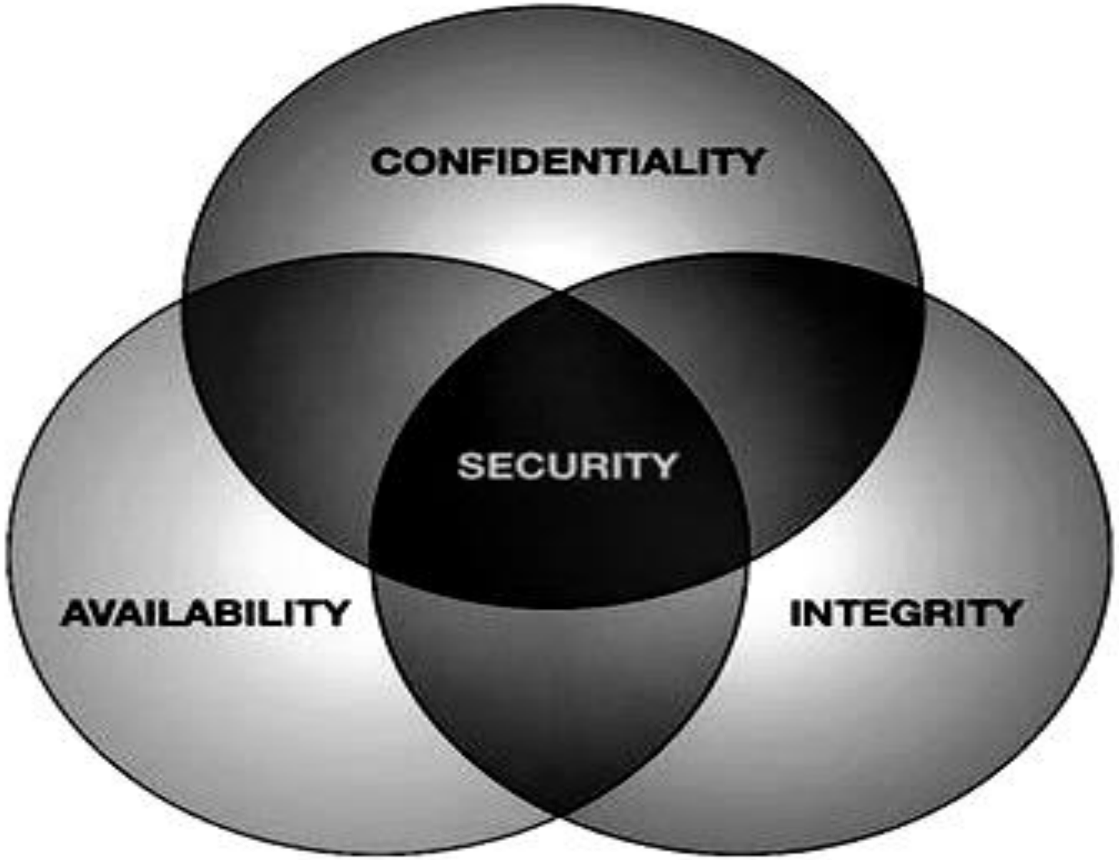
CSS

Prof. Amit K. Nerurkar
Assistant Professor
Department of Computer Engineering
Vidyalankar Institute of Technology, Wadala

1.1 Security Goals, Services, Mechanisms and attacks, The OSI security architecture, Network security model, Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, play fair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers, steganography.

Goals of security



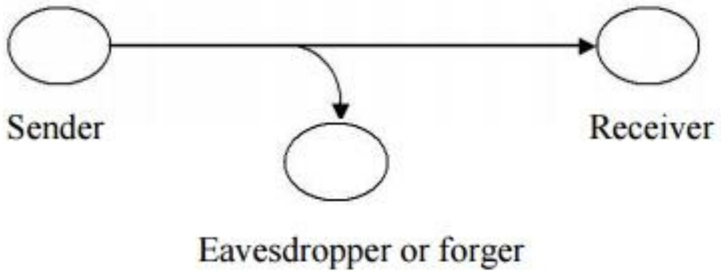
Confidentiality is a set of rules that limits access to information

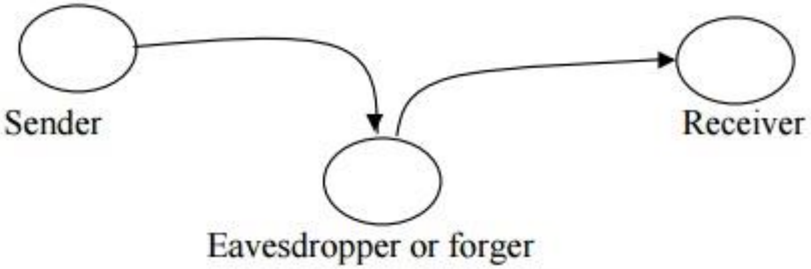
Integrity is the assurance that the information is trustworthy and accurate

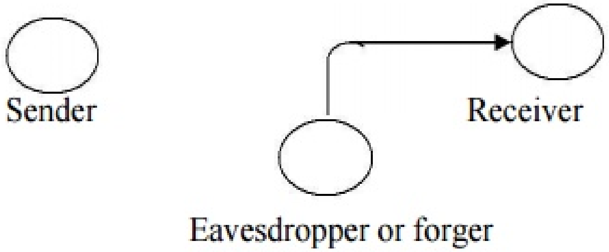
Availability is guarantee of reliable access to the information by authorized people

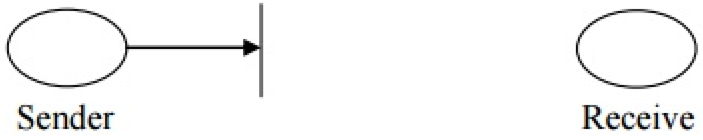
Threat

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

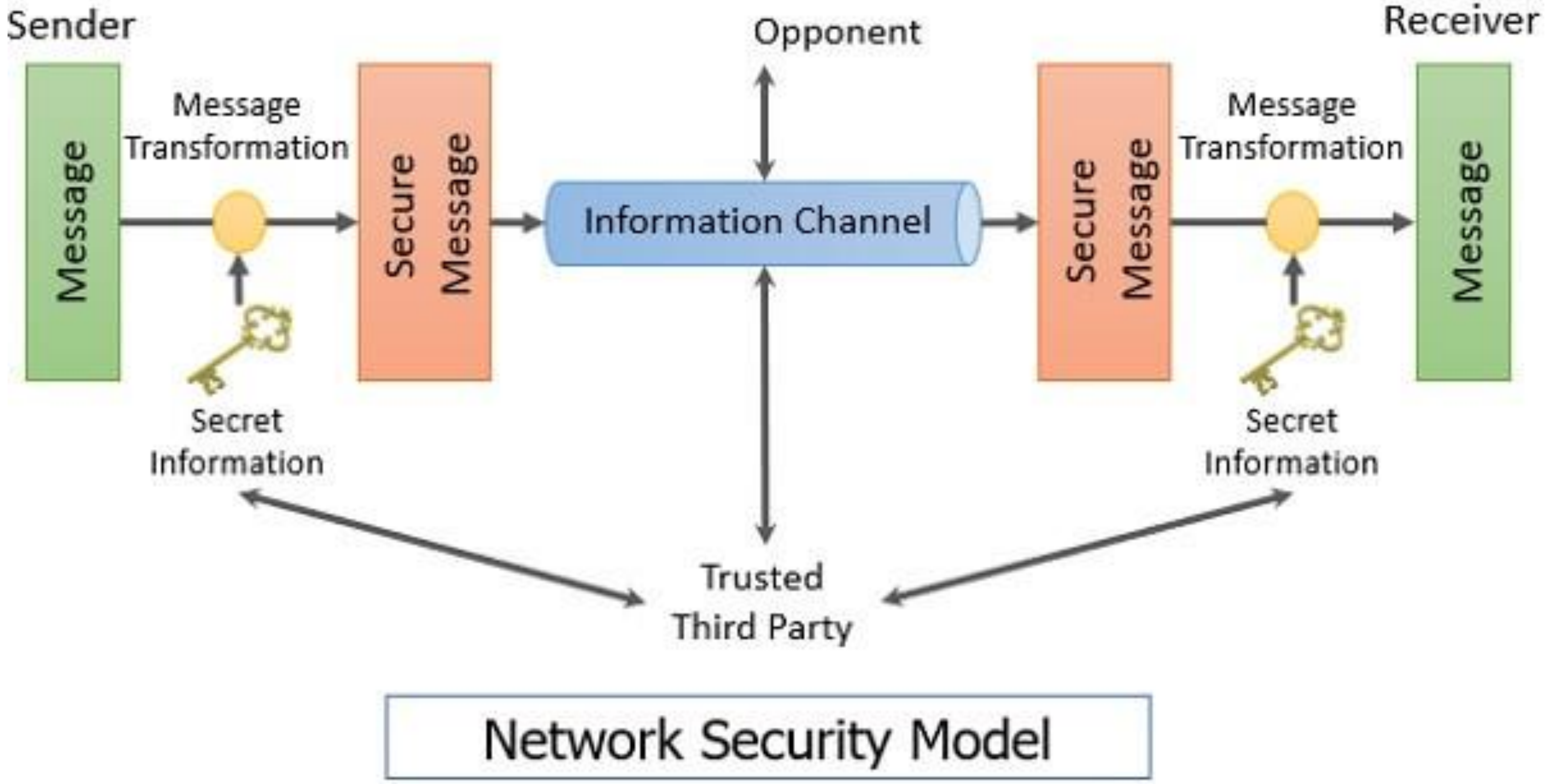






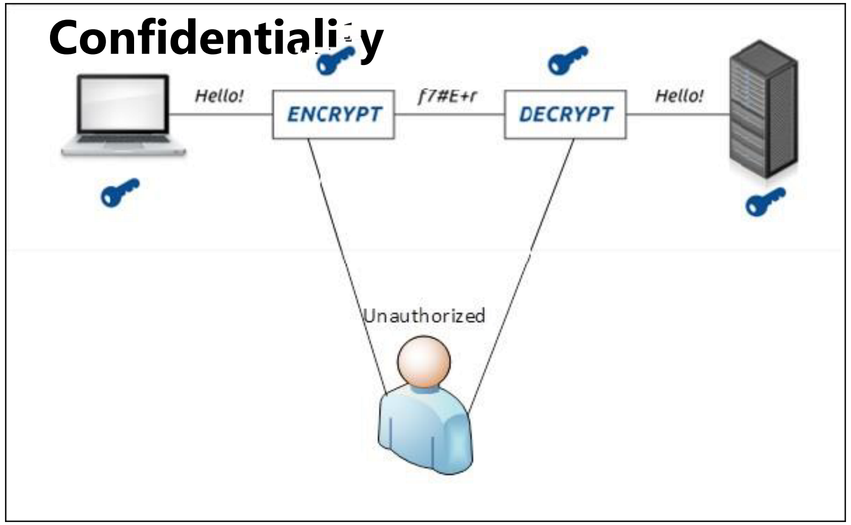


Network Security Model

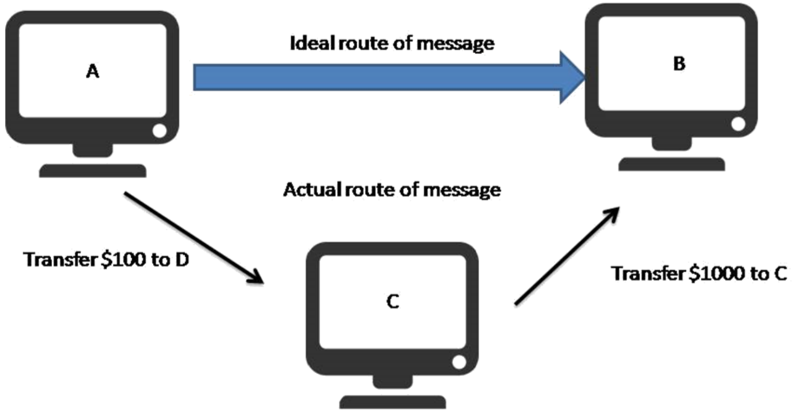


SECURITY SERVICES

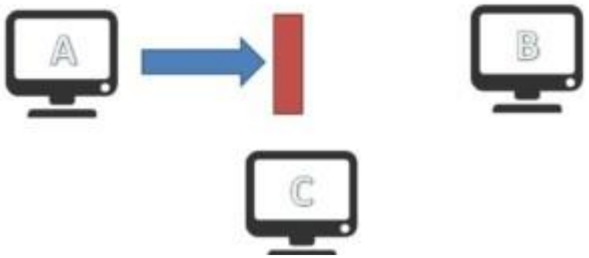
Confidentiality



Integrity

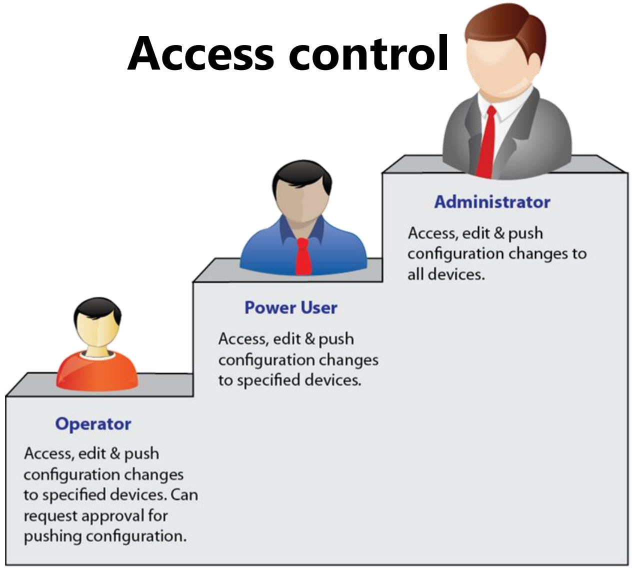


Availability



Authentication

Access control



Administrator

Access, edit & push configuration changes to all devices.

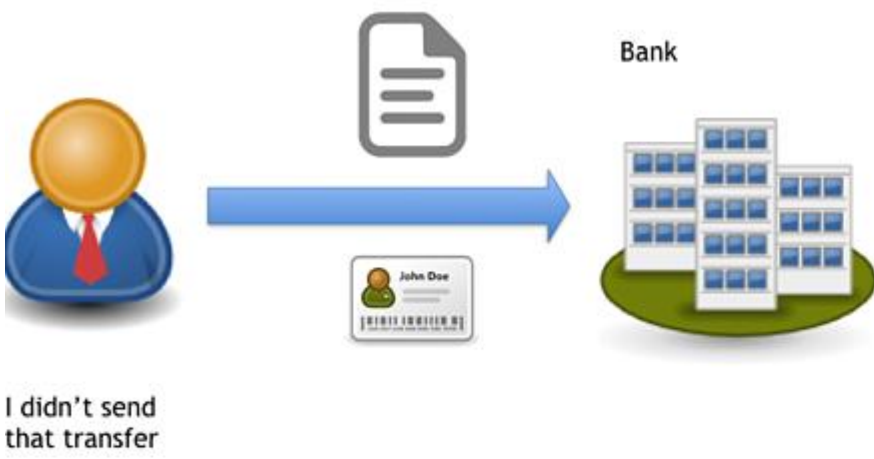
Power User

Access, edit & push configuration changes to specified devices.

Operator

Access, edit & push configuration changes to specified devices. Can request approval for pushing configuration.

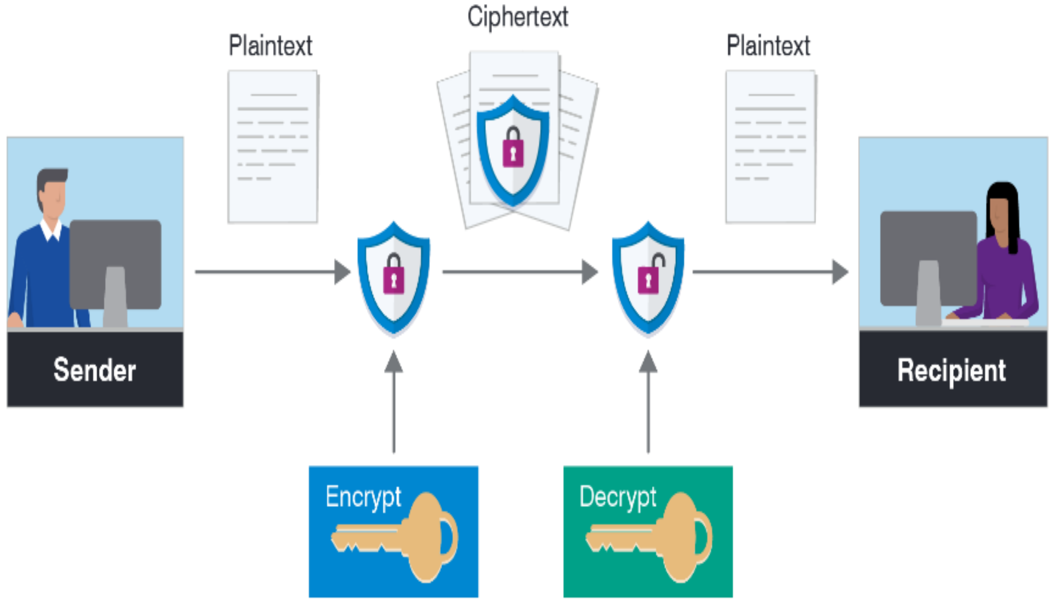
Non repudiation



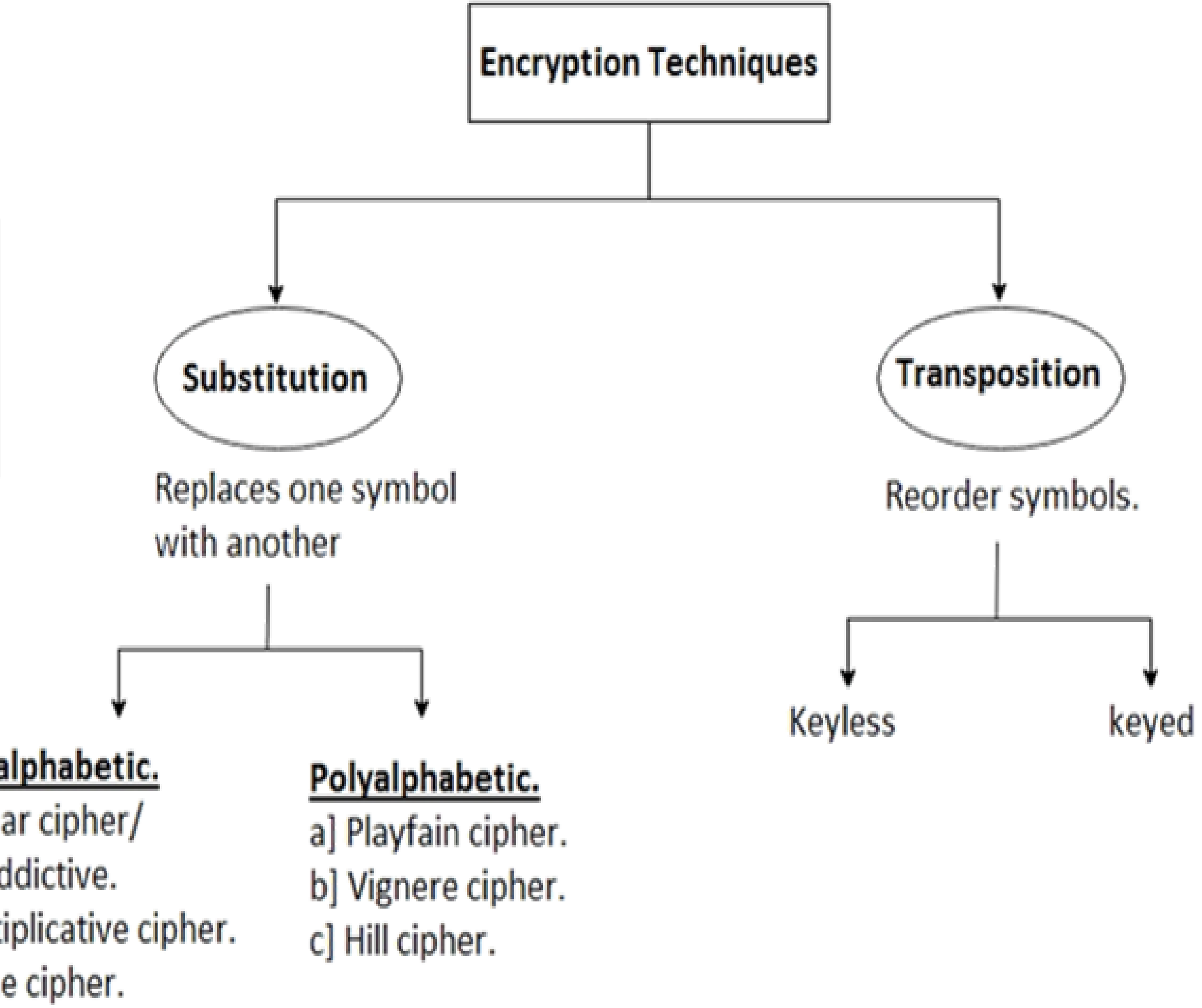
Encryption and Decryption

Encryption is a process which transforms the original information into an unrecognizable form.

Decryption is a process of converting encoded/**encrypted** data in a form that is readable and understood by a human or a computer.



Different keys are used to encrypt and decrypt messages



Encryption Techniques

Substitution

Replaces one symbol with another

Mono alphabetic.

a] Caesar cipher/ shift/Addictive.

b] Multiplicative cipher.

c] Affine cipher.

Polyalphabetic.

a] Playfain cipher.

b] Vignere cipher.

c] Hill cipher.

Transposition

Reorder symbols.

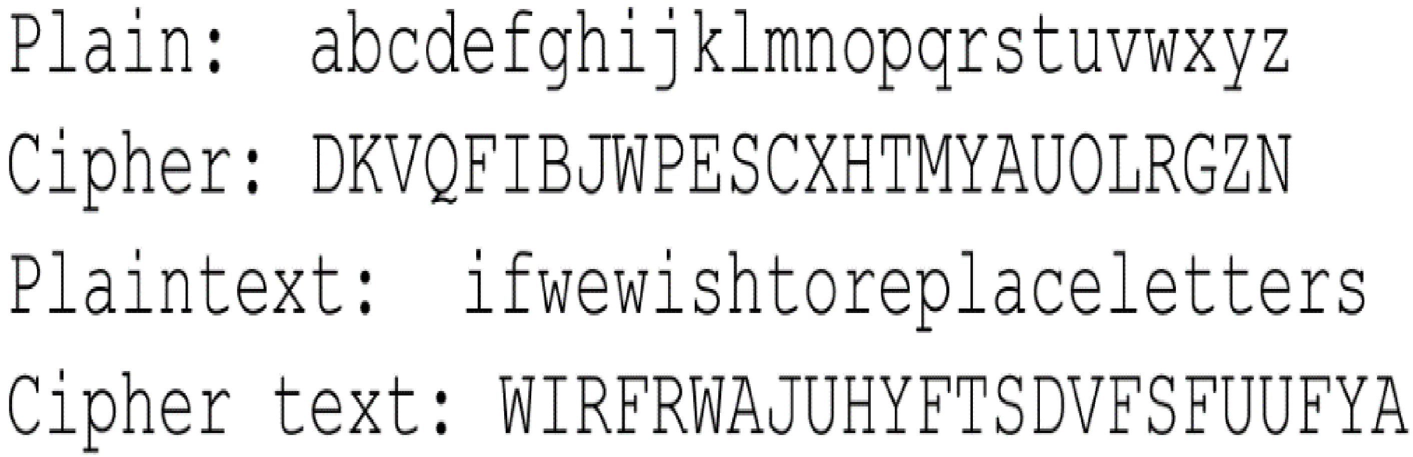
Keyless

keyed

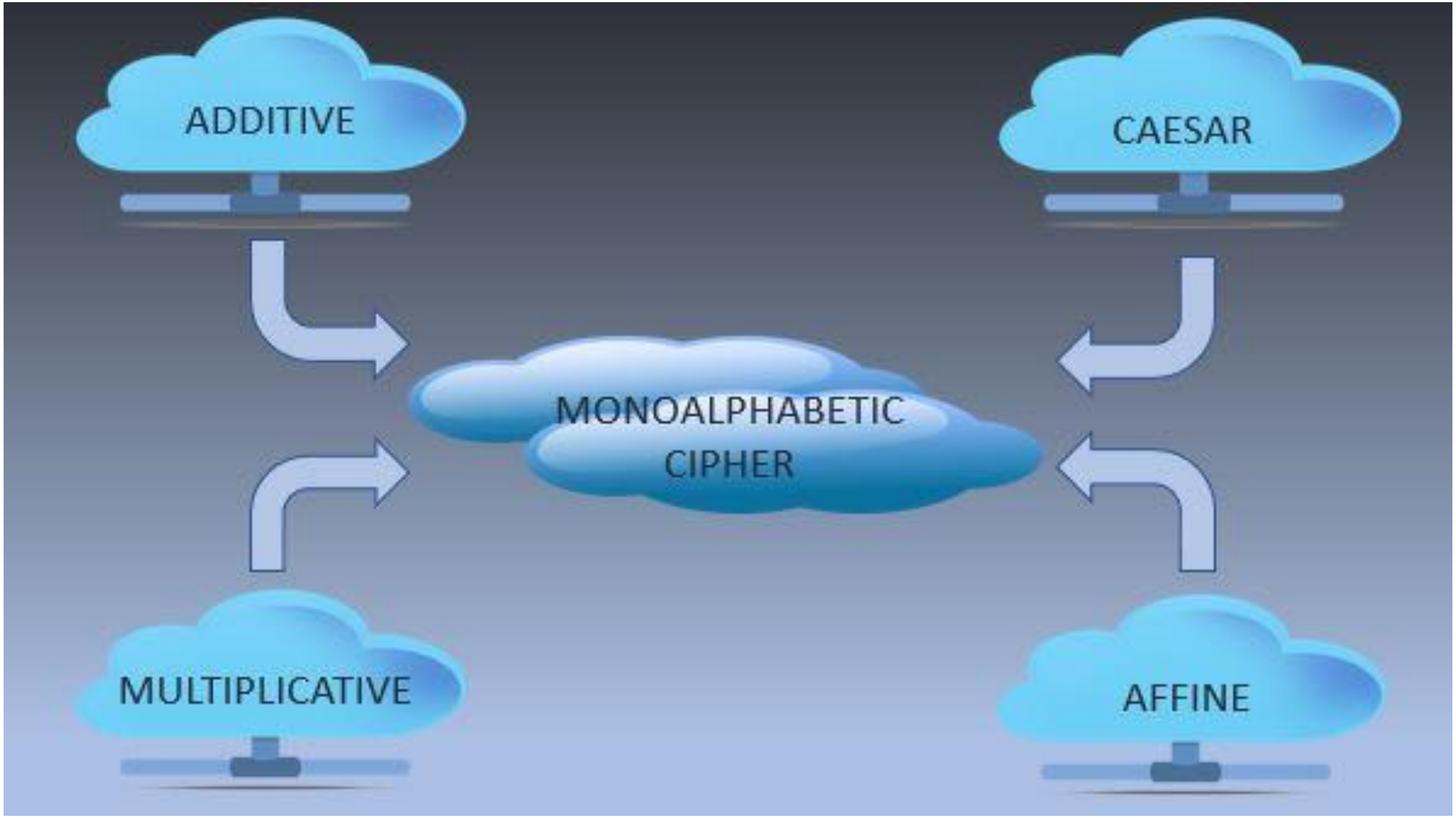
Substitution

A: Mono Alphabetic Substitution

If 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.



```
Plain:   abcdefghijklmnopqrstuvwxyz
Cipher:  DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:   ifwewishtoreplaceletters
Cipher text: WIRFRWAJUHYFTSDVFSFUUFYA
```


ADDITIVE
CAESAR
MONOALPHABETIC CIPHER
MULTIPLICATIVE
AFFINE

1. Ceaser Cipher:

$E\_n(x)=(x+n)\bmod 26$
(Encryption Phase with shift n)

$D\_n(x)=(x-n)\bmod 26$
(Decryption Phase with shift n)

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Note:

$-x \bmod y$

$\hookrightarrow y-(x \bmod y)$

S E C U R I T Y $\boxed{n=5}$

Soln

P.T.	S	E	C	U	R	I	T	Y
Pos.	18	4	2	20	17	8	19	24
⊕ n	5	5	5	5	5	5	5	5
	23	9	7	25	22	13	24	29
Mod	26	26	26	26	26	26	26	26
	23	9	7	25	22	13	24	3
C.T.	X	J	H	Z	W	N	Y	D

C.T.	X	J	H	Z	W	N	Y	D
Pos	23	9	7	25	22	13	24	3
⊖ n	5	5	5	5	5	5	5	5
	18	4	2	20	17	8	19	$\boxed{-2}$
mod	26	26	26	26	26	26	26	26
	18	4	2	20	17	8	19	24
P.T.	S	E	C	U	R	I	T	Y

$-26-(2 \bmod 26)$

$= 26-2$

$= 24$

B. Polyalphabetic Cipher

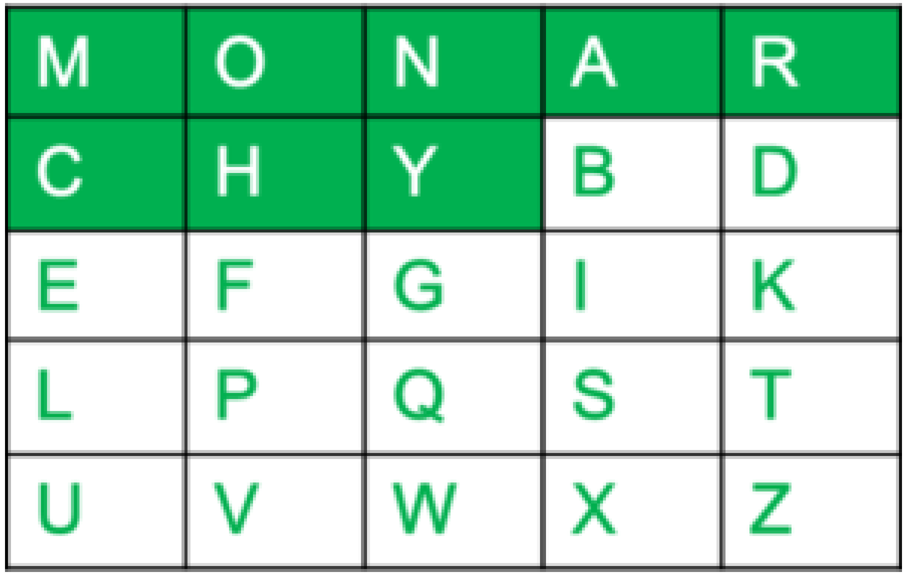
A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

1. Playfair cipher

The Playfair Cipher Encryption Algorithm:
The Algorithm consists of 2 steps
Generate the key Square(5×5):

For example:

The key is "**monarchy**"Thus the initial entires are**'m', 'o', 'n', 'a', 'r', 'c', 'h', 'y'**followed by remaining characters of **a-z(except 'j')** in that order.



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

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"

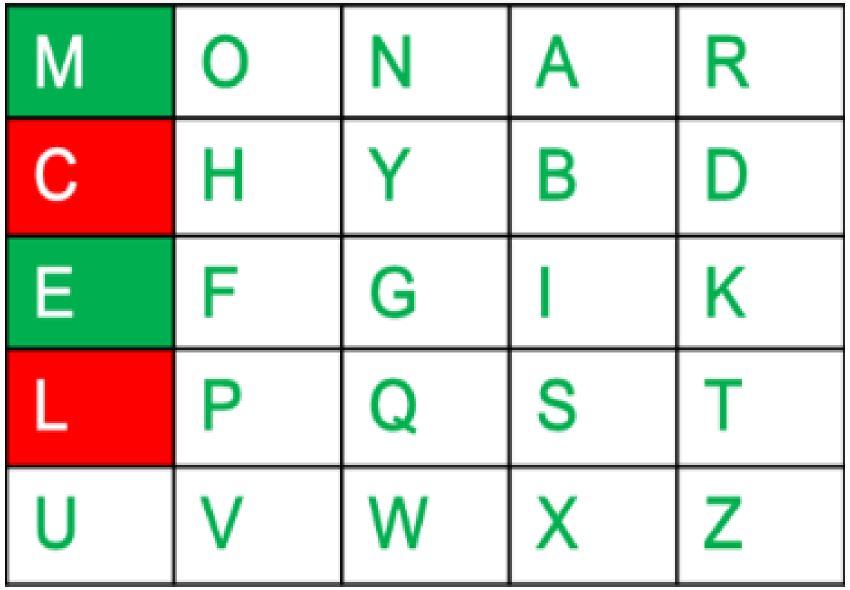
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

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

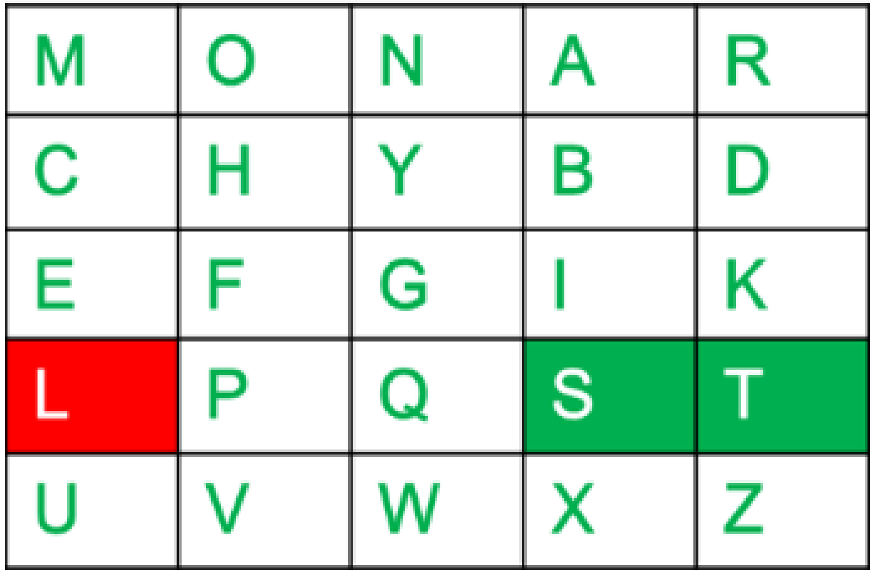


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

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
t -> 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

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:

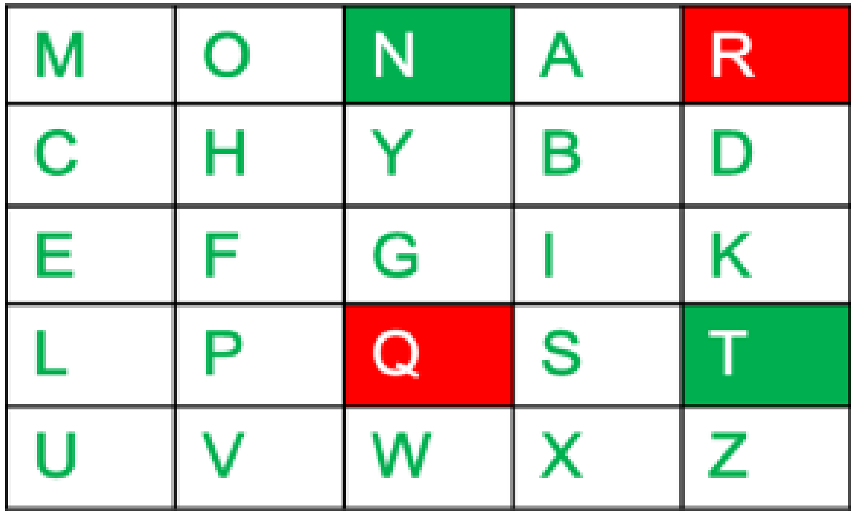
Diagraph: "nt"

Encrypted Text: rq

Encryption:

n -> r

t -> q

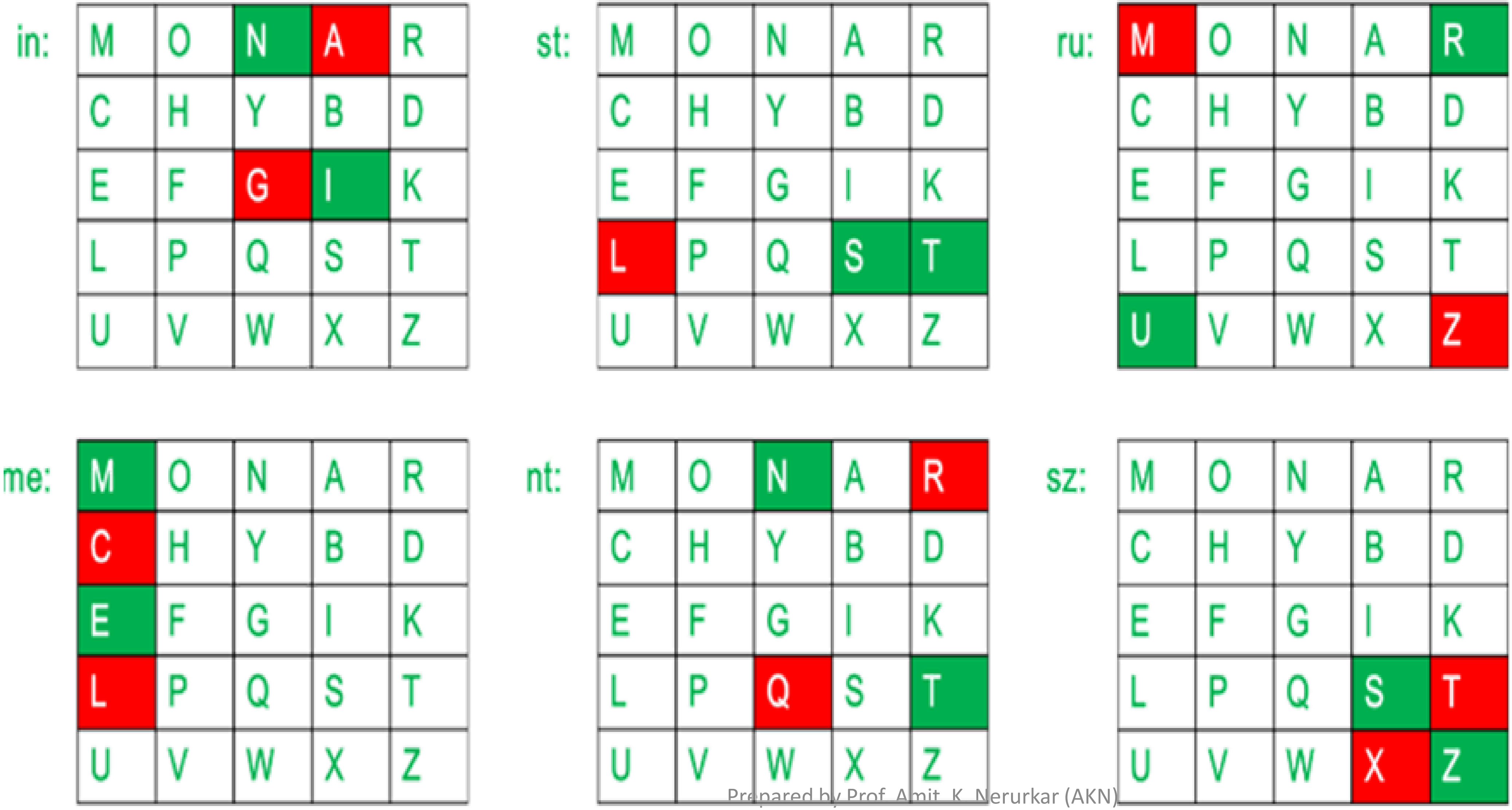


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

Plain Text: "instrumentsz"

Encrypted Text: gatlmzclrqtx



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

Decryption Technique

Rules for Decryption:

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

For example:

Diagraph: "cl"
Decrypted Text: me
Decryption:
c -> m
l -> e

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

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

For example:

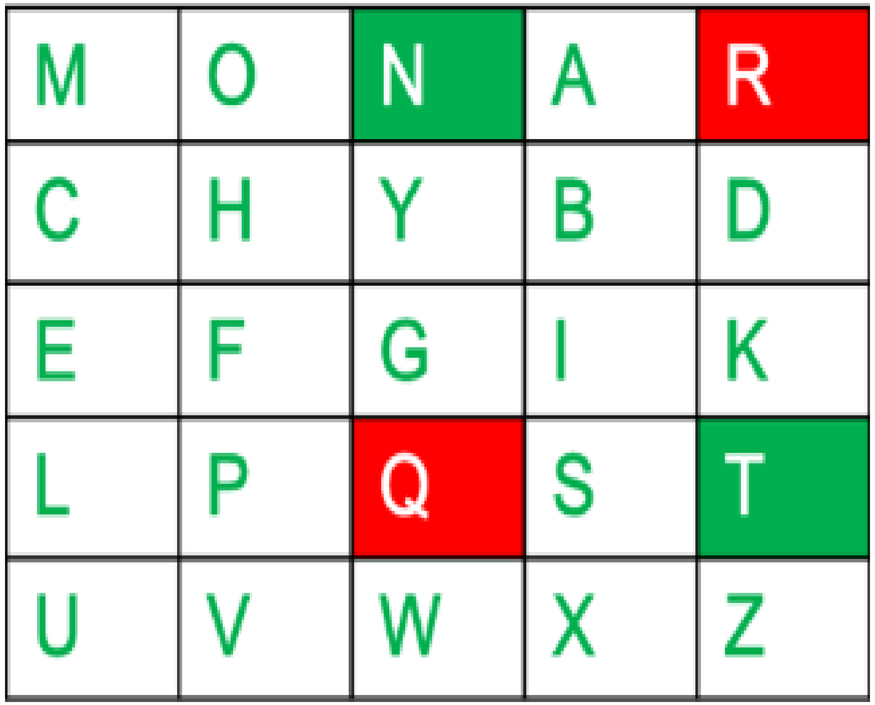
Diagraph: "tl"
Decrypted Text: st
Decryption:
t -> s
l -> t

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

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: "rq"
Decrypted Text: nt
Decryption:
r -> n
q -> t



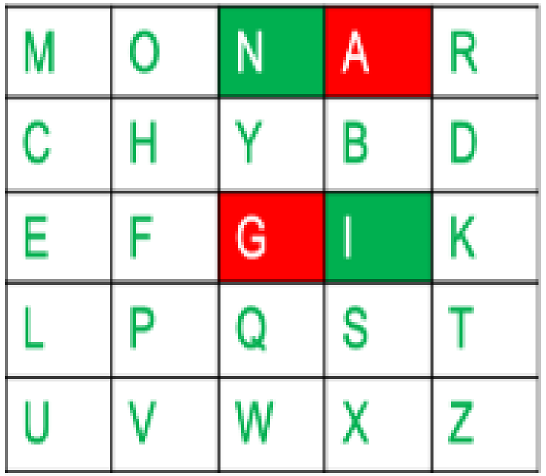
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

Plain Text: "gatlmzclrqtx"

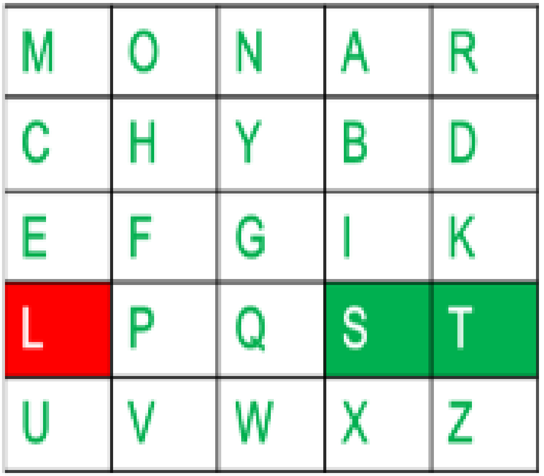
Decrypted Text: instrumentsz

in:



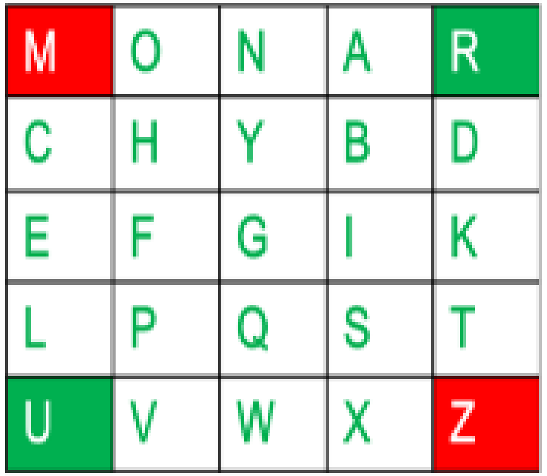
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

st:



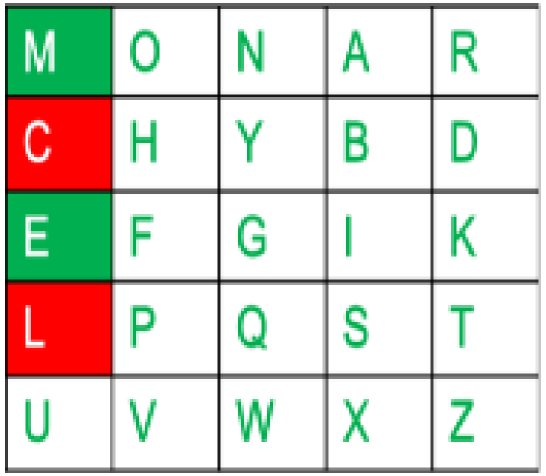
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

ru:



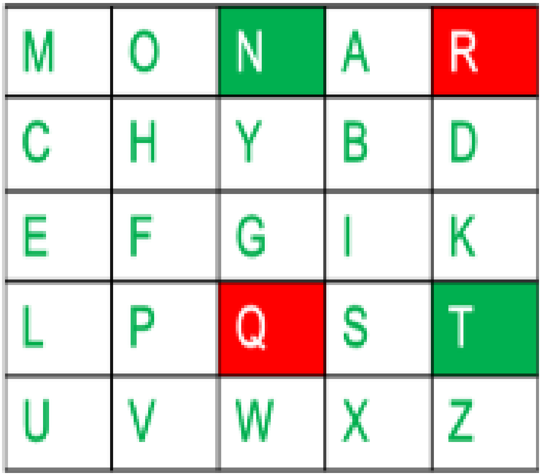
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

me:



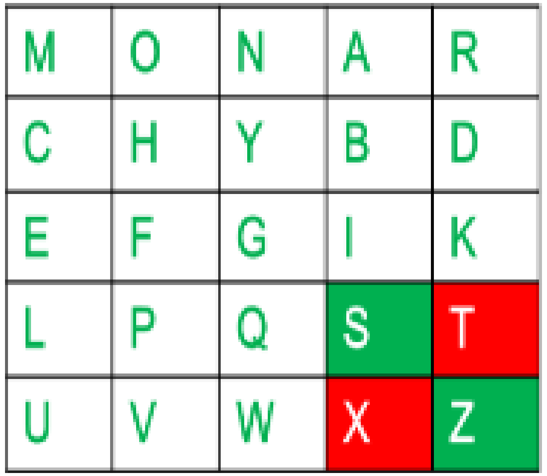
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

nt:



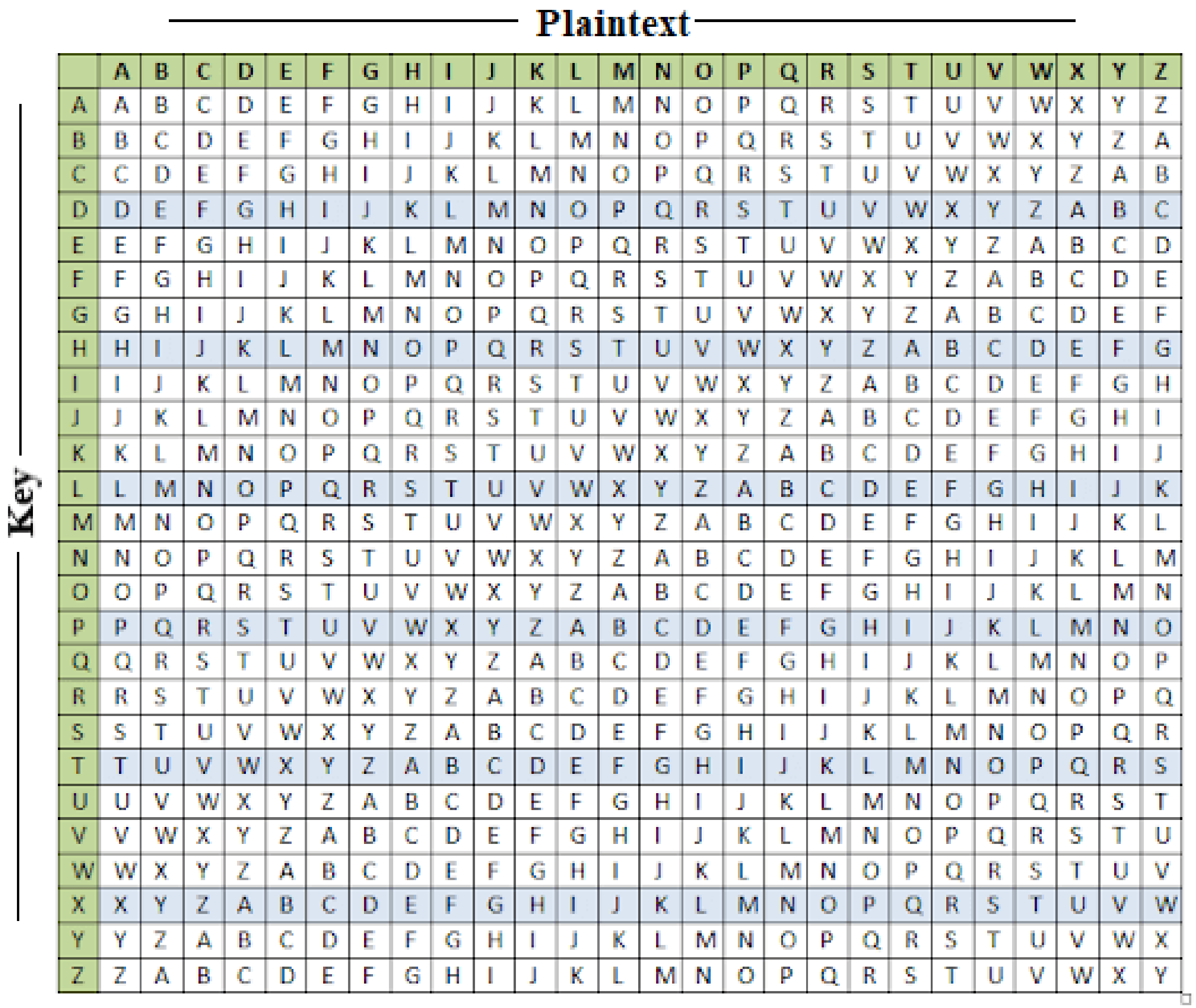
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

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

2. Vigenère cipher



Plaintext

Key

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

Example: The plaintext is "NETWORK", and the key is "VIT".

To generate a new key, the given key is repeated in a circular manner, as long as the length of the plain text does not equal to the new key.

N	E	T	W	O	R	K
V	I	T	V	I	T	V

I	M	M	S	W	T	F
V	I	T	V	I	T	V

3. Hill Cipher

Encryption

We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:

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

The message 'ACT' is written as vector:

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

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of 'POH'

Decryption

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

For the previous Ciphertext ‘POH’:

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

which gives us back ‘ACT’.

① Vernam [one time Pad] cipher ·

eg. P.T. V I D Y A L A N K A R

Key M O N E Y

Soln

P.T.	V	I	D	Y	A	L	A	N	K	A	R
Posn	21	8	3	24	0	11	0	13	10	0	17
+ Key	M	O	N	E	Y	M	O	N	E	Y	M
Posn	12	14	13	4	24	12	14	13	4	24	12
	33	22	16	28	24	23	14	26	14	24	29
≥26	−26	↓	↓	−26	↓	↓	↓	−26	↓	↓	−26
	7	22	16	2	24	23	14	0	14	24	3
C.T.	H	W	Q	C	Y	X	O	A	O	Y	D

C.T.	H	W	Q	C	Y	X	O	A	O	Y	D
Pos	7	22	16	2	24	23	14	0	14	24	3
− Key	M	O	N	E	Y	M	O	N	E	Y	M
Pos	12	14	13	4	24	12	14	13	4	24	12
	−5	8	3	−2	0	11	0	−13	10	0	−9
−ve	+26	↓	↓	+26	↓	↓	↓	+26	↓	↓	+26
		8	3	24	0	11	0	13	10	0	17
P.T.	V	I	D	Y	A	L	A	N	K	A	R

P.T. M A H A R A S H T R A

Key M U M B A I

Transposition:

Keyed Transposition

Plain text	F	O	U	R		F	I	V	E
Key	2	4	0	1		2	4	0	1
Positions	0	1	2	4		0	1	2	4
Cipher Text	U	R	F	O		V	E	F	I
Positions	0	1	2	4		0	1	2	4
Key	2	4	0	1		2	4	0	1
Plain text	F	O	U	R		F	I	V	E

P.T.	S	E	C	U	R	I	T	Y
Key ↓	9	7	4	2	1	0	6	5
SORT	0	1	2	4	5	6	7	9
C.T.	I	R	U	C	Y	T	E	S

C.T.	I	R	U	C	Y	T	E	S
Key SORT.	0	1	2	4	5	6	7	9
Key	9	7	4	2	1	0	6	5
P.T.	S	E	C	U	R	I	T	Y

Keyless Transposition

Rail Fence algorithm.

Encryption

Plaintext T H I S I S A S E C R E T M E S S A G E

Rail Fence
Encoding
key = 3

T				I				E				T				S			
	H		S		S		S		C		E		M		S		A		E
		I				A				R				E				G	

Ciphertext T I E T S H S S S C E M S A E I A R E G

Decryption

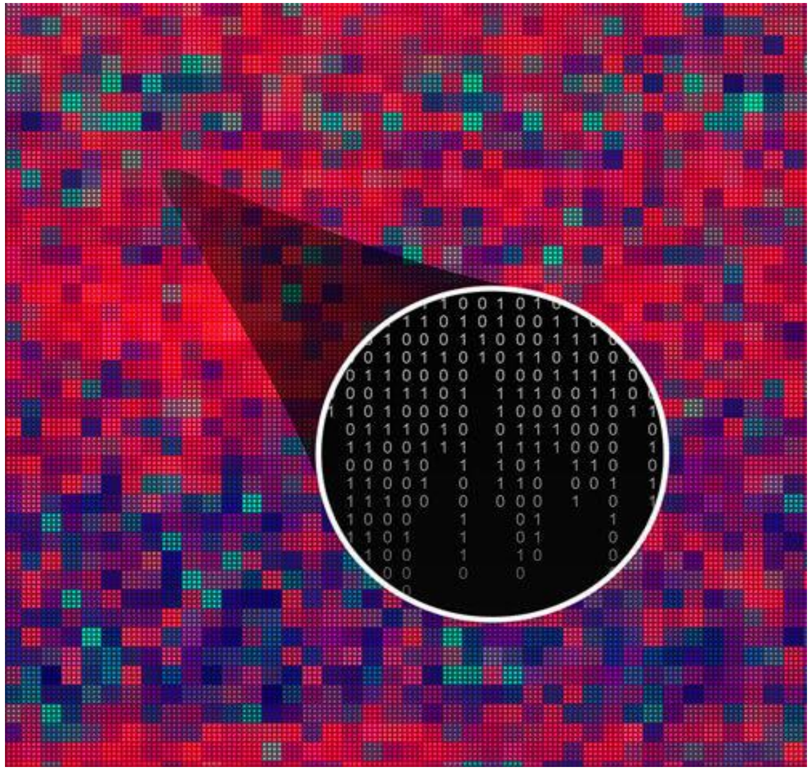
Cipher	T				I				E				T				S			
		-		-		-		-		-		-		-		-		-		-
			-				-				-				-				-	

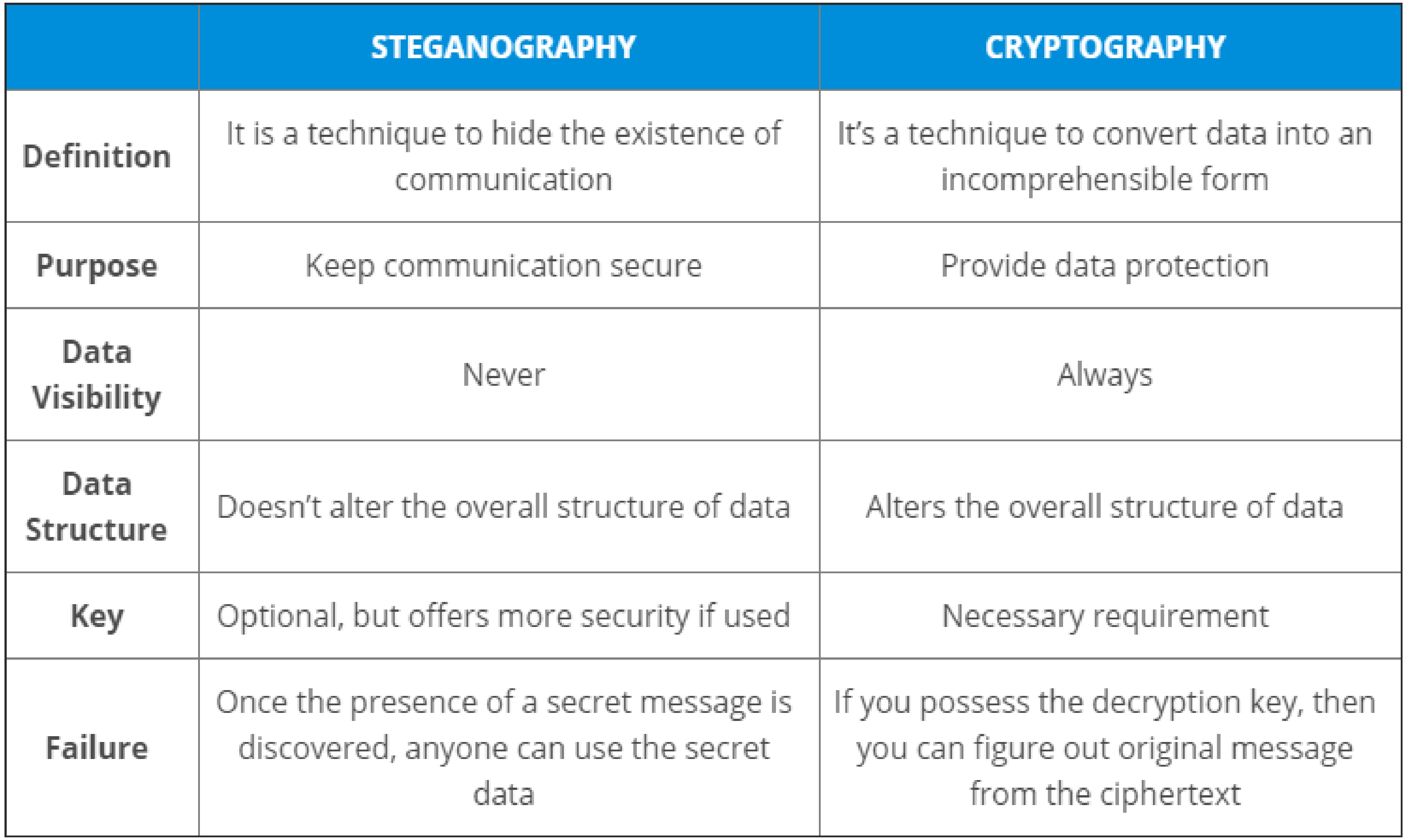
Cipher	**T**				**I**				**E**				**T**				**S**			
		H		S		S		S		C		E		M		S		A		E
			-				-				-				-				-	

Cipher	**T**				**I**				**E**				**T**				**S**			
		H		**S**		**S**		**S**		**C**		**E**		**M**		**S**		**A**		**E**
			I				A				R				E				G	

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.





	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

Thank You

Name: Amit K. Nerurkar

Designation: Assistant Professor

College: Vidyalankar Institute of Technology