22CS701 CRYPTOGRAPHY AND CYBER SECURITY

Topics:

- **Computer Security Concepts**
- **OSI Security Architecture**
- **Network Security Model**
- **Classical Encryption Techniques**

➢ **Substitution**

➢ **Transposition**

Computer Security Concepts

- Computer security, also known as **cybersecurity**, refers to the protection of computer systems and networks from information disclosure, theft, damage, or disruption.
- **Confidentiality**
- **Integrity**
- **Availability**
- **Authentication**
- **Authorization**
- **Non-Repudiation**
- **Threats and Vulnerabilities**
- **Security Mechanisms**
- **Security Policies**
- **CIA Triad (Core of Security)**

INTRODUCTION

- CRYPTOLOGY

  Cryptology is the study of codes, both creating and solving them. It's a combination of Cryptography and Cryptanalysis

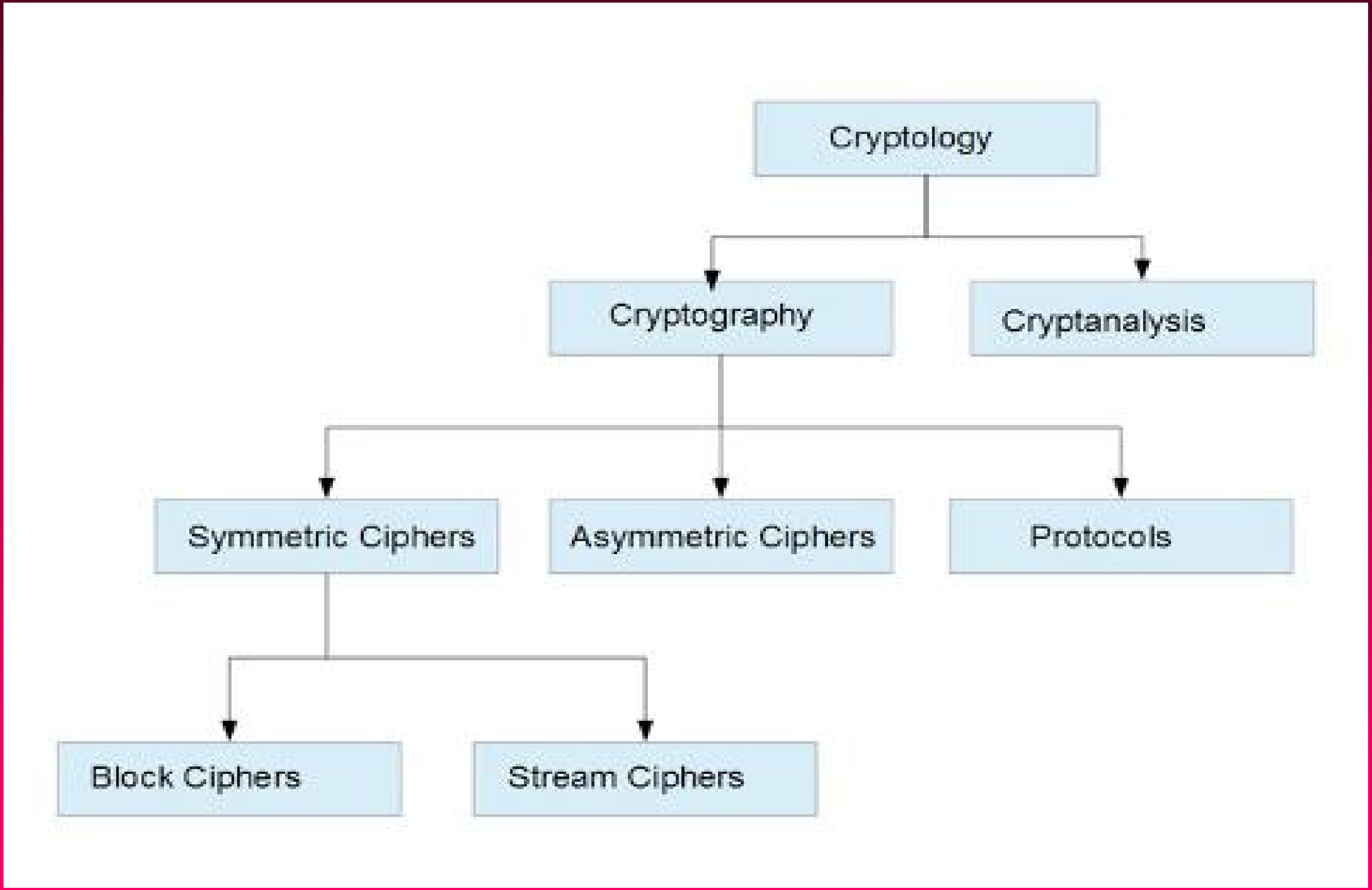
- CRYPTOGRAPHY

  Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.

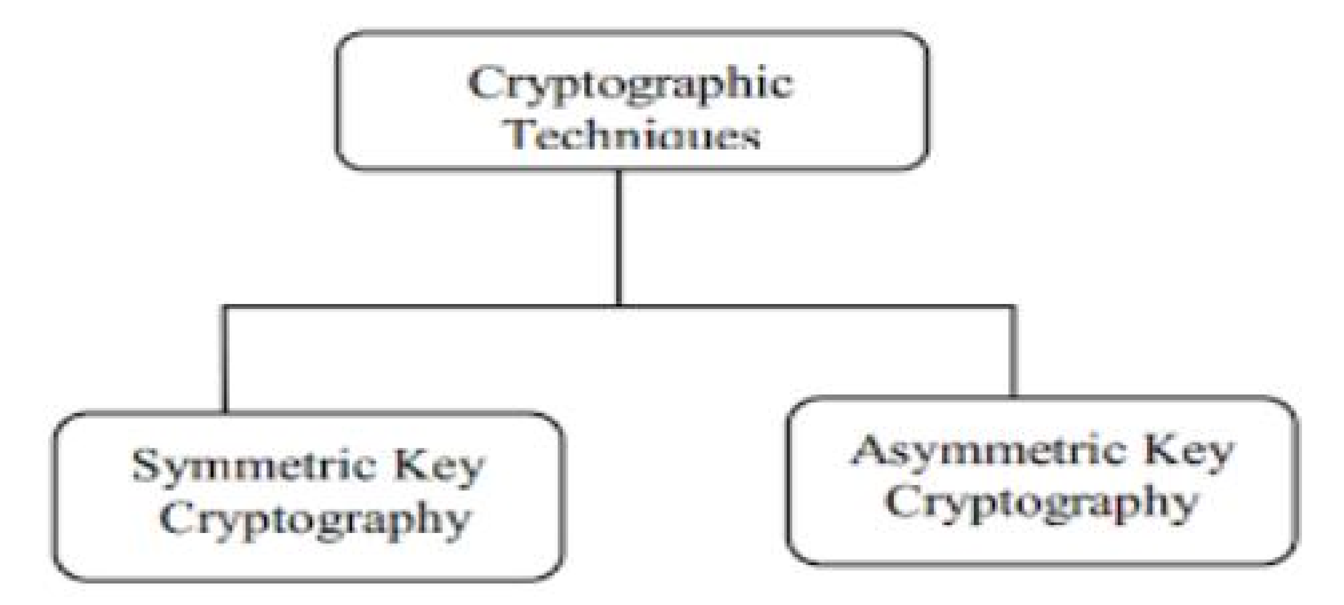
- CRYPTANALYSIS

  Cryptanalysis is the process of deciphering coded messages without being told the key.

CRYPTOLOGY


Cryptology
Cryptography
Cryptanalysis
Symmetric Ciphers
Asymmetric Ciphers
Protocols
Block Ciphers
Stream Ciphers

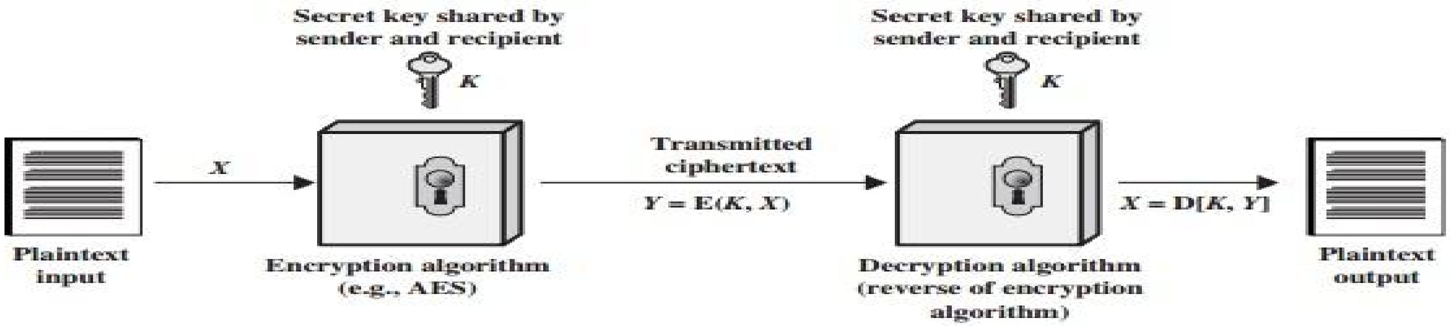
TYPES OF CRYPTOGRAPHY



Symmetric cipher model: Sender and receiver shares the same secret key

Asymmetric cipher model: Sender and receiver shares the different key pairs

SYMMETRIC CIPHER MODEL



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

INGREDIENTS OF SYMMETRIC CIPHER MODEL

1.Plain text-Original Message

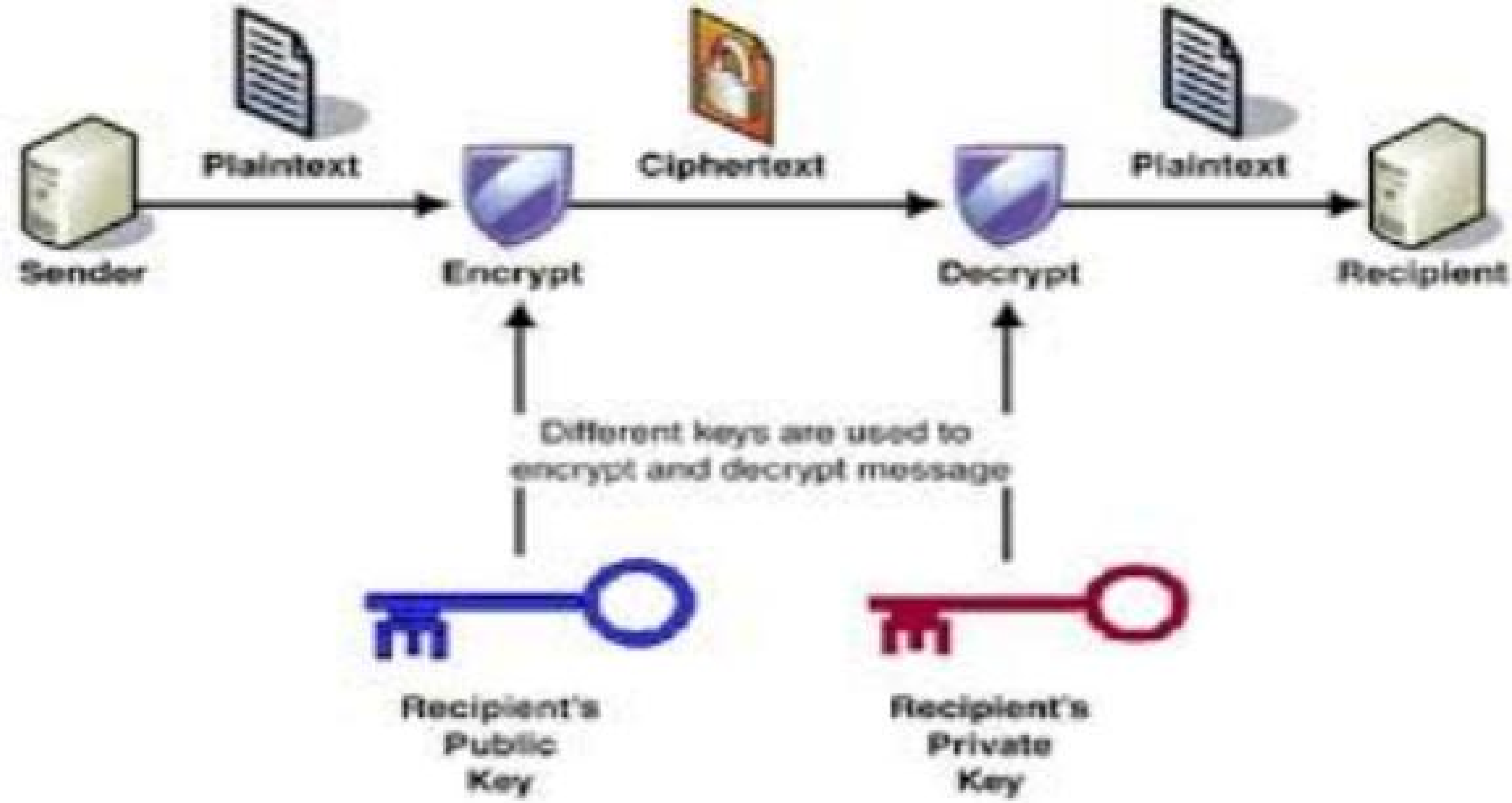
2.Encryption Algorithm-Converting plaintext into cipher text using Substitution and Transposition Technique

3.Secret key-Its an independent values of P.T and algorithm An adversary cannot decrypt the message without knowing the **secret key**

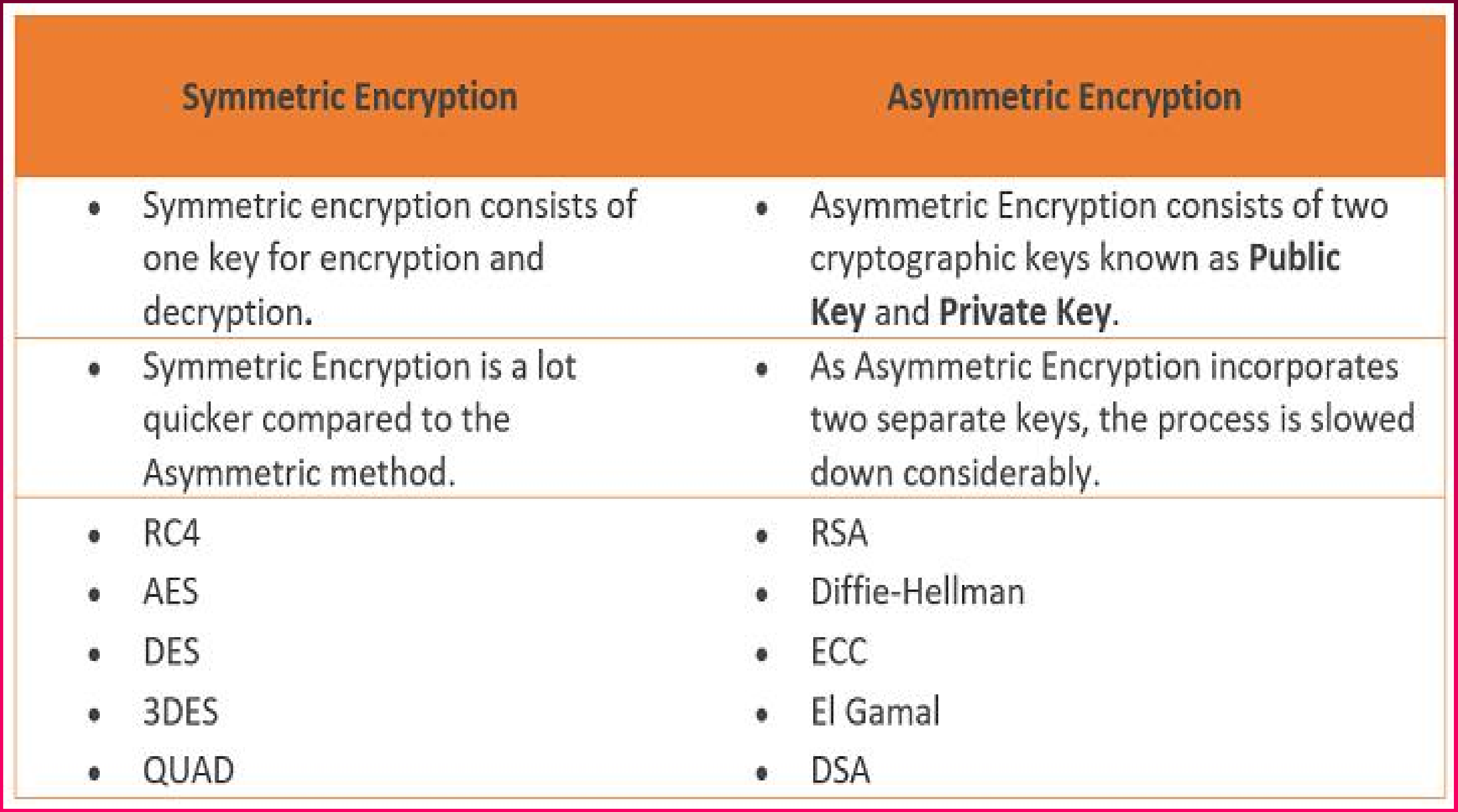
4.Cipher text-unreadable form

5.Decryption Algorithm-opposite process of encryption algorithm

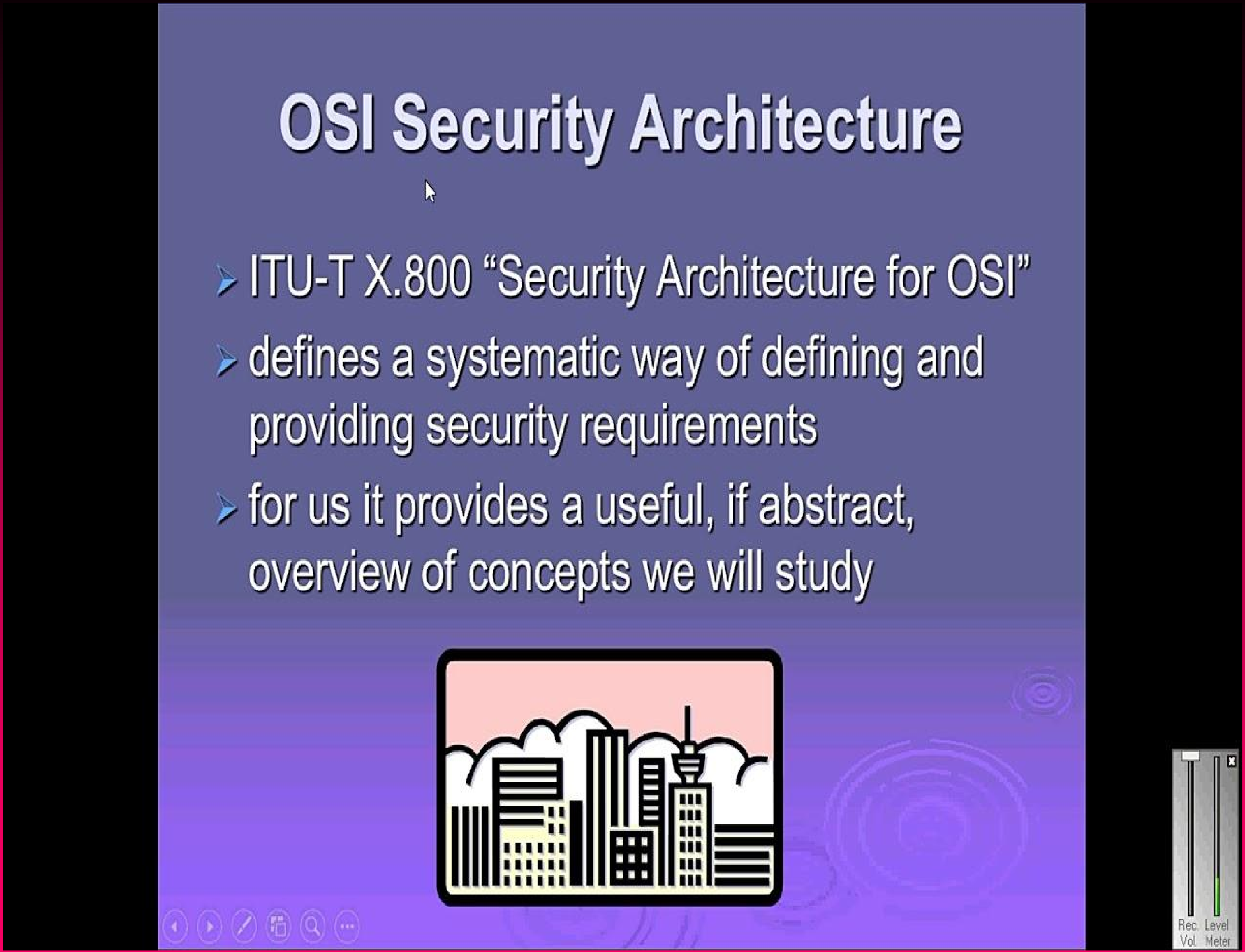
ASYMMETRIC MODEL



Examples of Symmetric and Asymmetric key cryptography



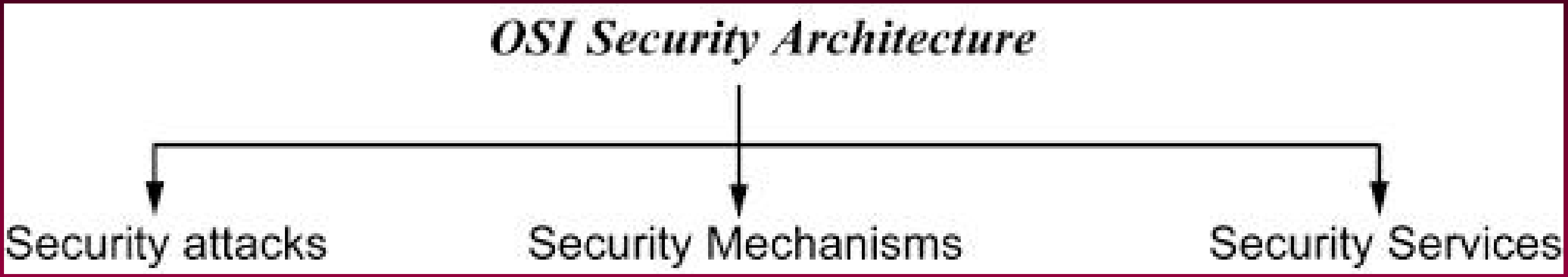
Symmetric Encryption	Asymmetric Encryption
- Symmetric encryption consists of one key for encryption and decryption.	- Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
- Symmetric Encryption is a lot quicker compared to the Asymmetric method.	- As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
- RC4 - AES - DES - 3DES - QUAD	- RSA - Diffie-Hellman - ECC - El Gamal - DSA



OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

OSI SECURITY ARCHITECTURE



OSI Security Architecture

Security attacks

Security Mechanisms

Security Services

Security Services: Specific kind of protection to System resources

Security Attacks: Any action that compromises the security of information owned by an organization

Security Mechanisms: A process of detect ,prevent or recover from a security Attack

Security Services

- Authentication – Assurance between the two communicating entities
- Access Control-Avoid Unauthorized use of Resources
- Data Confidentiality-Protection of data from unauthorized use of resources
- Data Integrity-Data Received exactly sent by an Authorized entity
- Non Repudiation- Protection against denial of service

Security Attacks

- Its an unethical activity gain the information with out any authorized permission
- Types:
- Active – data alteration
- Passive – Eaves dropping

Active Attacks:

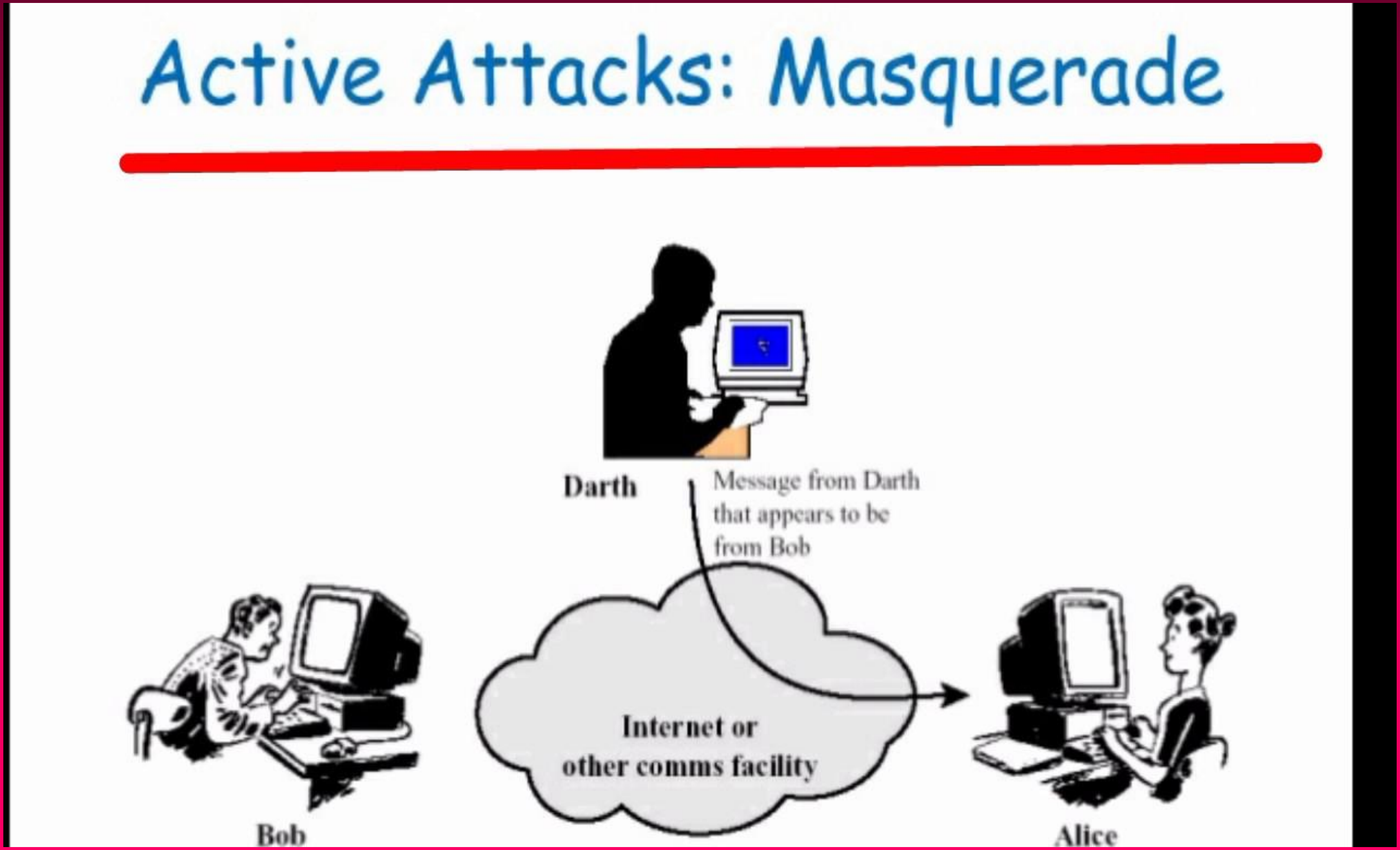
- Masquerade
- Replay
- Modification of Messages
- Denial of Service

Passive Attacks:

- Release of message contents
- Traffic Analysis

Active Attacks

(i)Masquerade - one entity pretends to be a different entity

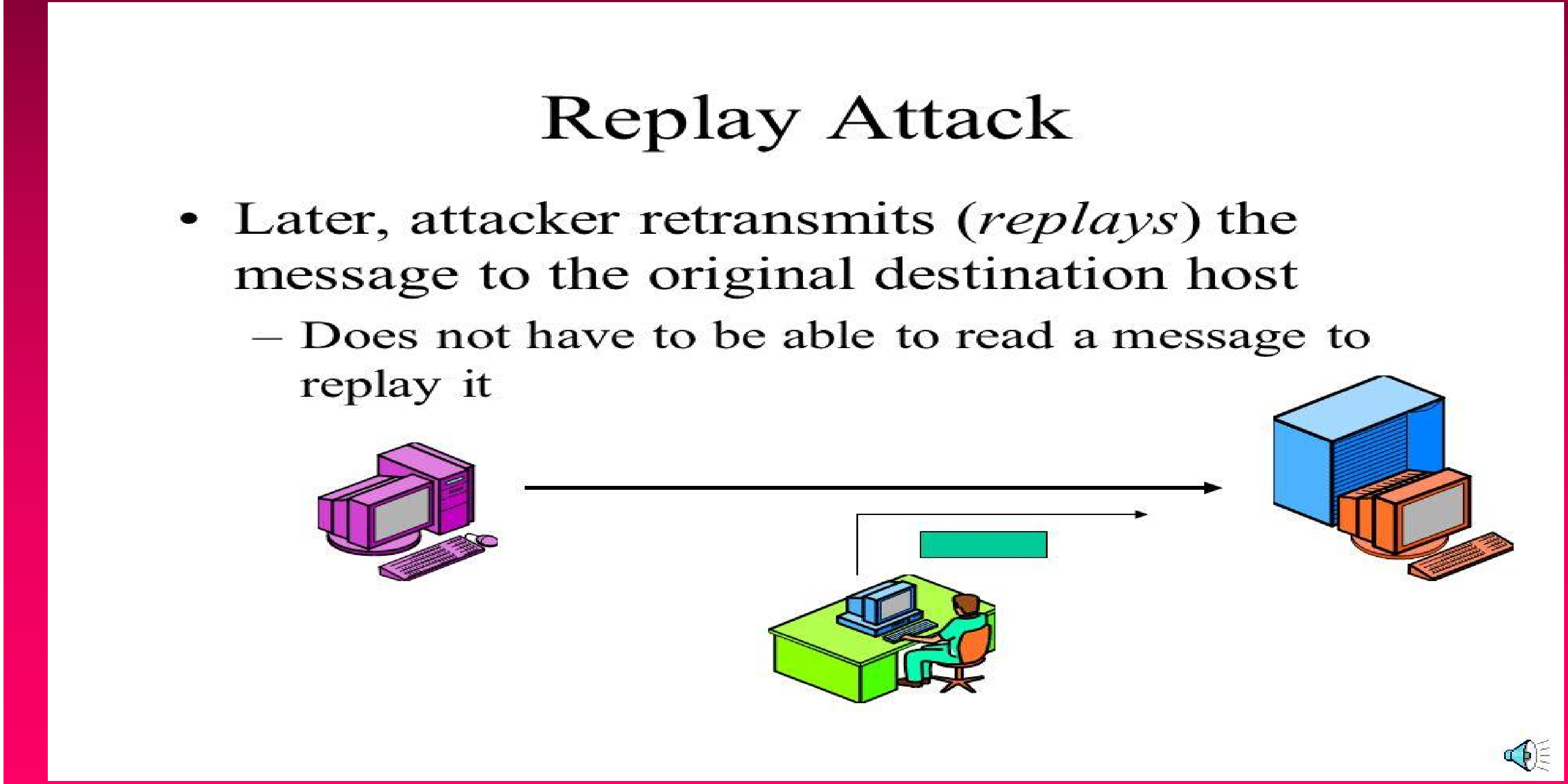


Active Attacks: Masquerade

Message from Darth that appears to be from Bob

Active Attacks

- Replay-Capture a unit of data and retransmit the data

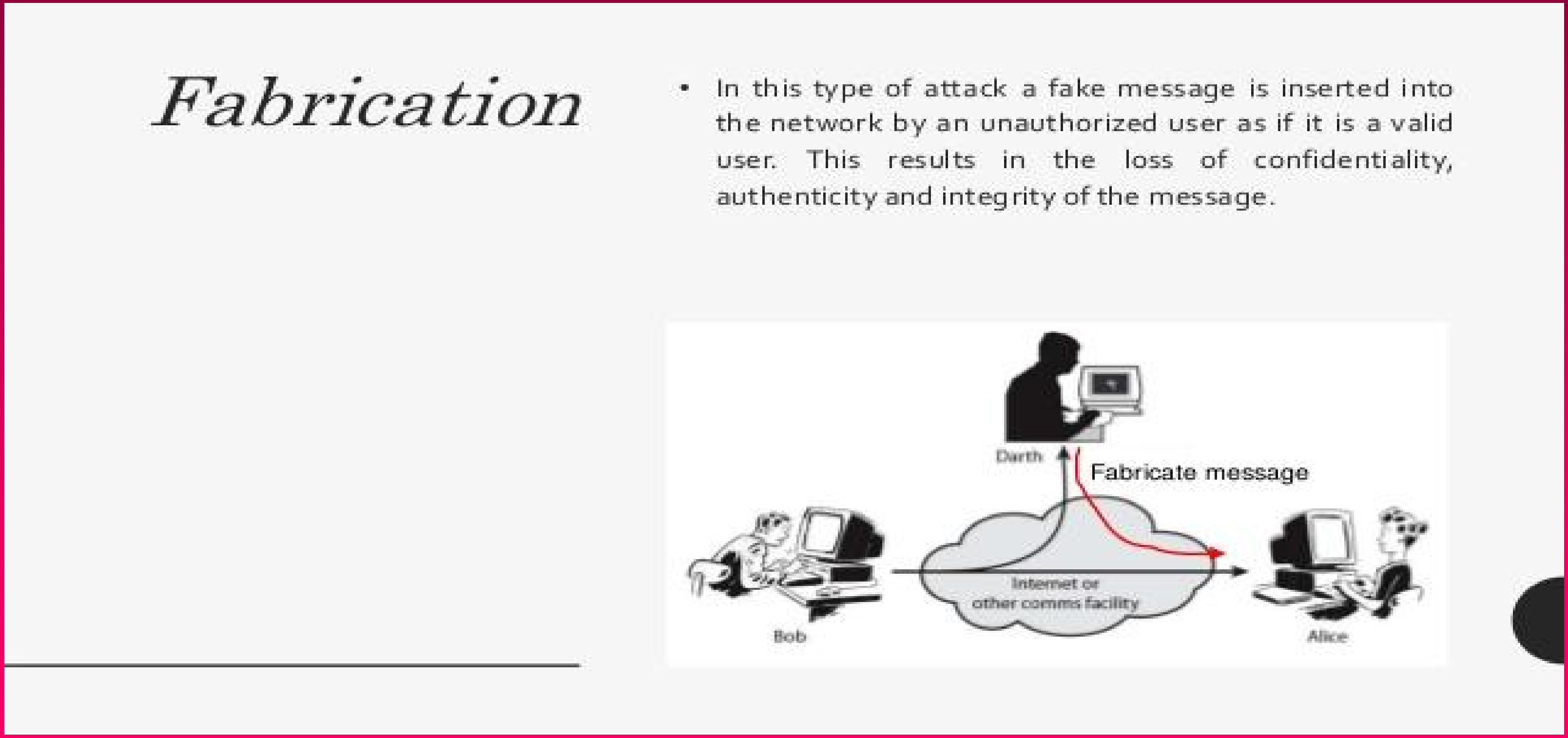


Replay Attack

- Later, attacker retransmits (*replays*) the message to the original destination host
  - Does not have to be able to read a message to replay it

Active Attacks

- Modification of Messages – Some portion of the messages is altered or deleted or reordered to produce unauthorized effect

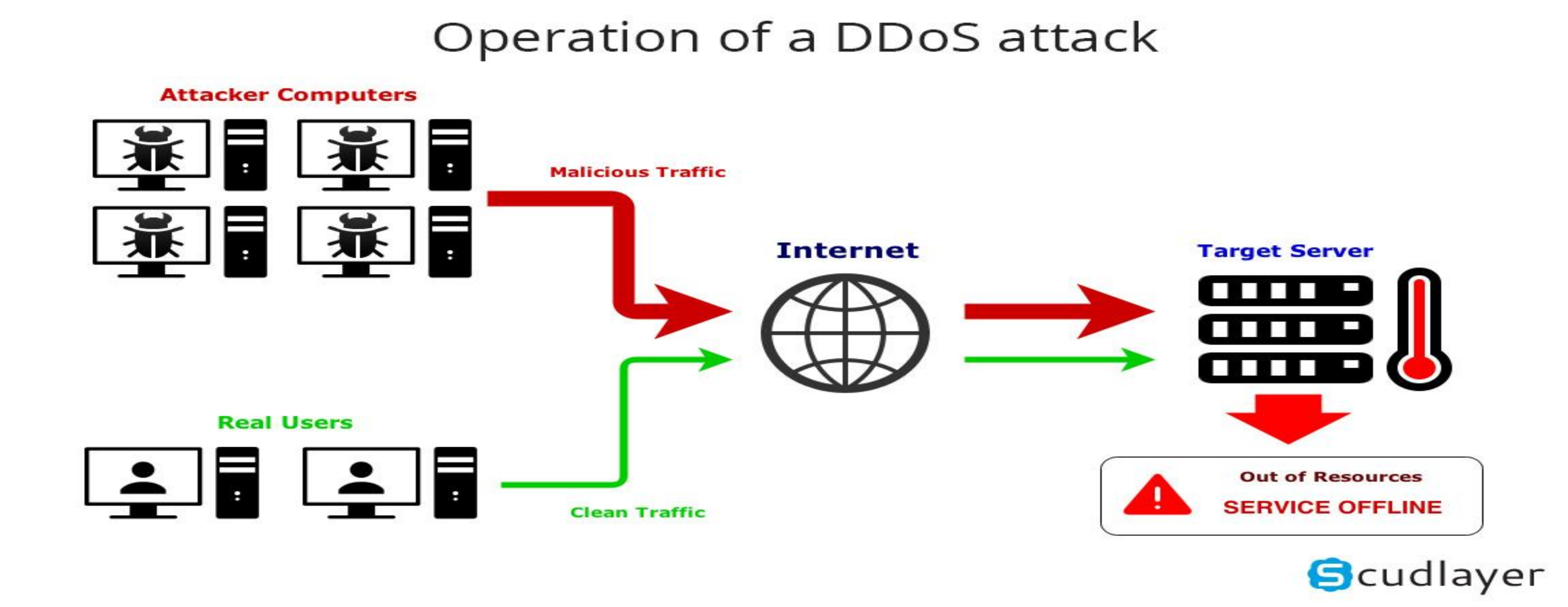


Fabrication

- In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user. This results in the loss of confidentiality, authenticity and integrity of the message.

Active Attacks

- Denial of Service- This attack may have a specific target it may be a single system or a Network
- All messages directed to the single system..
- DDoS



Passive Attacks

- The main objective of passive attack is monitoring the transmission and obtain the information is being transmitted
- Release of Message contents-the **contents** of the transmitted data. Passive attacks are very difficult to detect because they do not involve any alteration of the data
- Traffic Analysis- eavesdropping **attacks**, **traffic analysis attacks** are based on what the attacker hears in the network

Security Mechanisms

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Routing Control
- Notarization
- Authentication Access

STEGANOGRAPHY

- **Steganography** is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection;
- the secret data is then extracted at its destination. The use of **steganography** can be combined with encryption as an extra step for hiding or protecting data

TYPES:

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

NETWORK SECURITY MODEL

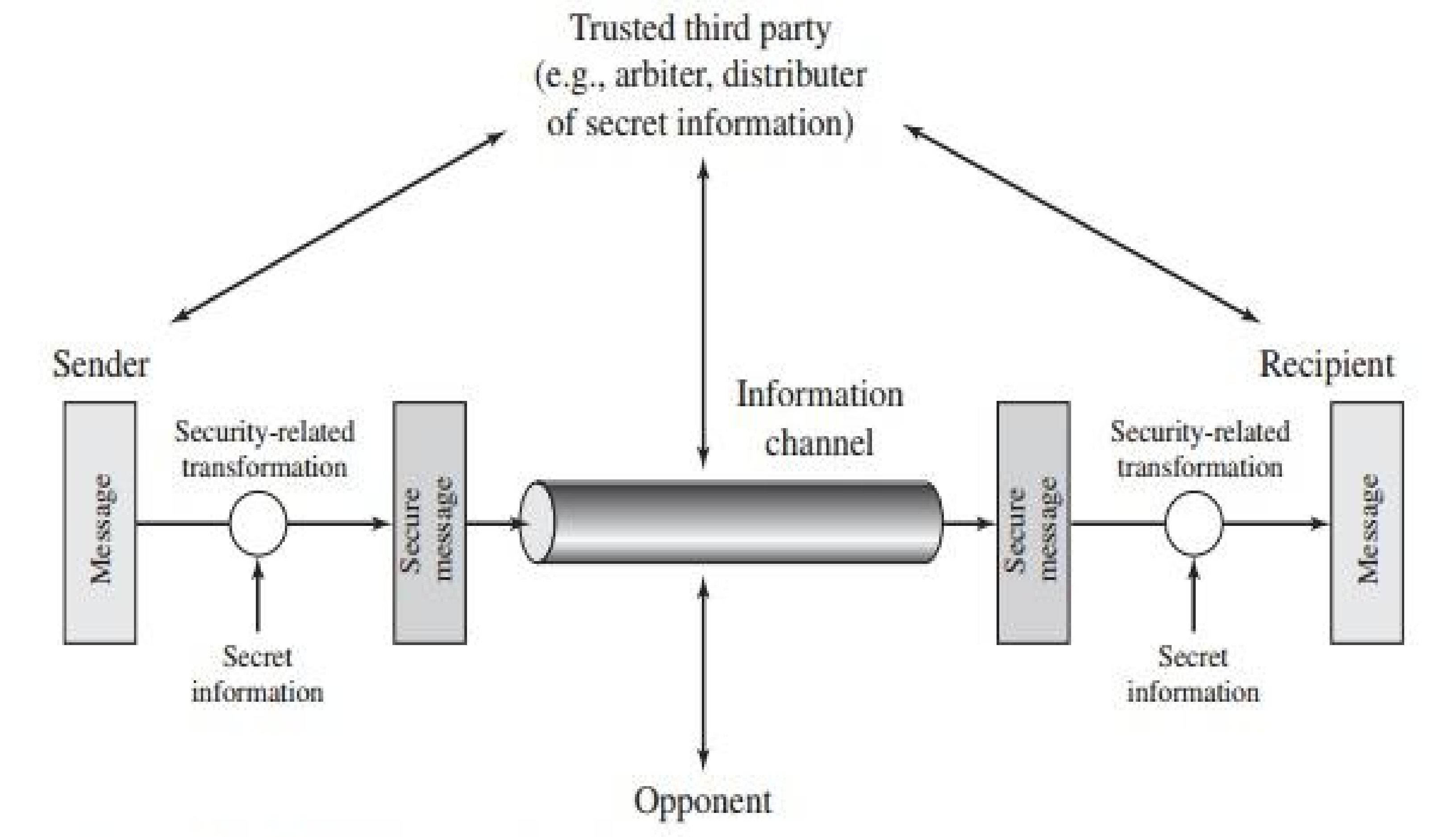


Figure 1.4 Model for Network Security

CLASSICAL ENCRYPTION TECHNIQUES

- Substitution
- Caesar Cipher
- Mono Alphabetic
- Poly Alphabetic or vigenere Cipher
- Playfair cipher
- Hill Cipher
- Vernam Cipher or One time pad

CLASSICAL ENCRYPTION TECHNIQUES

- Transposition
- Rail Fence Method
- Simple columnar Method

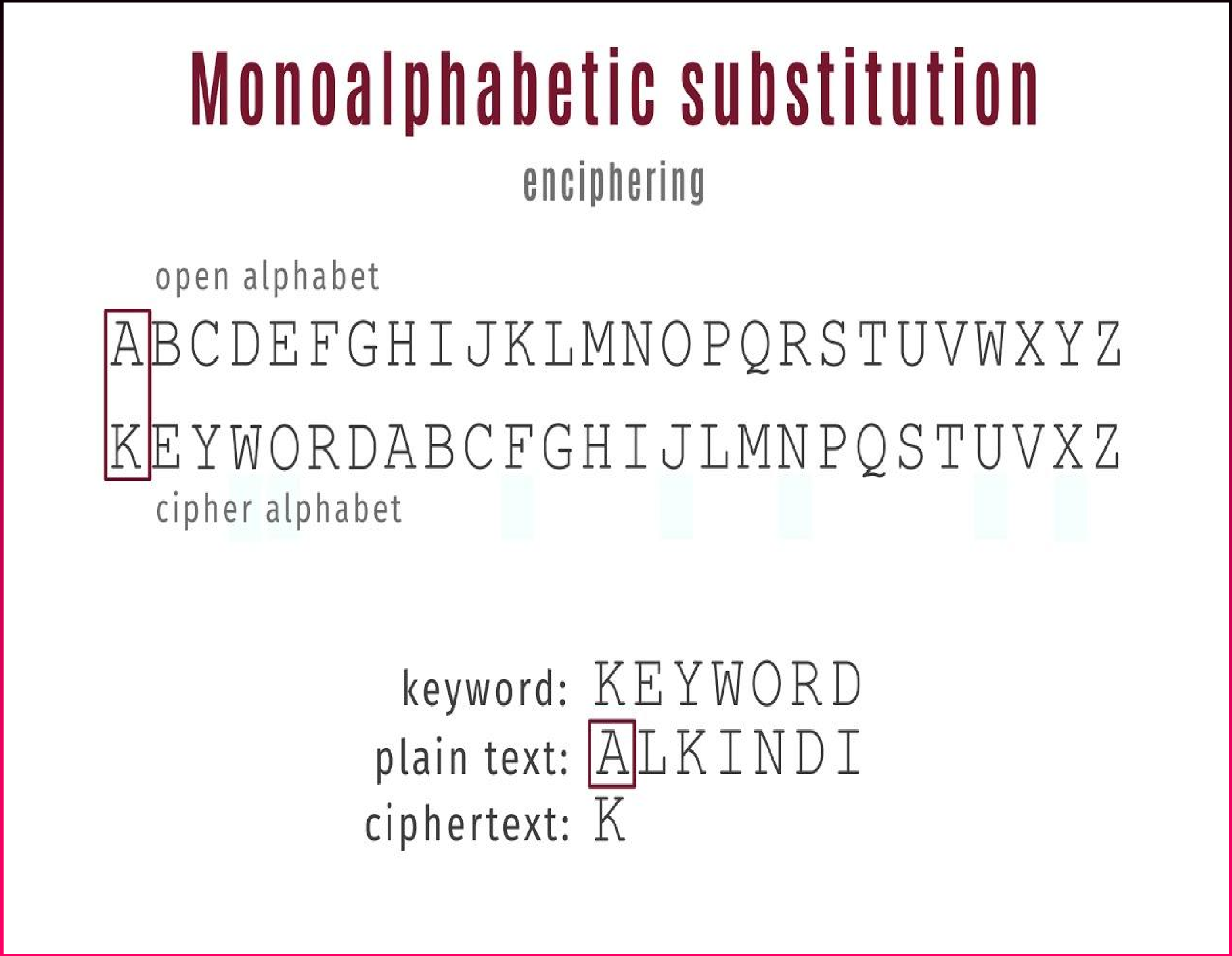
Caesar Cipher

Encryption

- C=(P+K) mod 26
- C-cipher Text
- P-plain text
- K-Secret key

Decryption

- P=(C-K) mod 26



Monoalphabetic substitution

enciphering

open alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

KEYWORDABCFGHIJLMNPQSTUVXZ

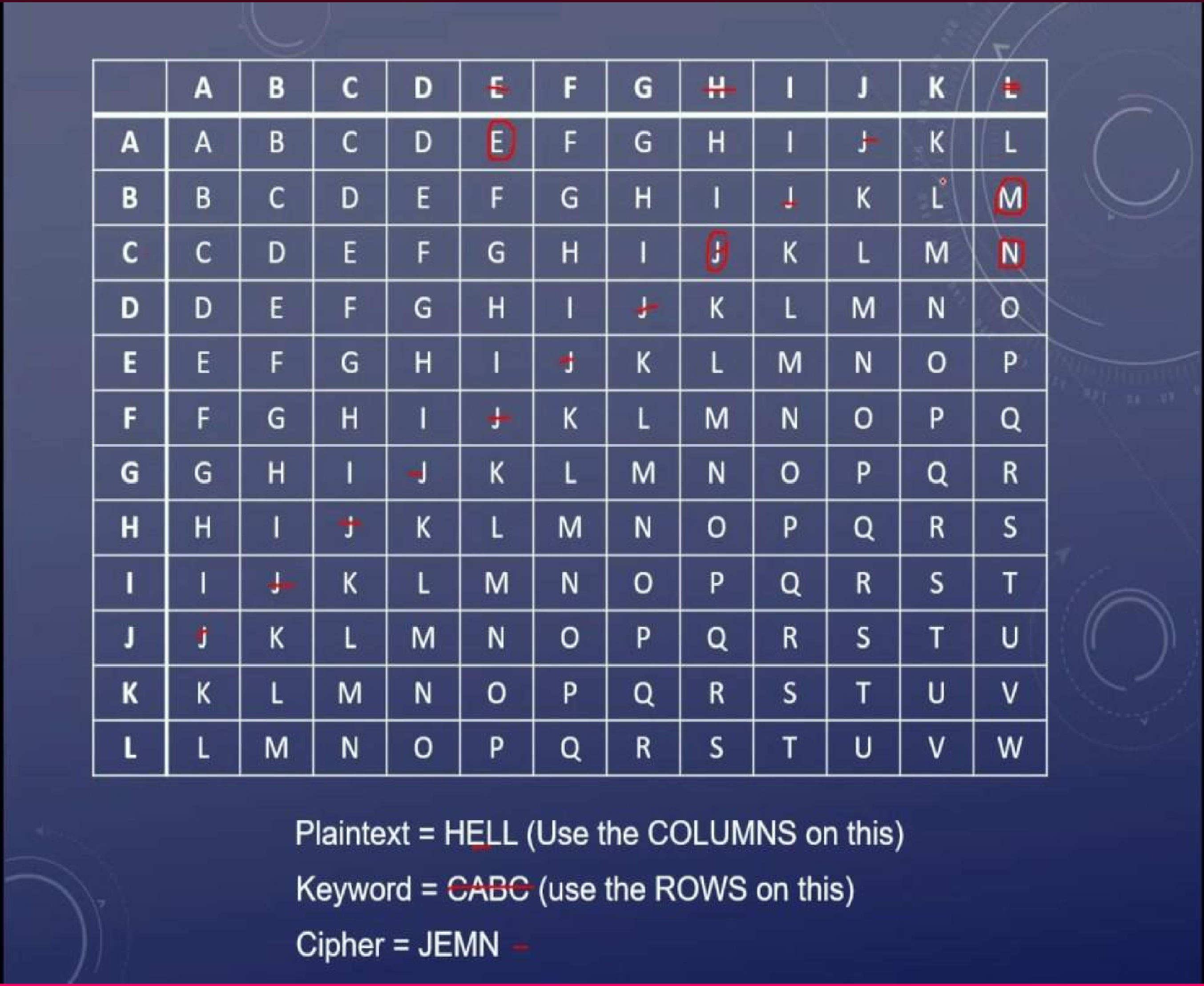
cipher alphabet

keyword: KEYWORD

plain text: ALKINDI

ciphertext: K

Poly alphabetic Cipher



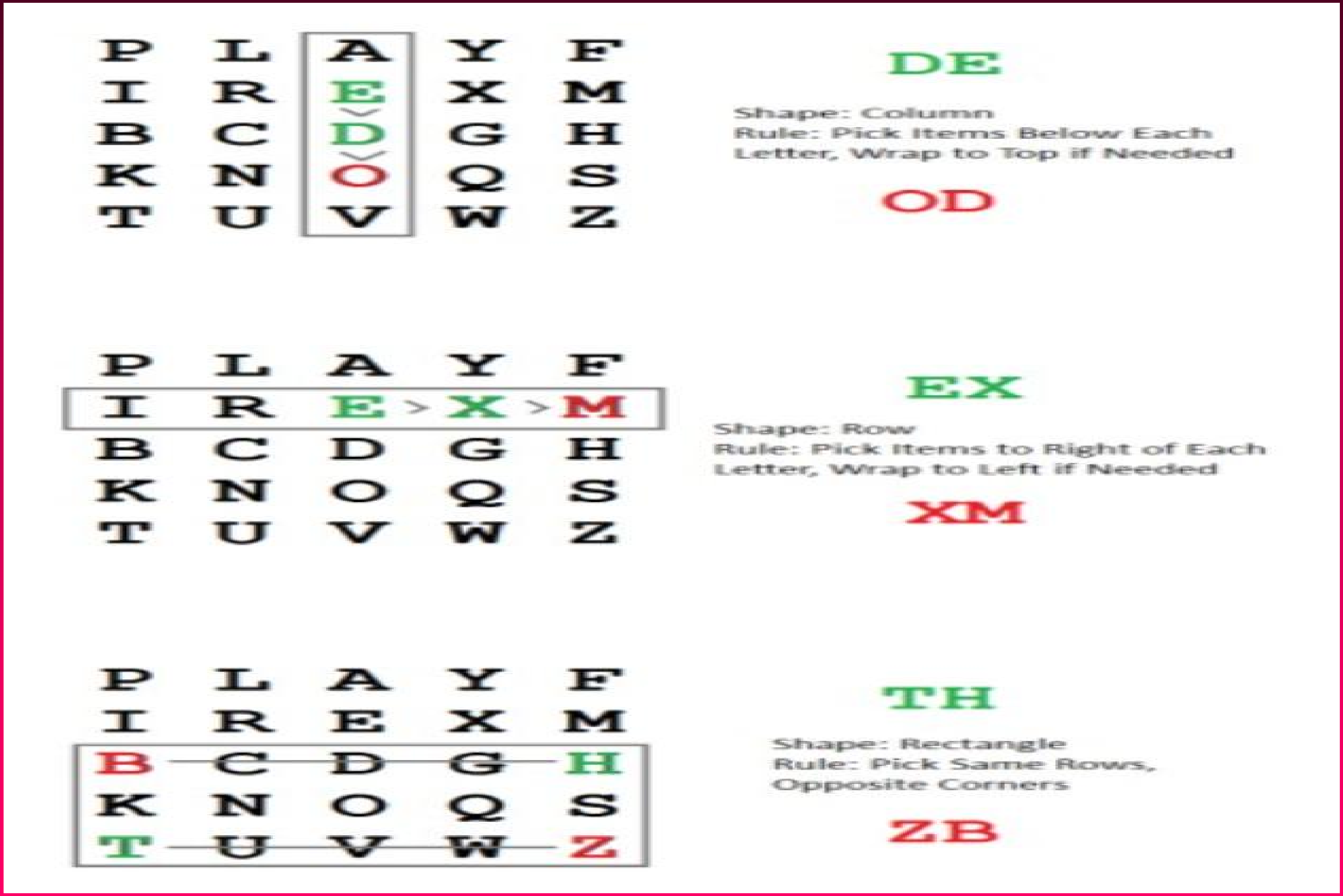
	A	B	C	D	~~E~~	F	G	~~H~~	I	J	K	~~L~~
A	A	B	C	D	E	F	G	H	I	~~J~~	K	L
B	B	C	D	E	F	G	H	I	~~J~~	K	L	M
C	C	D	E	F	G	H	I	J	K	L	M	N
D	D	E	F	G	H	I	~~J~~	K	L	M	N	O
E	E	F	G	H	I	~~J~~	K	L	M	N	O	P
F	F	G	H	I	~~J~~	K	L	M	N	O	P	Q
G	G	H	I	~~J~~	K	L	M	N	O	P	Q	R
H	H	I	~~J~~	K	L	M	N	O	P	Q	R	S
I	I	~~J~~	K	L	M	N	O	P	Q	R	S	T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

Plaintext = HELL (Use the COLUMNS on this)

Keyword = ~~CABC~~ (use the ROWS on this)

Cipher = JEMN

Play fair cipher



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

DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

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

EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

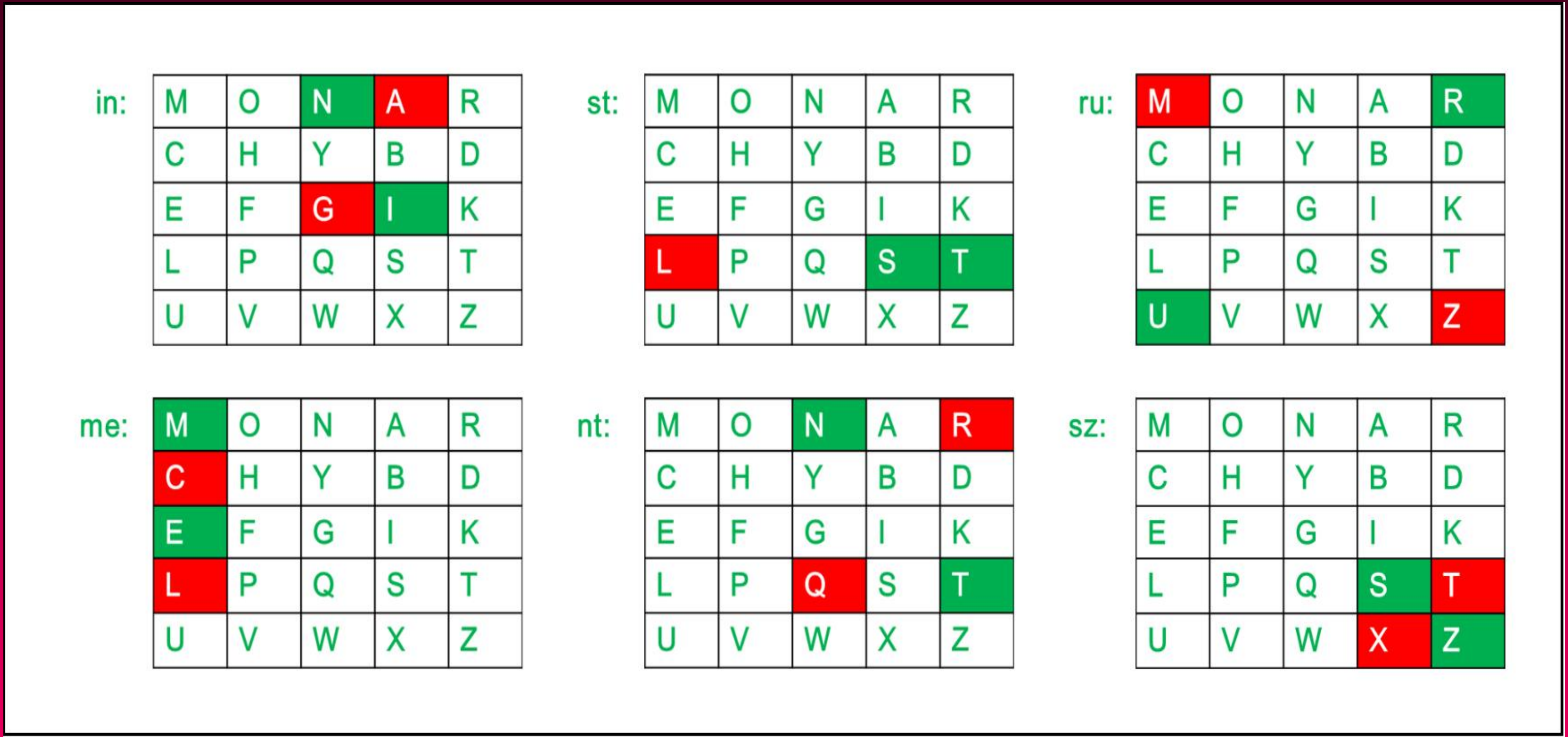
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

Play fair Cipher



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:

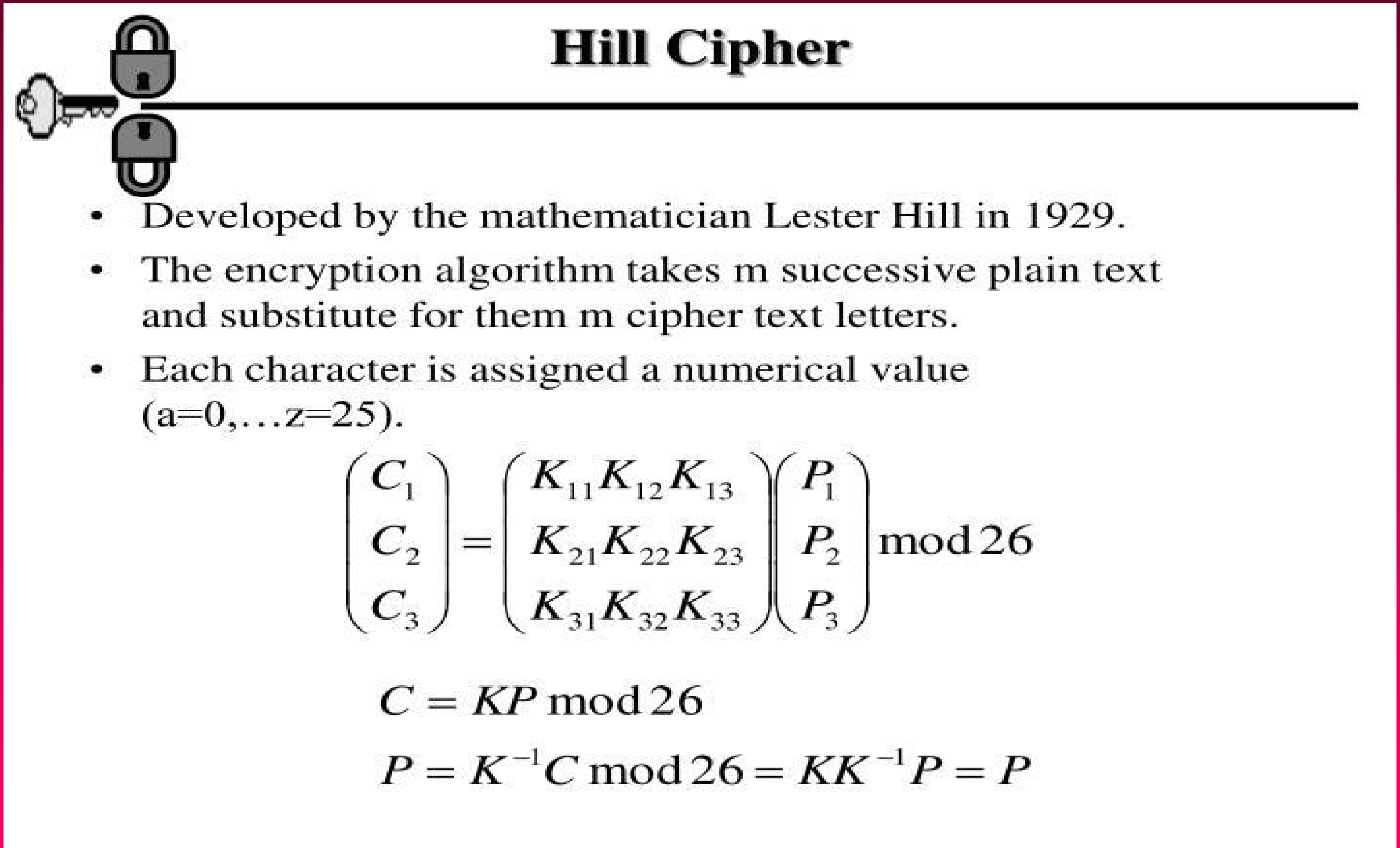
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Plaintext : CRYPTOGRAPHY

Secretkey:MONARCHY

CipherText:DM HQ PR KN OS YB

Hill cipher



Hill Cipher

- Developed by the mathematician Lester Hill in 1929.
- The encryption algorithm takes m successive plain text and substitute for them m cipher text letters.
- Each character is assigned a numerical value (a=0,…z=25).

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

$$C = KP \bmod 26$$

$$P = K^{-1}C \bmod 26 = KK^{-1}P = P$$

…Decryption

- Key = $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

Step 1 : Find Determinant of Key

Step 2 : Transpose Key Matrix

Step 3 : Find Minor

Step 4 : Find Co-Factor

Vernam cipher

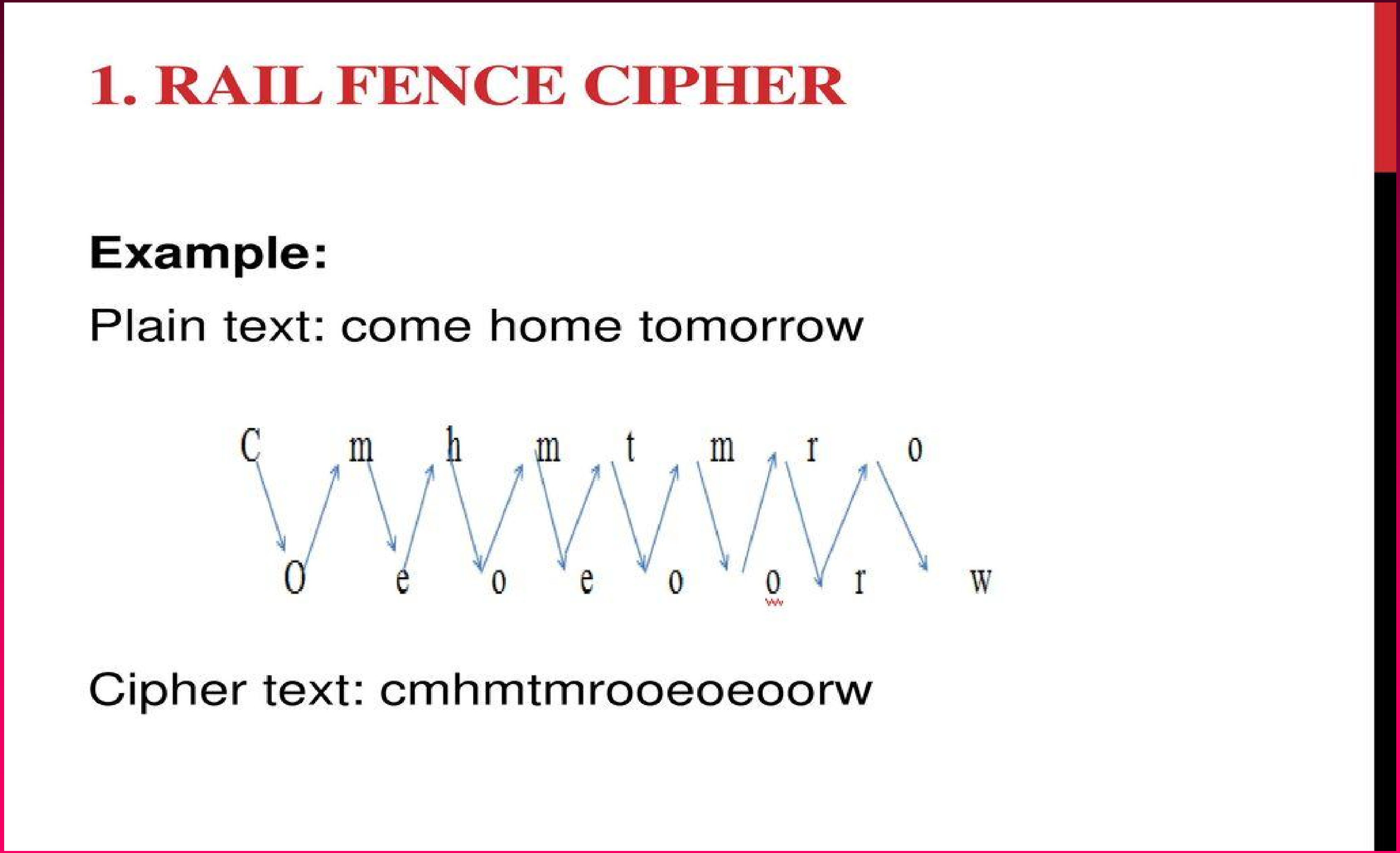
Plaintext:	H	E	L	L	O
	7	4	11	11	14
Key :	X	M	C	K	L
	23	12	2	10	11
Add :	30	16	13	21	25
Do subtract 26 if >25	4	16	13	21	25
	E	Q	N	V	Z

Vernam Cipher

- E Q N V Z
- 4 16 13 21 25
- X M C K L
- 23 12 2 10 11

- -19 4 11 11 14
- Add 26 if (-)
- 7 4 11 11 14=HELLO

Transposition Technique



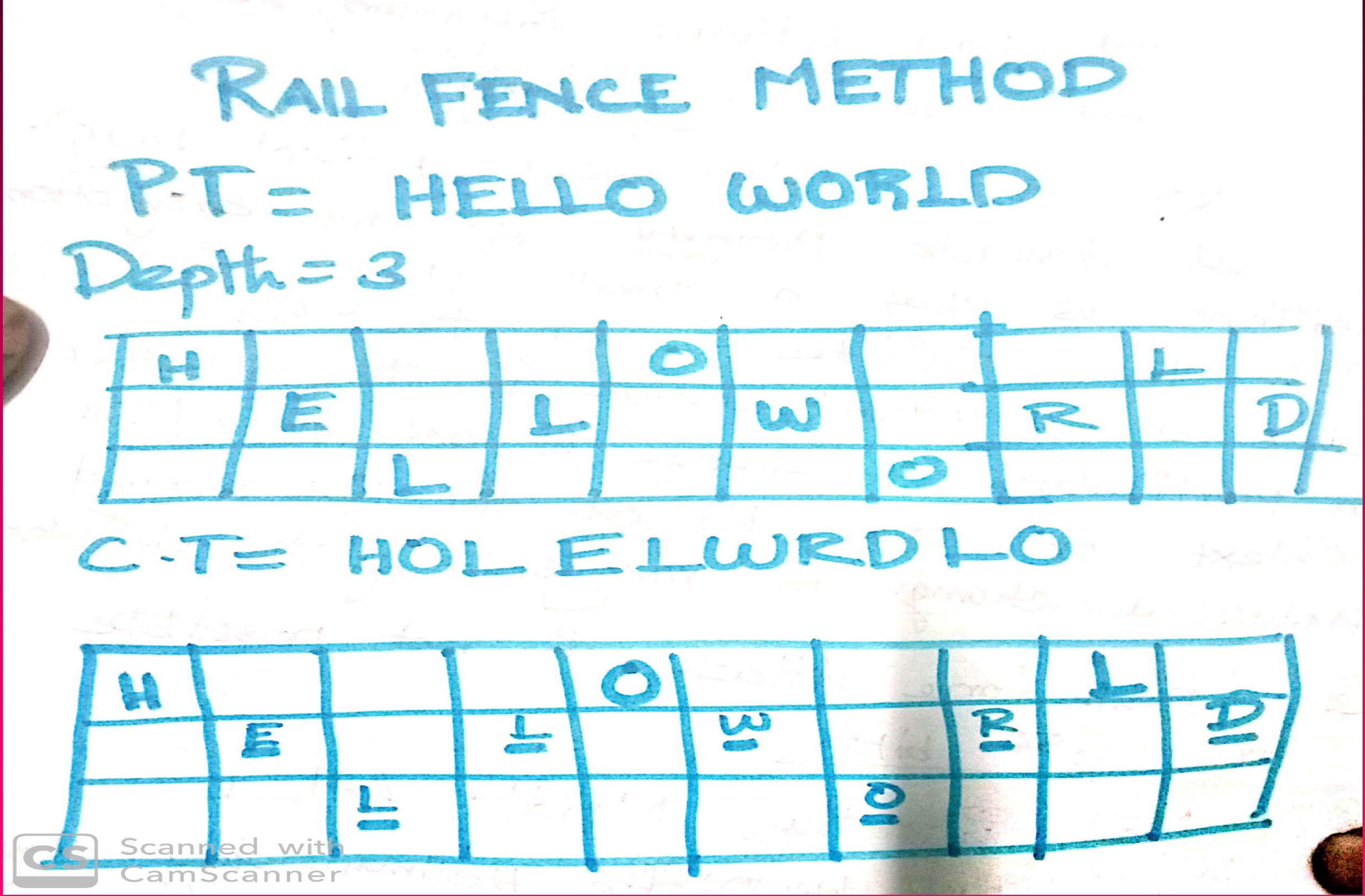
1. RAIL FENCE CIPHER

Example:

Plain text: come home tomorrow

Cipher text: cmhmtmrooeoeoorw

Rail fence method depth 3



RAIL FENCE METHOD

P.T = HELLO WORLD

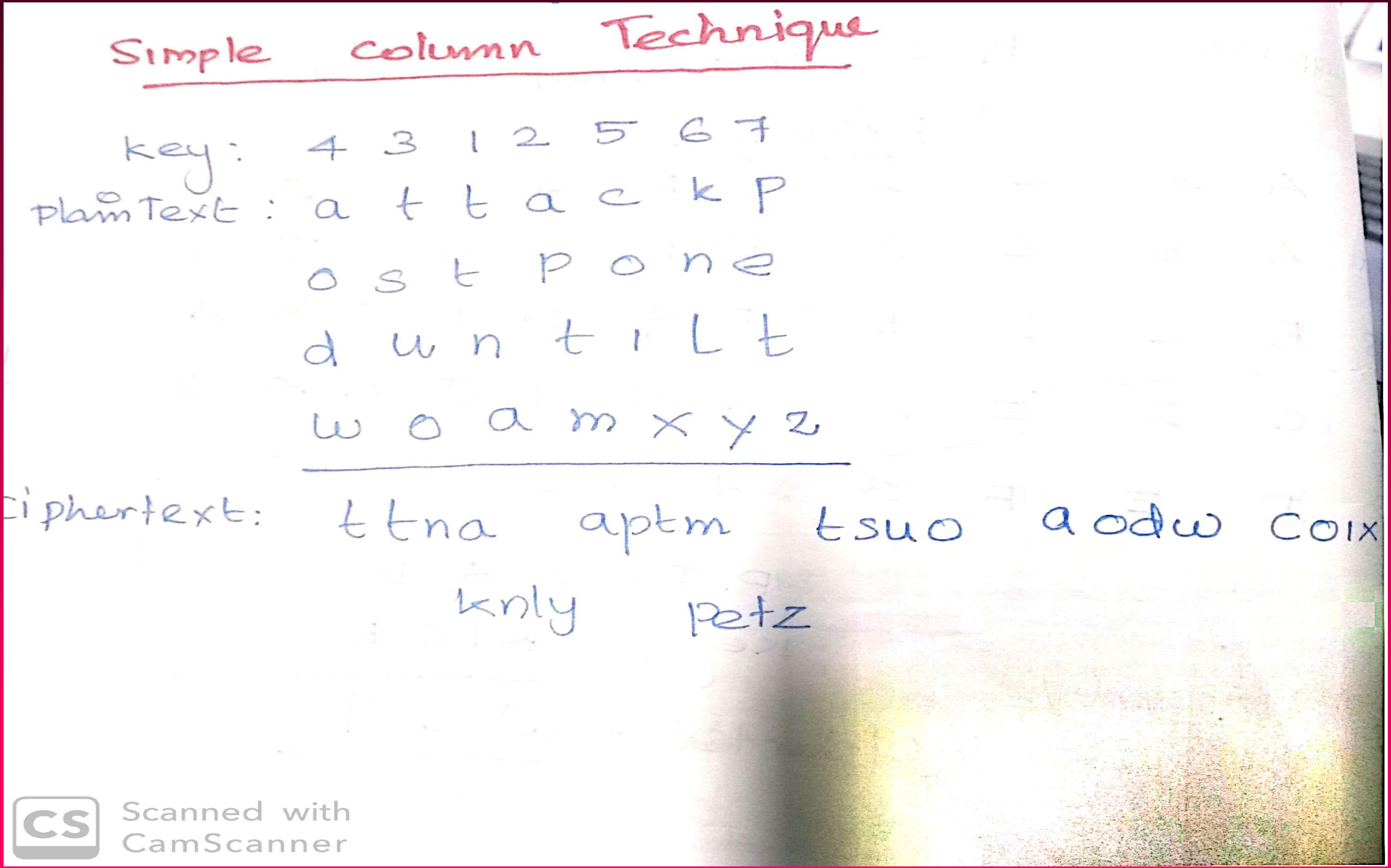
Depth = 3

H				O				L	
	E		L		W		R		D
		L				O			

C.T = HOL ELWRD LO

H				O				L	
	E		L		W		R		D
		L				O			

Simple column method



Simple column Technique

key:	4	3	1	2	5	6	7
Plain Text:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

ciphertext: ttna aptm tsuo aodw coix knly petz

Important Links

- https://www.youtube.com/watch?v=gOaawmoLlOc
- https://youtu.be/TnPzuP5FRsE
- https://youtu.be/Tn3gZ6Sno2Q
- https://youtu.be/PqFwEbgW74E
- https://youtu.be/M51ZgpKaWtQ

thank you
FungiStaaan.com