each use a different key, the system is referred to as Symmetric , two key or public key encryption.

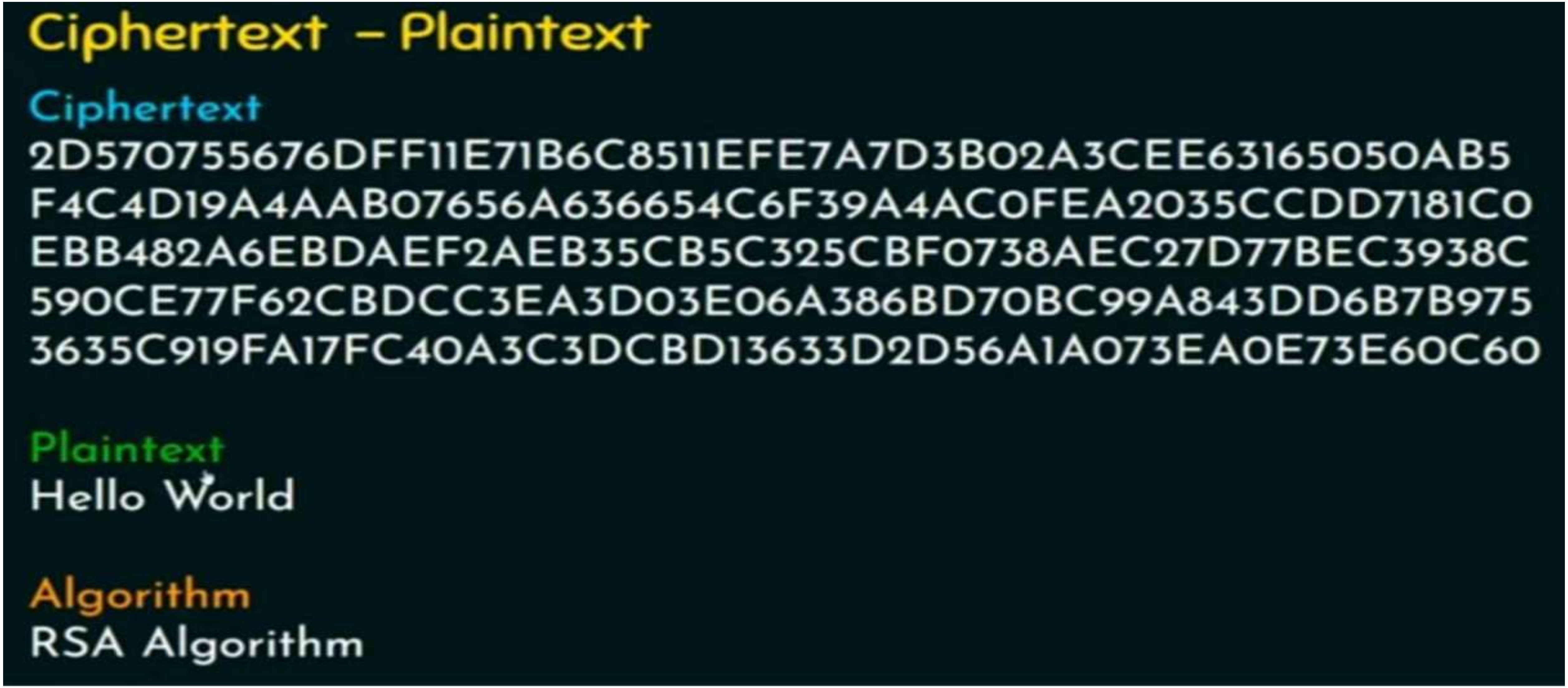
3) **The way in which the plain text is processed:**

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A Stream cipher processes the input elements continuously , Producing output one element at a time, as it goes along.

There are **two general approaches** to attacking a conventional encryption scheme.

1).Cryptanalysis:

It is the art of deciphering an encrypted message without complete Knowledge of the key required for decryption. An attempted cryptanalysis is called a cryptanalytic attack



Ciphertext – Plaintext

Ciphertext

```
2D570755676DFF11E71B6C8511EFE7A7D3B02A3CEE63165050AB5
F4C4D19A4AAB07656A636654C6F39A4AC0FEA2035CCDD7181C0
EBB482A6EBDAEF2AEB35CB5C325CBF0738AEC27D77BEC3938C
590CE77F62CBDCC3EA3D03E06A386BD70BC99A843DD6B7B975
3635C919FA17FC40A3C3DCBD13633D2D56A1A073EA0E73E60C60
```

Plaintext

Hello World

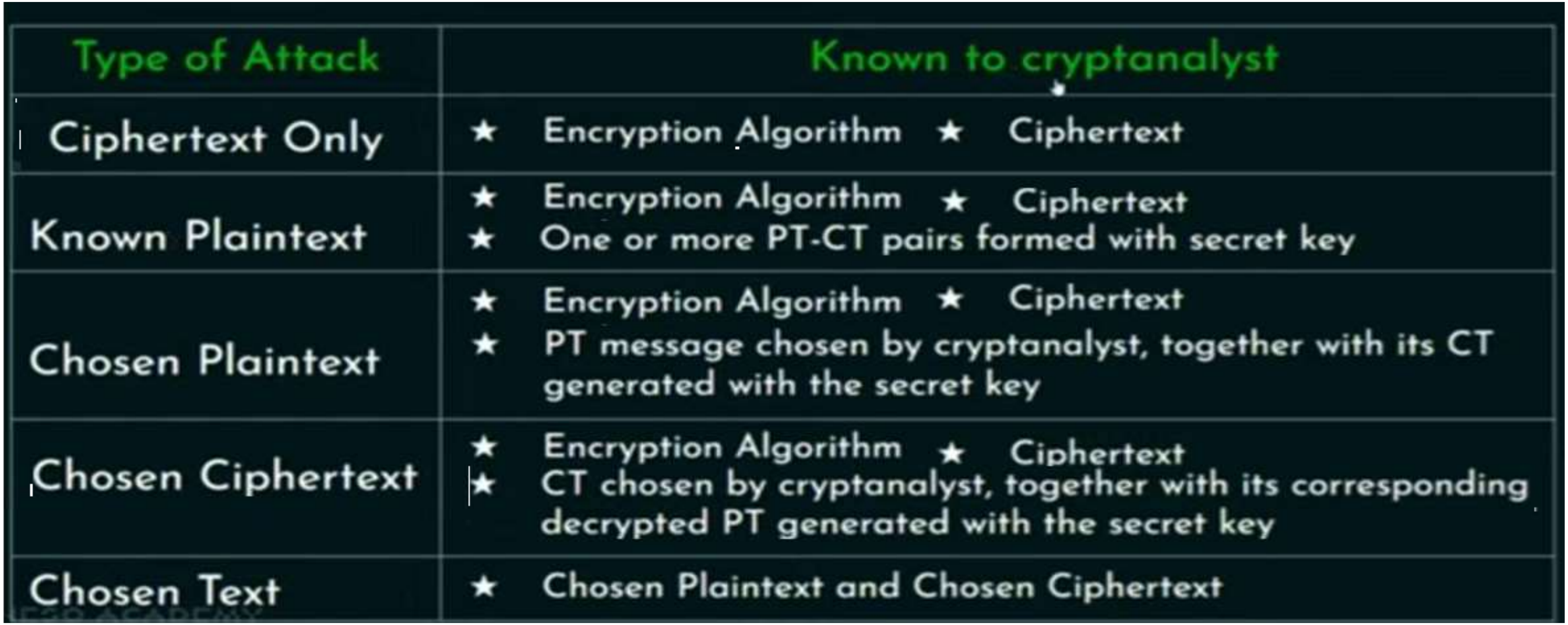
Algorithm

RSA Algorithm

Cryptanalytic Attacks:

A Cryptanalyst can attack a Cryptosystem in several ways.

The following are the various type of attacks.



Type of Attack	Known to cryptanalyst
Ciphertext Only	★ Encryption Algorithm ★ Ciphertext
Known Plaintext	★ Encryption Algorithm ★ Ciphertext ★ One or more PT-CT pairs formed with secret key
Chosen Plaintext	★ Encryption Algorithm ★ Ciphertext ★ PT message chosen by cryptanalyst, together with its CT generated with the secret key
Chosen Ciphertext	★ Encryption Algorithm ★ Ciphertext ★ CT chosen by cryptanalyst, together with its corresponding decrypted PT generated with the secret key
Chosen Text	★ Chosen Plaintext and Chosen Ciphertext

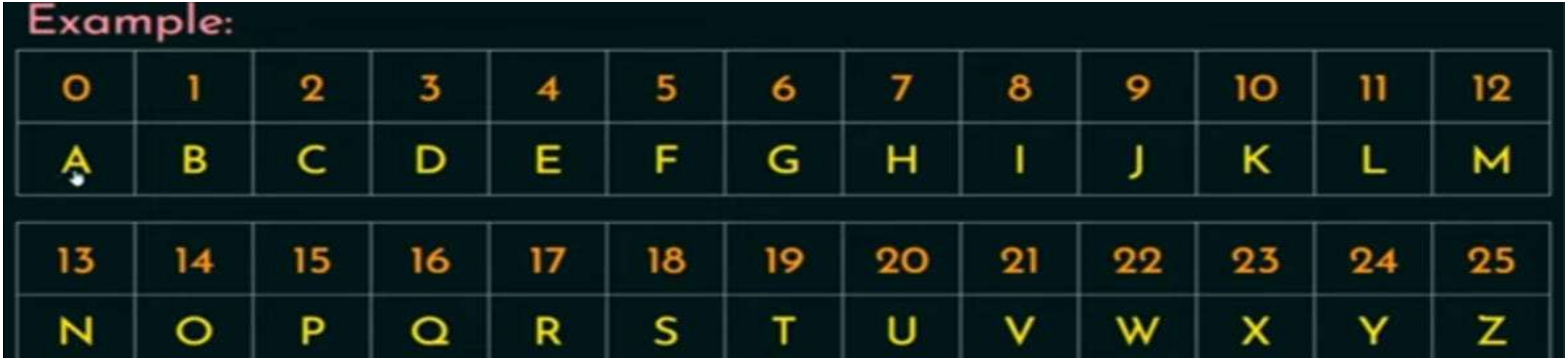
2) Brute-Force Attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plain text is obtained. On average, half of all possible keys must be tried to achieve success.

Substitution Techniques

Substitution Techniques: A Substitution Technique is one in which the letters of plain text are replaced by other letters or by number or symbols.

The Various substitution Techniques are:

1). **Caeser Cipher:** Letters are replaced by other letters. The earlier known and simplest method used be Julius Caeser. Replacing each letter of the alphabet with the letter standing three places further down the alphabet.



Example:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Algorithm:

For each plaintext letter ‘p’, substitute the ciphertext letter ‘C’.

$C=E(p,k)\bmod 26=(p+k)\bmod 26$, $P=D(C,k)\bmod 26=(C-k)\bmod 26$

Ex: Let key K=3, word= NEW

N=>m=12, C=(12+3) mod 26=15=>P, E=>m=4, C=(4+3) mod 26=7=>H

W=>m=22, C=(22+3) mod 26=25=>Z

Caeser cipher is also Known as additive cipher or shift ciphers

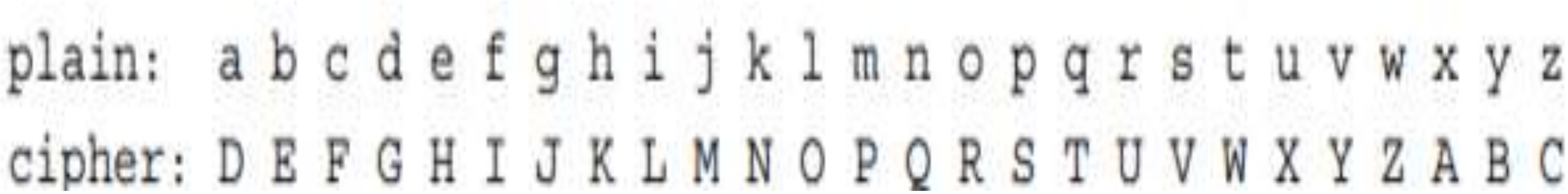
2) Monoalphabetic substitution cipher:

In monoalphabetic substitution, the relationship between a symbol in the plain text to a symbol in the cipher text is always one-to-one.

After sender and receiver agreed to a single key , that key is used to encrypt each letter in the plain text or decrypt each letter in the cipher text.

A better solution is to create a mapping between each plain text character and the corresponding cipher text character.

An example key for monoalphabetic substitution cipher



plain:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Eg:Message is machine

Plain text: machine

Cipher text:PDFKLQH

Substitution Techniques
[OR]

Substitution Techniques

3) Playfair cipher:

Aka Playfair square or Wheatstone-Playfair cipher.

Manual symmetric encryption technique.

The first literal digraphs substitution cipher.

Invented in 1854 by Charles Wheatstone.

Bore the name of Lord Playfair for promoting its use.

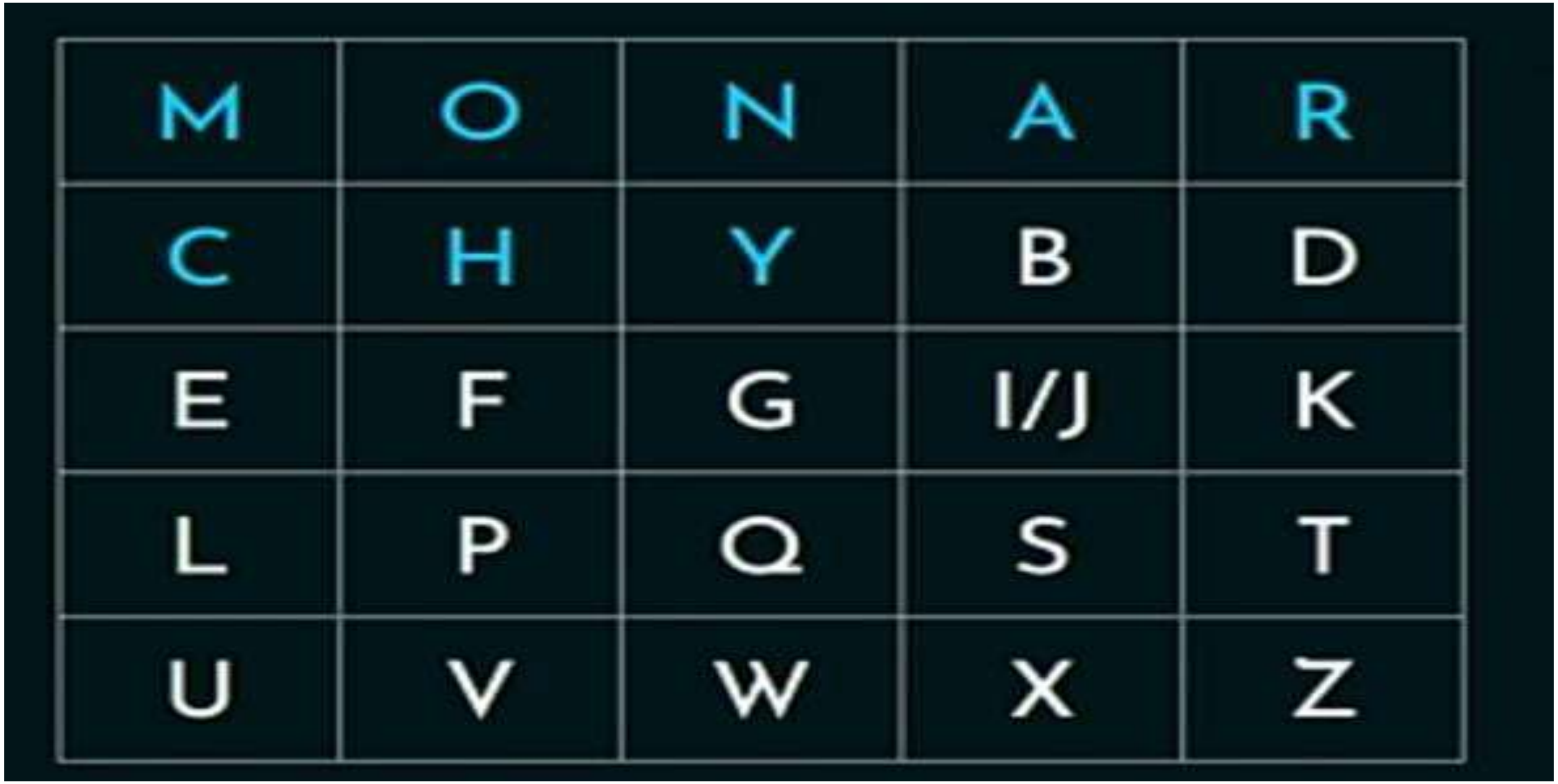
The Playfair Cipher Encryption Algorithm: The Algorithm consists of 2 steps:

Generate the key Square(5×5):

1).The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Ex: key is Monarchy



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

2) Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

i) Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’, Here **‘x’** is the bogus letter.

II) If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’, Here **‘z’** is the bogus letter.

Rules for Encryption:

1) If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:

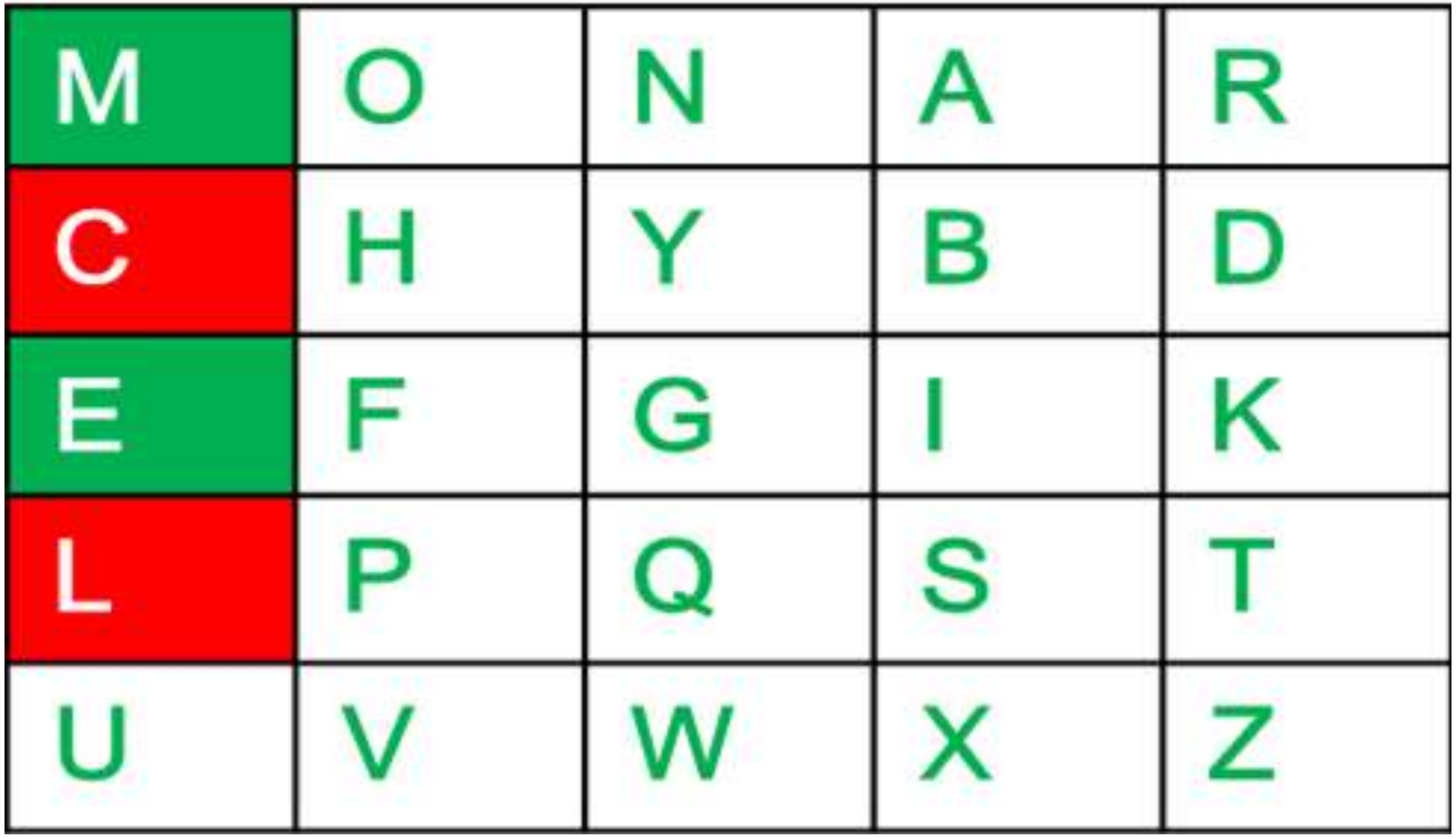
Diagraph: "me“

Encrypted Text: cl

Encryption:

m -> c

e -> l



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

Rules for Encryption:

2) If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

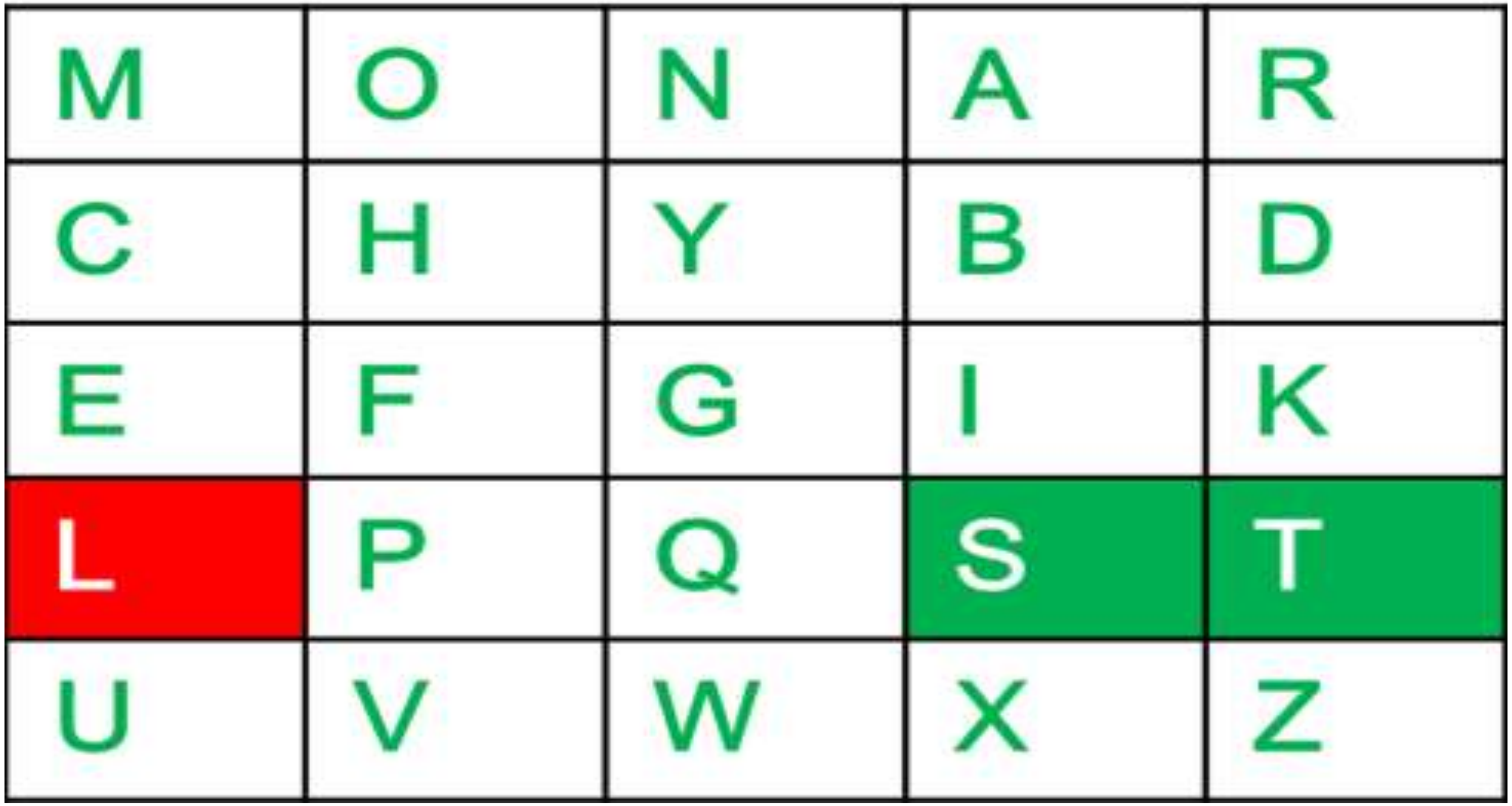
For example:

Diagraph: "st"

Encrypted Text: tl

Encryption:

s -> t



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

Rules for Encryption:

3) If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

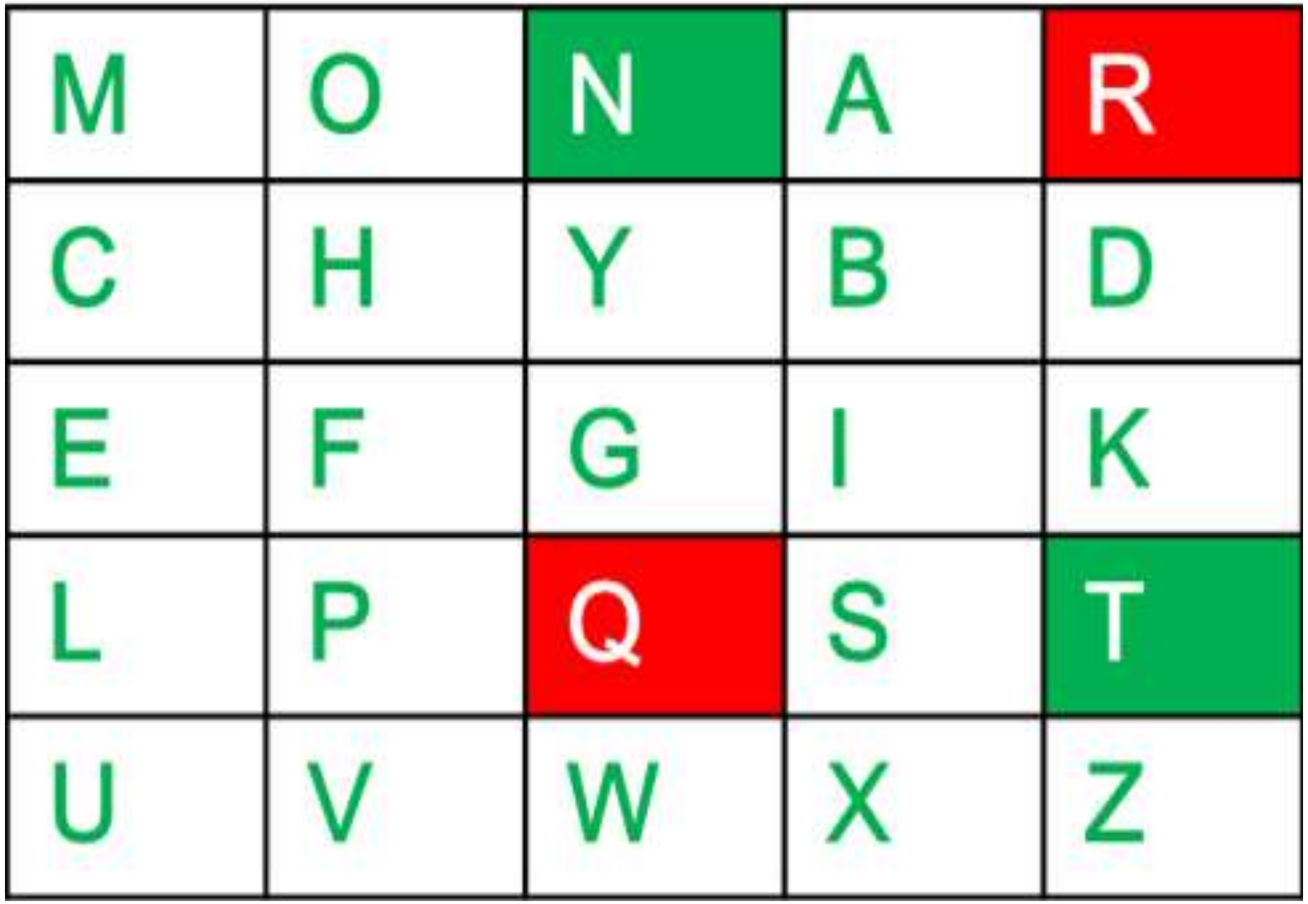
Diagraph: "nt"

Encrypted Text: rq

Encryption:

n -> r

t -> q



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

4) Hill Cipher:

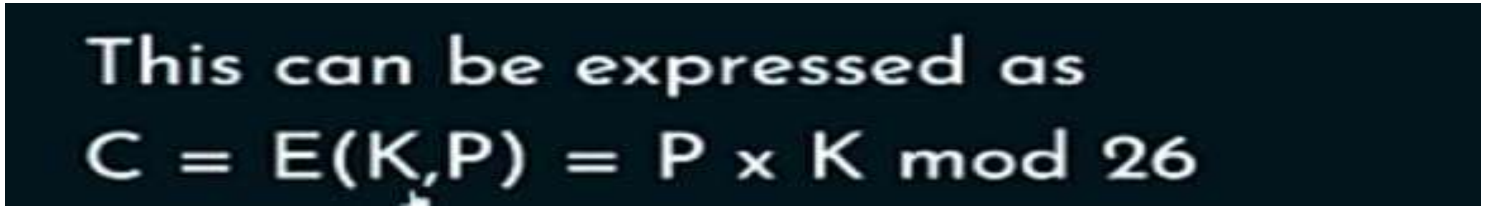
The hill cipher takes a mathematical approach to Multi-letter substitution.

A numerical value assigned to each letter of the alphabet.

Ex: Integers 0 through 25 -□ A through Z

Hill Algorithm:

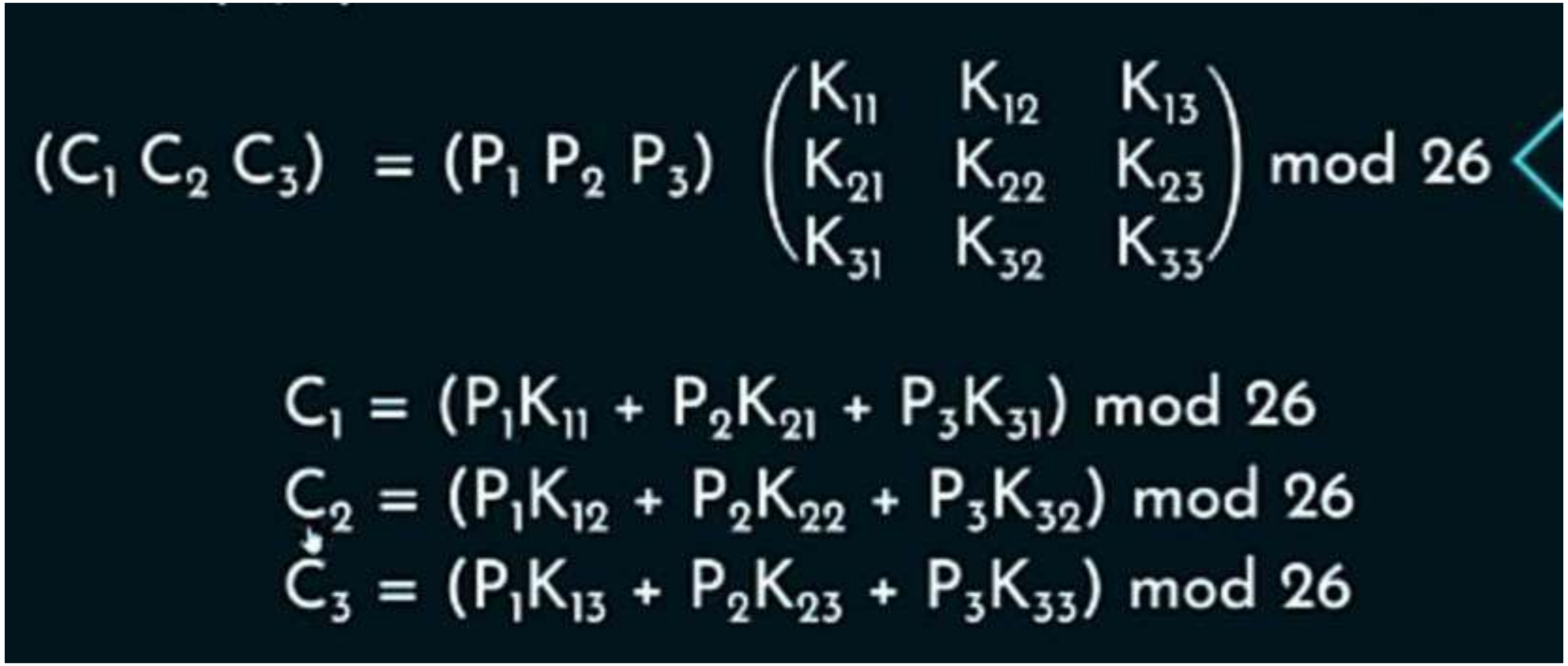
Encryption:



This can be expressed as

$C = E(K,P) = P \times K \bmod 26$

Here C:Cipher,
E:Encryption,
K:Key,
P:Plain text.



$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3)\begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$

Hill Cipher example:

Plaintext: ACT, Key: GYBNQKURP

We have to encrypt the message ‘ACT’ (n=3).

The key is ‘GYBNQKURP’ which can be written as the nxn matrix: Here G-> 6 number, Y->24 number,B->1 number so…on

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

Here A->0 number, C->2 number,T->19 number

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \text{Mod } 26$$

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \text{Mod } 26 \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix},$$

Here 15->P, 14->O, 7->H, so cipher text is POH

Decryption: To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix

$$P = D(K,C) = C\,K^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$$

Example:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

Hill Cipher: For the previous Ciphertext ‘POH’:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Here 0->A, 2->C, 19->T, hence plain text is ACT

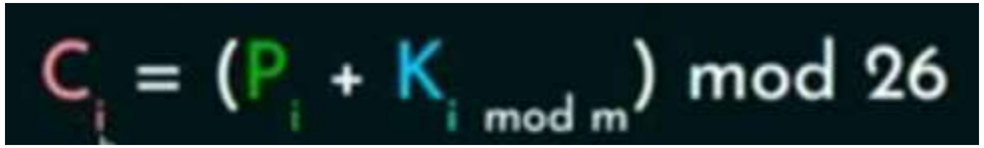
5) Polyalphabetic Cipher:

To improve on the simple monoalphabetic technique.

i)Vigenere Cipher:

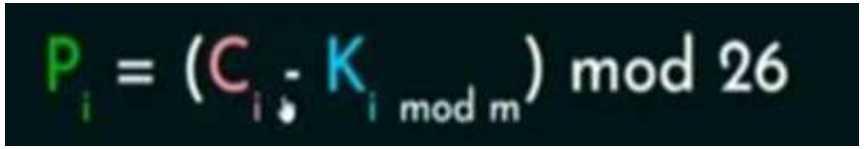
It consists of the 26 Caesar ciphers with shifts of 0 through 25.

Encryption process:



$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

Decryption process :



$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

Vigenere Cipher: Example:

Key: deceptivedeceptivedeceptive, Plaintext: wearediscoveredsaveyourself

Ciphertext :ZICVTWQNGRZGVTWAVZHCQYGLMG

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19

Key	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	22	0	21	25	7	2	16	24	6	11	12	6	9

ii).One Time Pad:

Improvement to the vigenere cipher.

It yields the ultimate in Security.

Random key that is as long as the message.

The Key need not be repeated.

In addition, the key is to be used to encrypt and decrypt a single message and then is discarded.

Each new message requires a new key of the same length as the new message

It produces random output.

No statistical relationship to the plaintext.

Because the cipher contains no information whatsoever about the plaintext, there is simply no way to break the code.

The code is unbreakable.

The security of the one-time pad is entirely due to the randomness of the key.

Two Fundamental Difficulties:

The practical problem of making large quantities of random keys.

Even more daunting is the problem of key distribution and protection.

Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.

Ex:**Input:** Message = HELLO, Key = MONEY

Output: Cipher – TSYPM, Message – HELLO

Explanation: Part 1: Plain text to Ciphertext

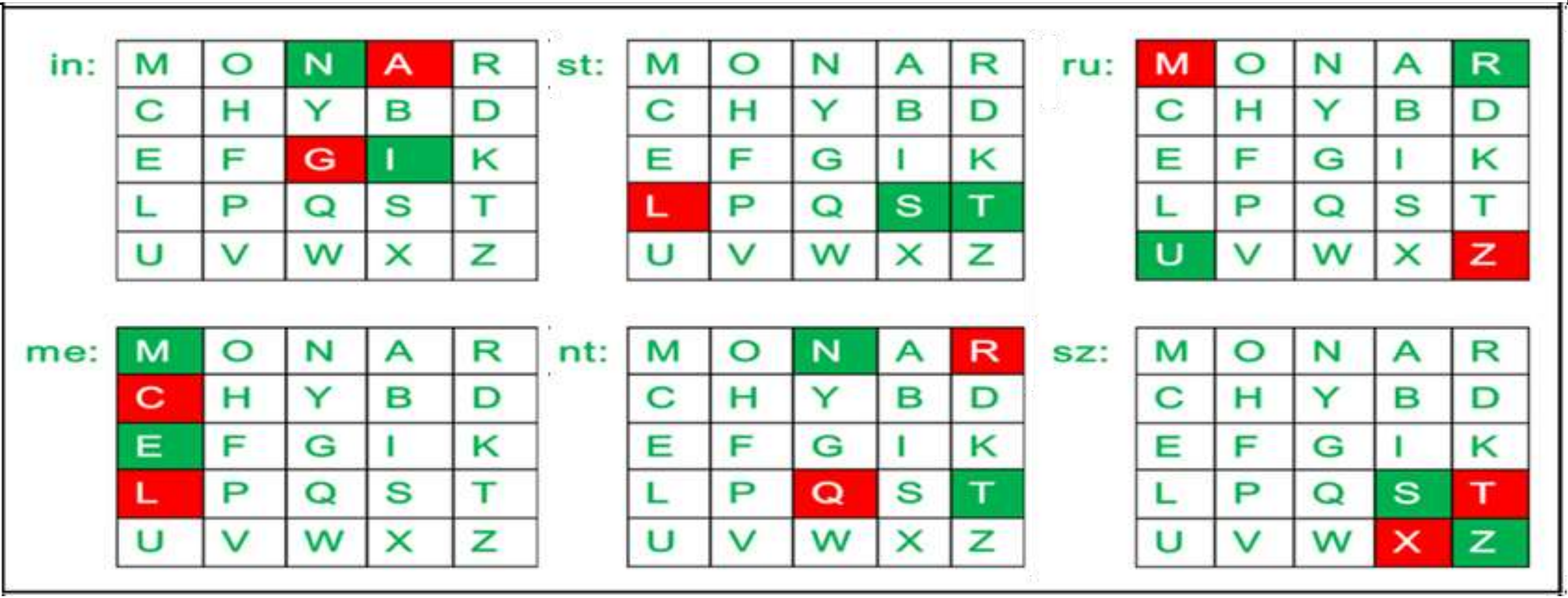
Plain text - H E L L O = 7 4 11 11 14, Key - M O N E Y = 12 14 13 424

Plain text + key = 19 18 24 15 38

Cipher – TSYPM

For example:

Plain Text: "instruments“, Keyword: Monarchy, After split: in st ru me nt sz



in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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

Encrypted Text: gatlmzclrqtx

TRANSPOSITION TECHNIQUES

➢ Transposition Techniques

- In transposition Techniques, the letters of plain text remain same, but their original sequence is changed in symmetric way.

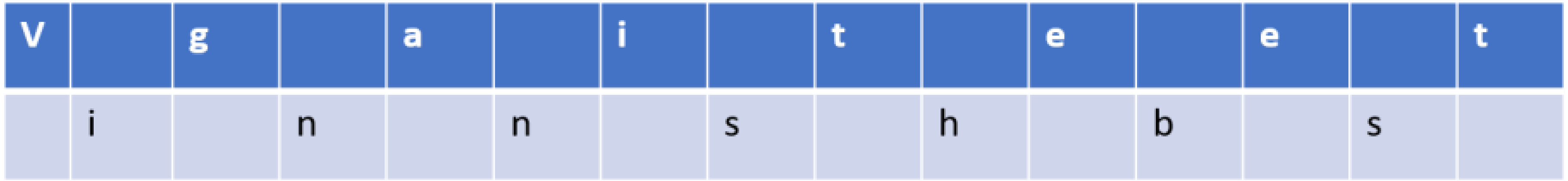
i) Rail Fence Technique:

- The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Example:

Encipher the message “ Vignan is the best” with a rail fence of depth 2

- Plaintext: Vignan is the best
- Depth: 2



V		g		a		i		t		e		e		t
	i		n		n		s		h		b		s	

- Ciphertext:VGAITEETINNSHBS

ii) Row Column Transposition:

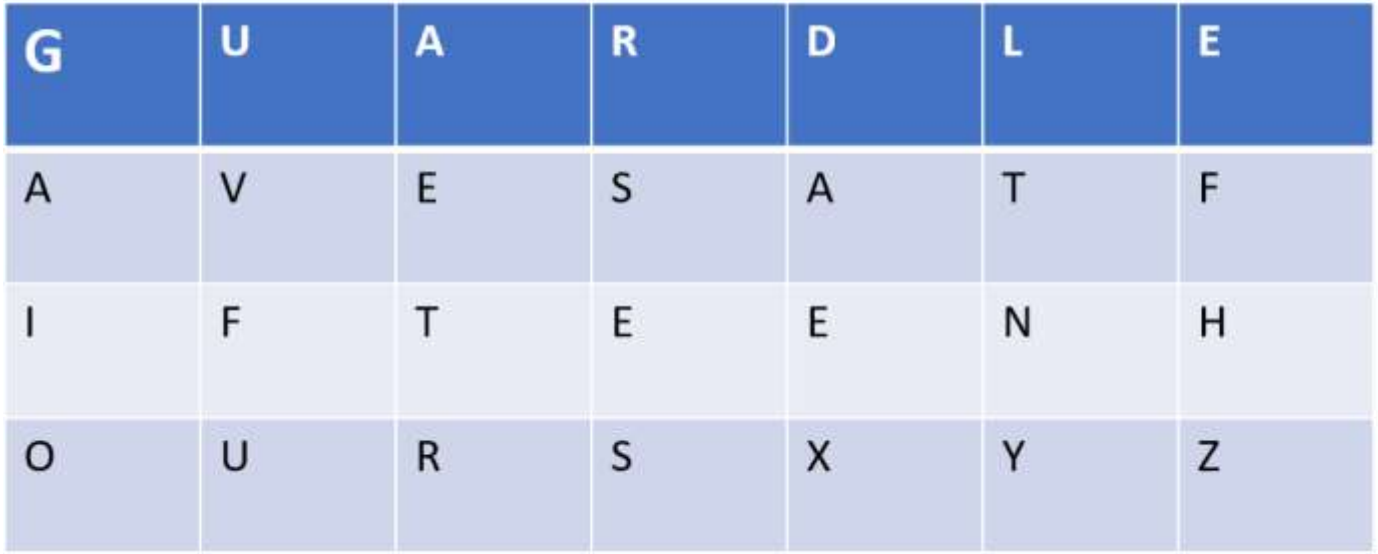
- A More Complex Scheme.
- Create Rectangle box.
- Write : Row by Row
- Read :Column by Column

Example: Encrypt the message “ Guard leaves at fifteen hours”

Plaintext: Guard leaves at fifteen hours

Key : 5263174

5 2 6 3 1 7 4



G	U	A	R	D	L	E
A	V	E	S	A	T	F
I	F	T	E	E	N	H
O	U	R	S	X	Y	Z

Ciphertext:DAEXUVFURSESEFHZGAIOAETRLTNY

➢ Steganography

- The technique of hiding message in another message or picture or audio/sound or video or any another source is known as steganography.
- Example for Steganography:

1) **Image Steganography:** Hide message in a message without disturbing the picture.
2) **Audio Steganography:** Hide message in an audio stream without effecting the actual sound
3) **Video Steganography:** Hide message in a video
4) **Invisible ink:** number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
5) **Pin Punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

A plaintext message may be hidden in any **one of the two ways**. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. e.g.,

(i) the sequence of first letters of each word of the overall message spells out the real (Hidden) message.

(ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been used historically, some of them are:

(iii) **Character marking** – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.

(iv) **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.

(v) **Pin punctures** – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.

(vi) **Typewritten correction ribbon** – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of steganography

- Requires a lot of overhead to hide a relatively few bits of information.
- Once the system is discovered, it becomes virtually worthless.

Symmetric-key Cryptography:

In Symmetric-key Cryptography the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

- It uses one key for both encryption and decryption.
- Faster and more efficient for large amounts of data.
- Requires a secure method to share the key between sender and receiver.
- Common algorithms include AES, DES, Blowfish.

Asymmetric key Cryptography:

Asymmetric key Cryptography is one of the most common cryptographic methods that involve using a Two keys, where one key is used to encrypt data and the second one is used to decrypt an encrypted text. The second key is kept highly secret, while the first one which is called a public key can be freely distributed among the service's users.

- It uses two keys a public key for encryption and a private key for decryption.
- More secure but slower than symmetric encryption.
- No need to share the private key, reducing the risk of exposure.
- Common algorithms include RSA, Diffie-Hellman.

UNIT - II

Symmetric key Ciphers:

- Block Cipher principles,
- DES,
- AES,
- Blowfish,
- RC5,
- IDEA,
- Block cipher operation,
- Stream ciphers,
- RC4.

Asymmetric key Ciphers:

- Principles of public key cryptosystems,
- RSA algorithm,
- Elgamal Cryptography,
- Diffie-Hellman Key Exchange,
- Knapsack Algorithm.

Symmetric key Ciphers:

- Block Cipher principles,

lock ciphers are a type of encryption algorithm that processes fixed-size blocks of data, typically 64 or 128 bits, to produce ciphertext. The of a block cipher involves several key principles to ensure the security and efficiency of the algorithm.

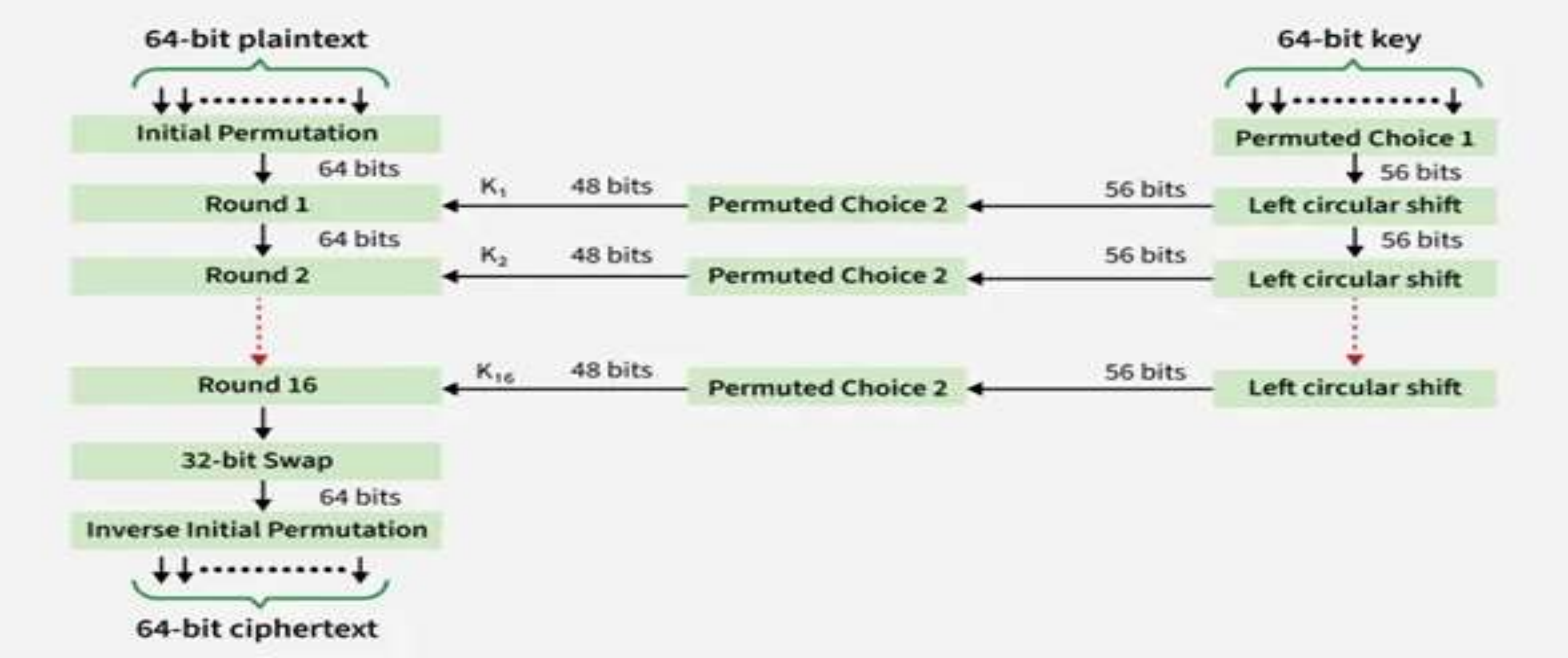
Number of Rounds

The number of rounds in a block cipher is crucial for its security. Each round applies a transformation to the data, making it more complex and secure. For example, the Data Encryption Standard (DES) uses 16 rounds**Design of Function F**

The core part of the Feistel block cipher structure is the round function, denoted as F.

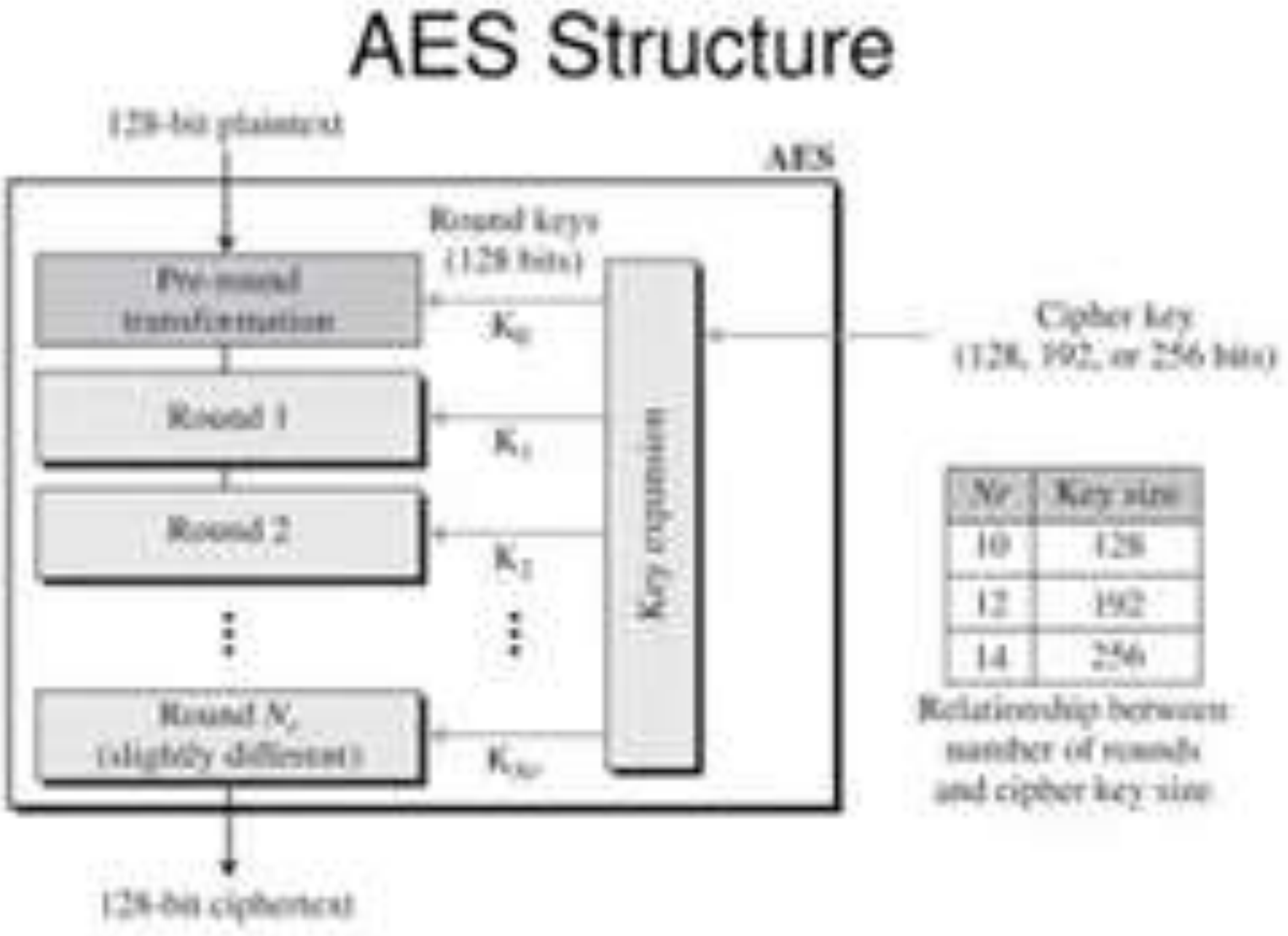
- DES

Data Encryption Standard (DES) is a symmetric block cipher. By 'symmetric', we mean that the size of input text and output text (ciphertext) is same (64-bits).



- AES

Advanced Encryption Standard (AE



AES Structure

Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

- Blowfish,

Blowfish is an encryption technique designed by **Bruce Schneier** in 1993 as an alternative to the 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 is a symmetric block cipher algorithm.

•**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]

THANK YOU