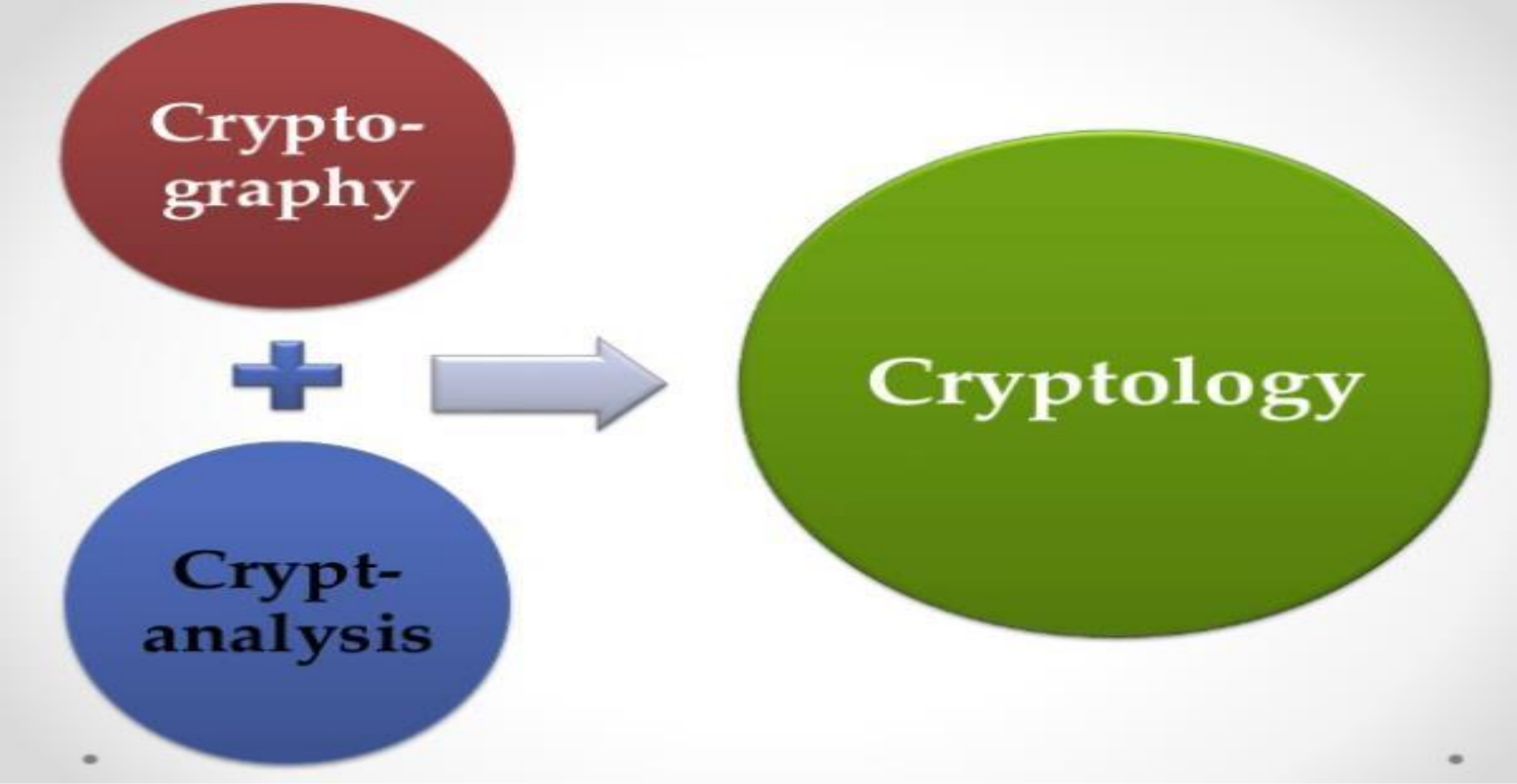
What’s Cryptography?

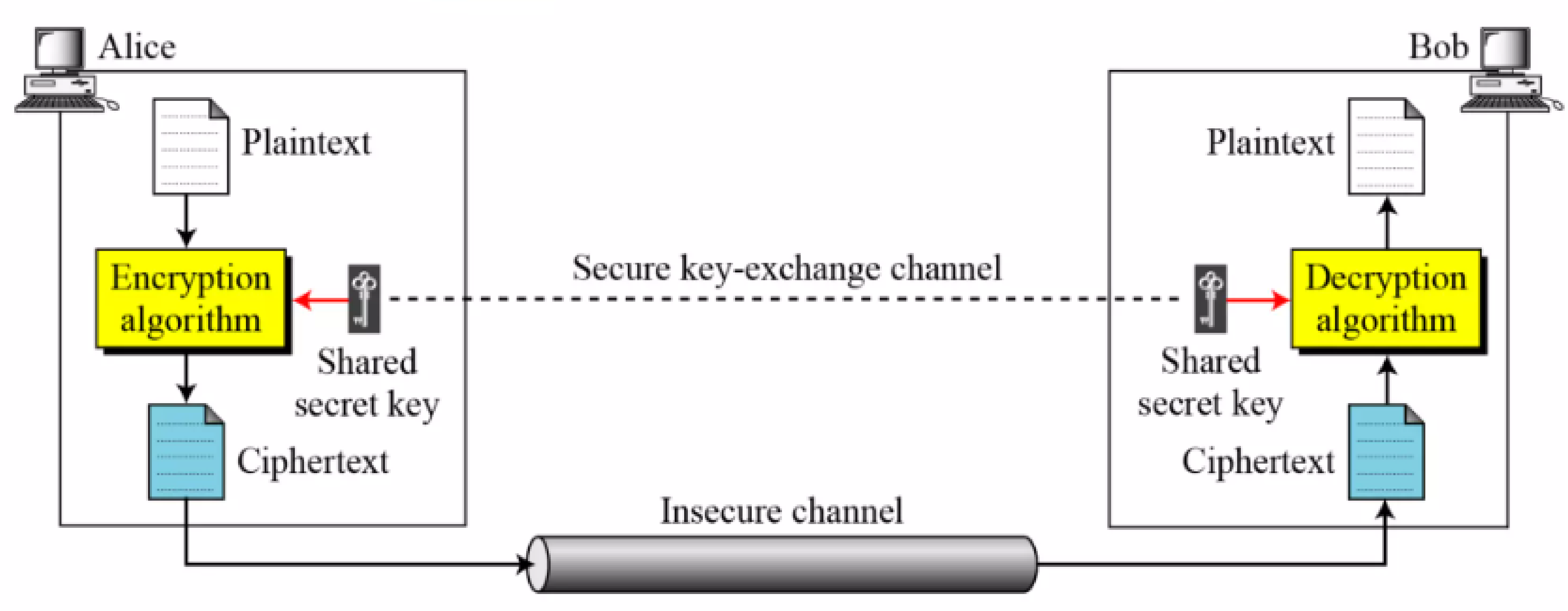


Cryptography

Cryptanalysis

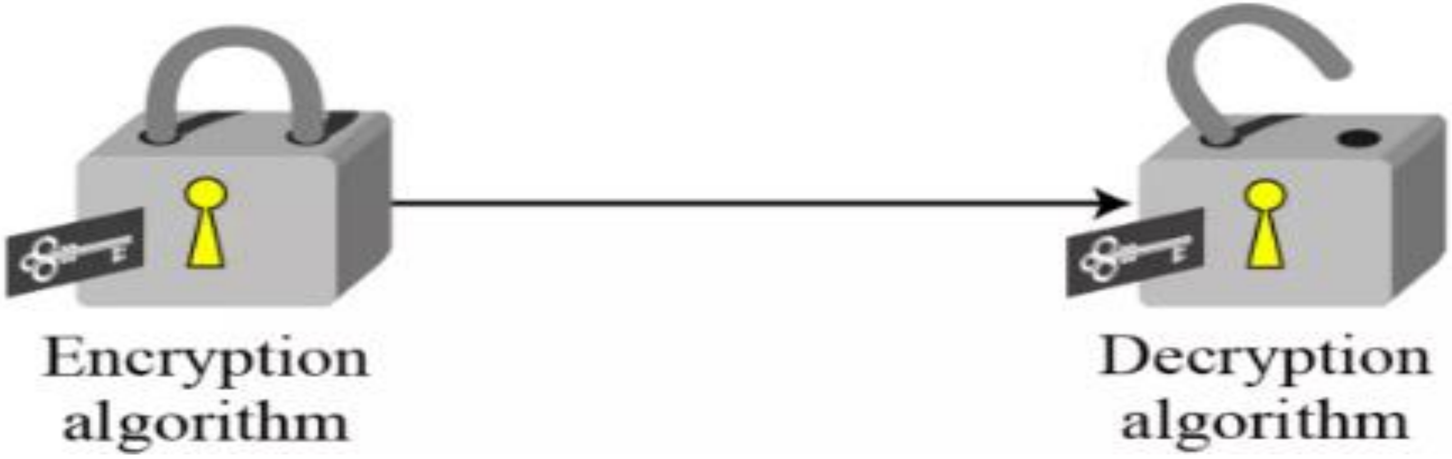
Cryptology

Symmetric Cipher Model



Symmetric Cipher Model (Contd..)

- Alice:- $C = E_k(P)$
- Bob:- $D = D_k(C) = D_k(E_k(P))$



Kerckhoff’s Principle

- Published by Auguste Kerckhoff in 1883.
- Uses 2 key principles:- Algorithm Transparency, and Key Secrecy

3 Independent Dimensions of Cryptographic Systems

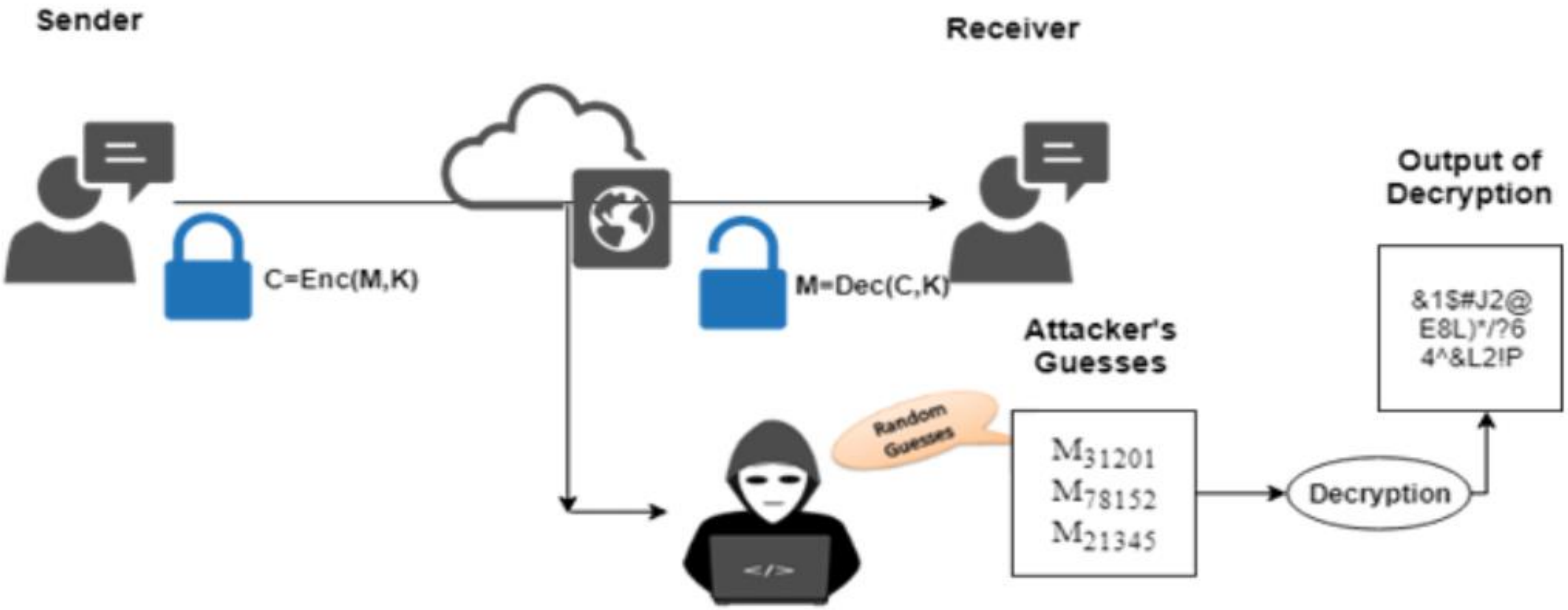
- Types of Operations used for transformation of PT to CT
- Number of keys used
- How PT is processed

CRYPTANALYSIS

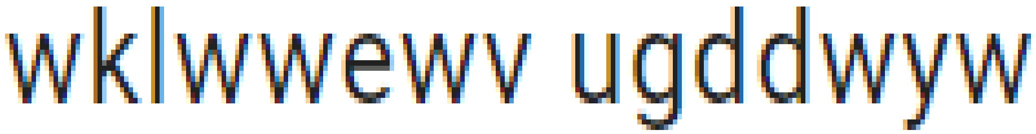
Cryptanalysis Techniques on Encrypted Data

1) Brute Force Attack (BFA)
2) Statistical Attack
3) Pattern Attack
4) Ciphertext Only Attack
5) Known Plaintext Attack
6) Chosen Plaintext Attack
7) Chosen Ciphertext Attack

BFA


Sender
Receiver
C=Enc(M,K)
M=Dec(C,K)
Attacker's Guesses
Random Guesses
M_{31201}
M_{78152}
M_{21345}
Decryption
Output of Decryption
&1S#J2@
E8L)*/?6
4^&L2!P
</>

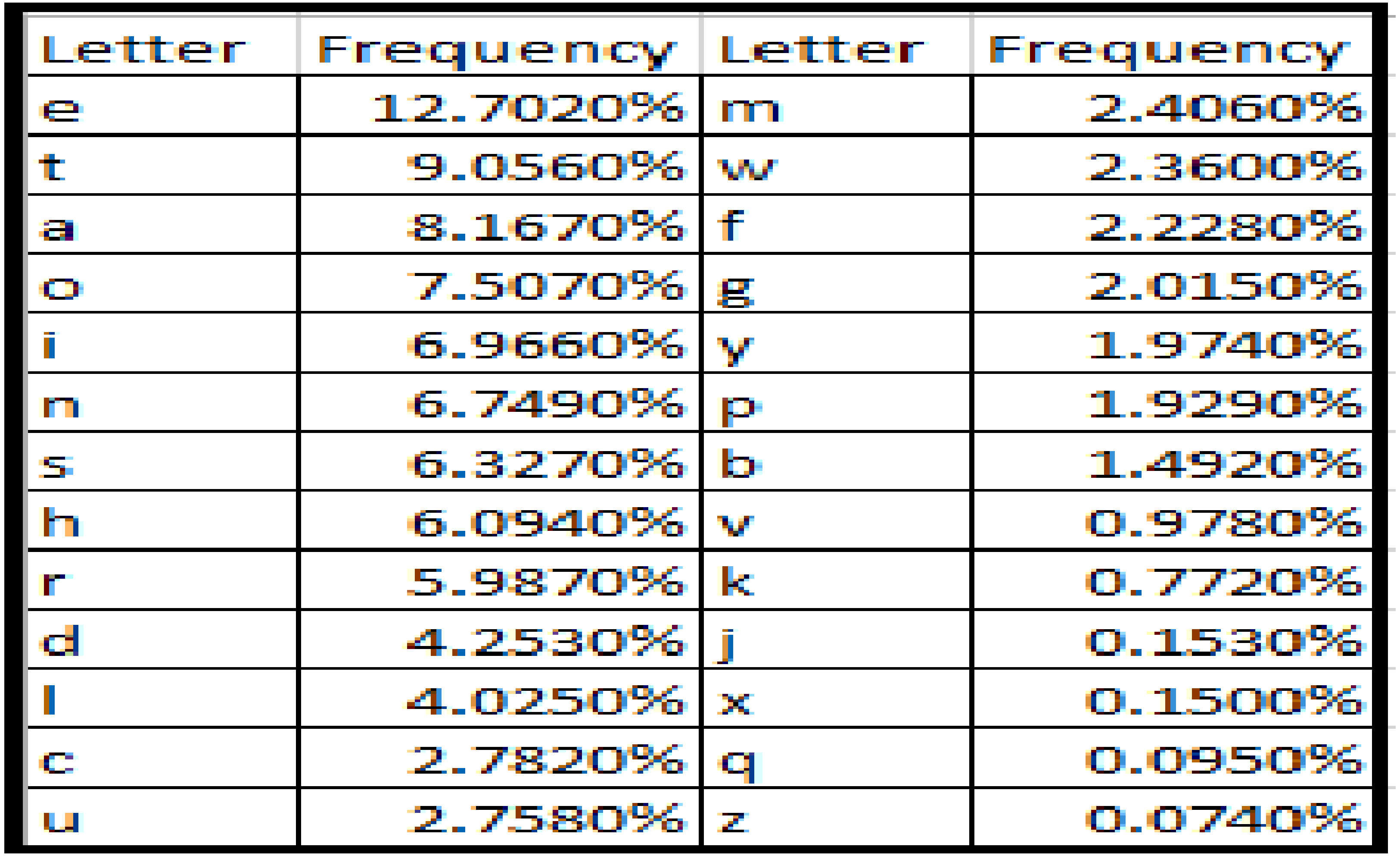
Statistical Attack

CT:- 

wklwwewv ugddwyw

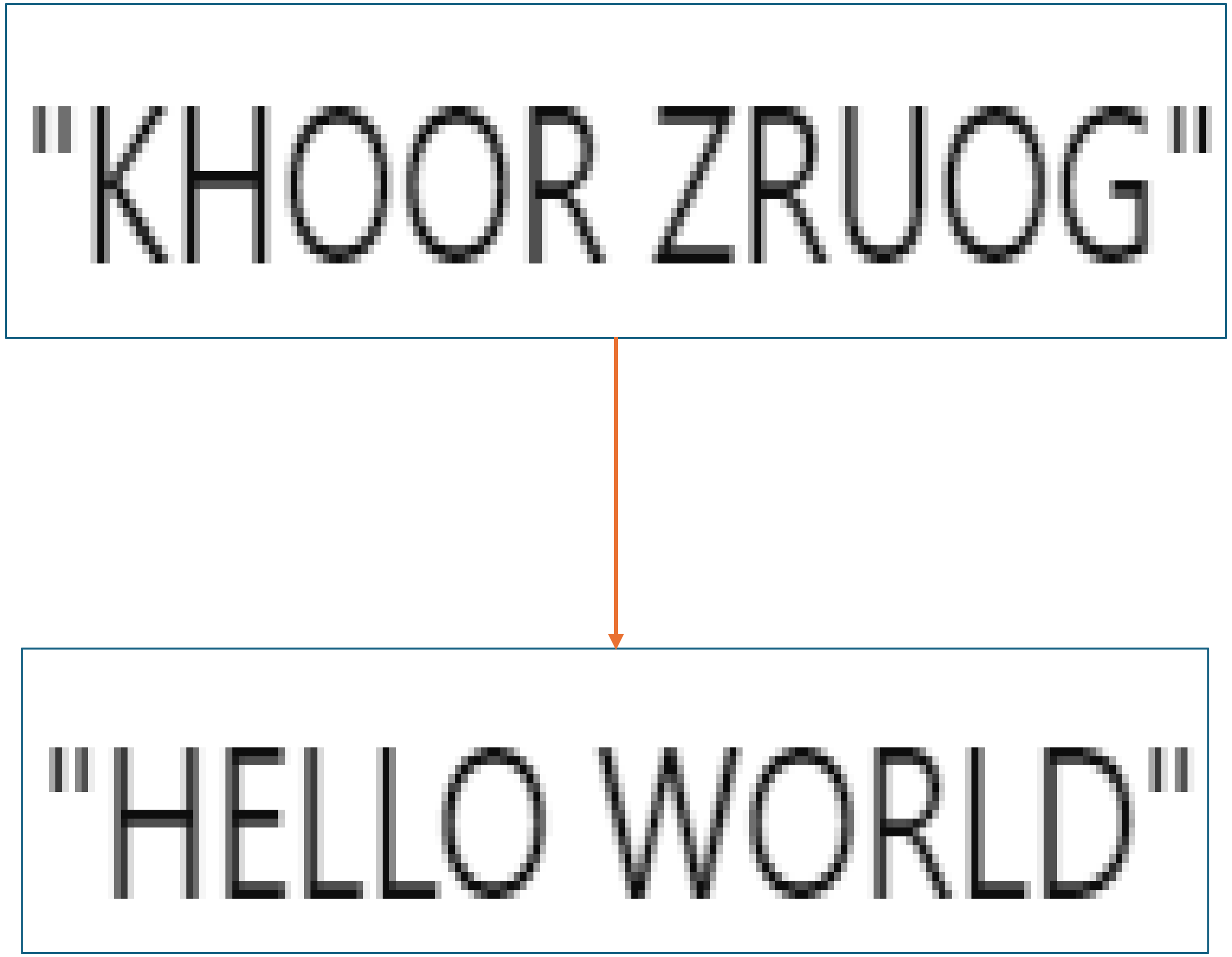
- The letter ‘e’ is the most frequently used English alphabet for plaintext.
- Hence, for the above CT, the attacker makes a best case guess that most probably the ciphertext character ‘w’ maps to the plaintext character ‘e’.

Statistical Attack (Contd..)



Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

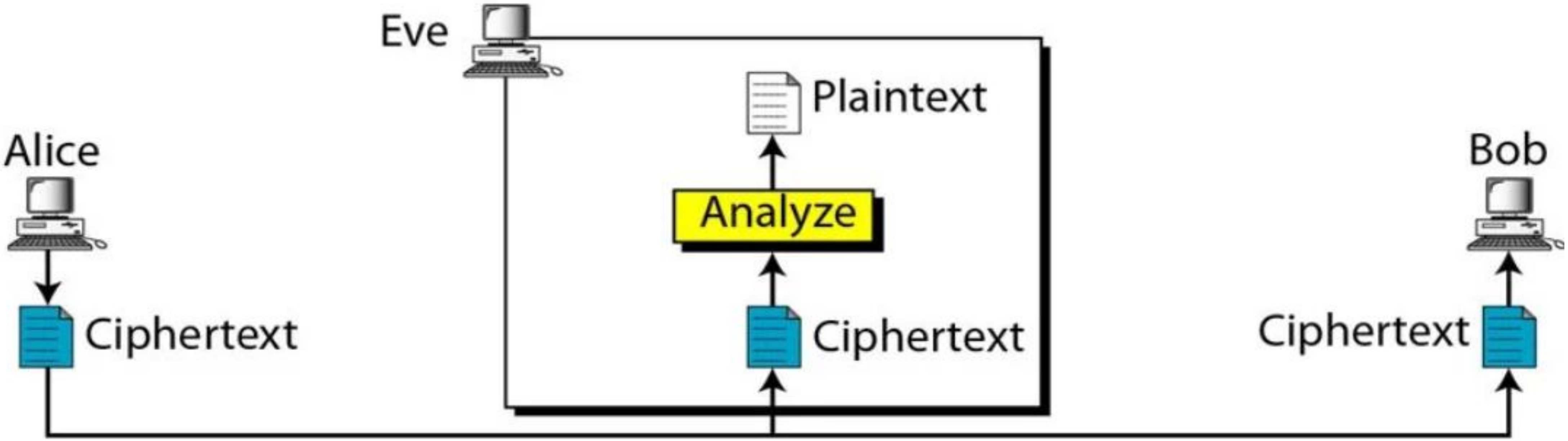
Pattern Attack



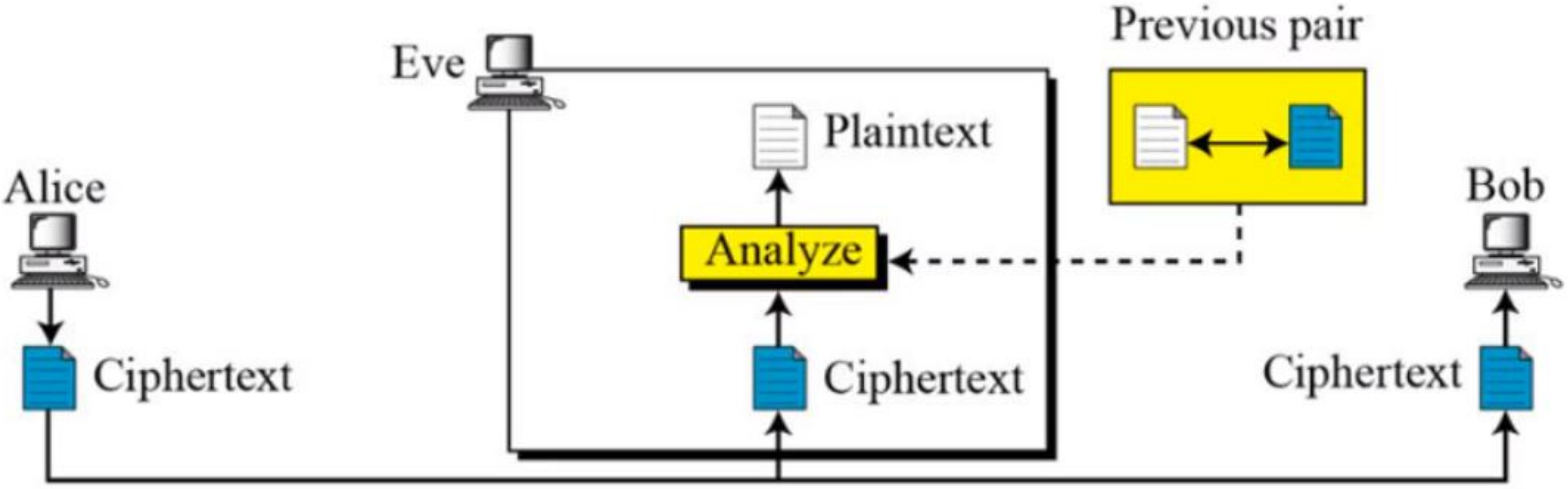
"KHOOR ZRUOG"

"HELLO WORLD"

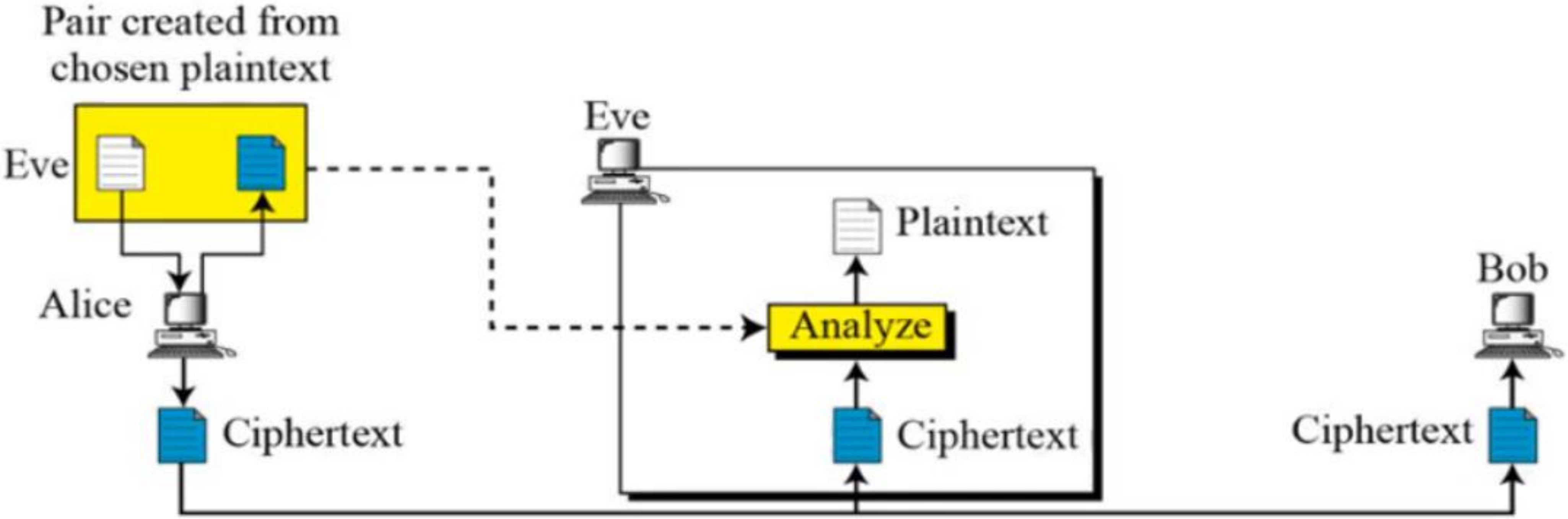
Ciphertext Only Attack



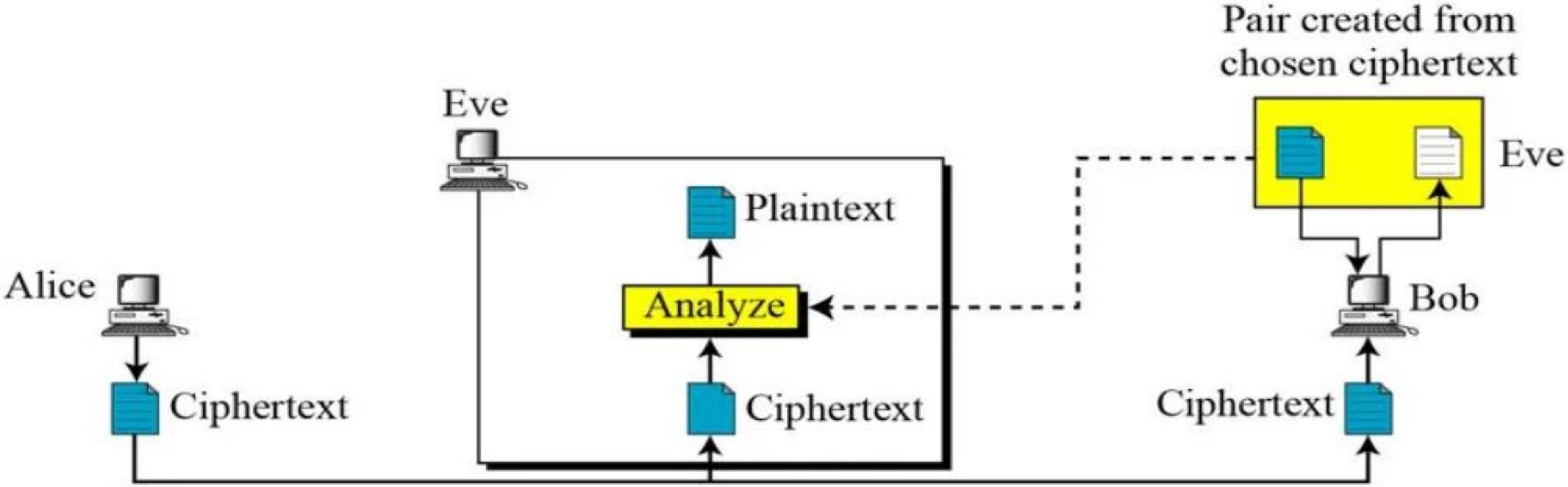
Known Plaintext Attack



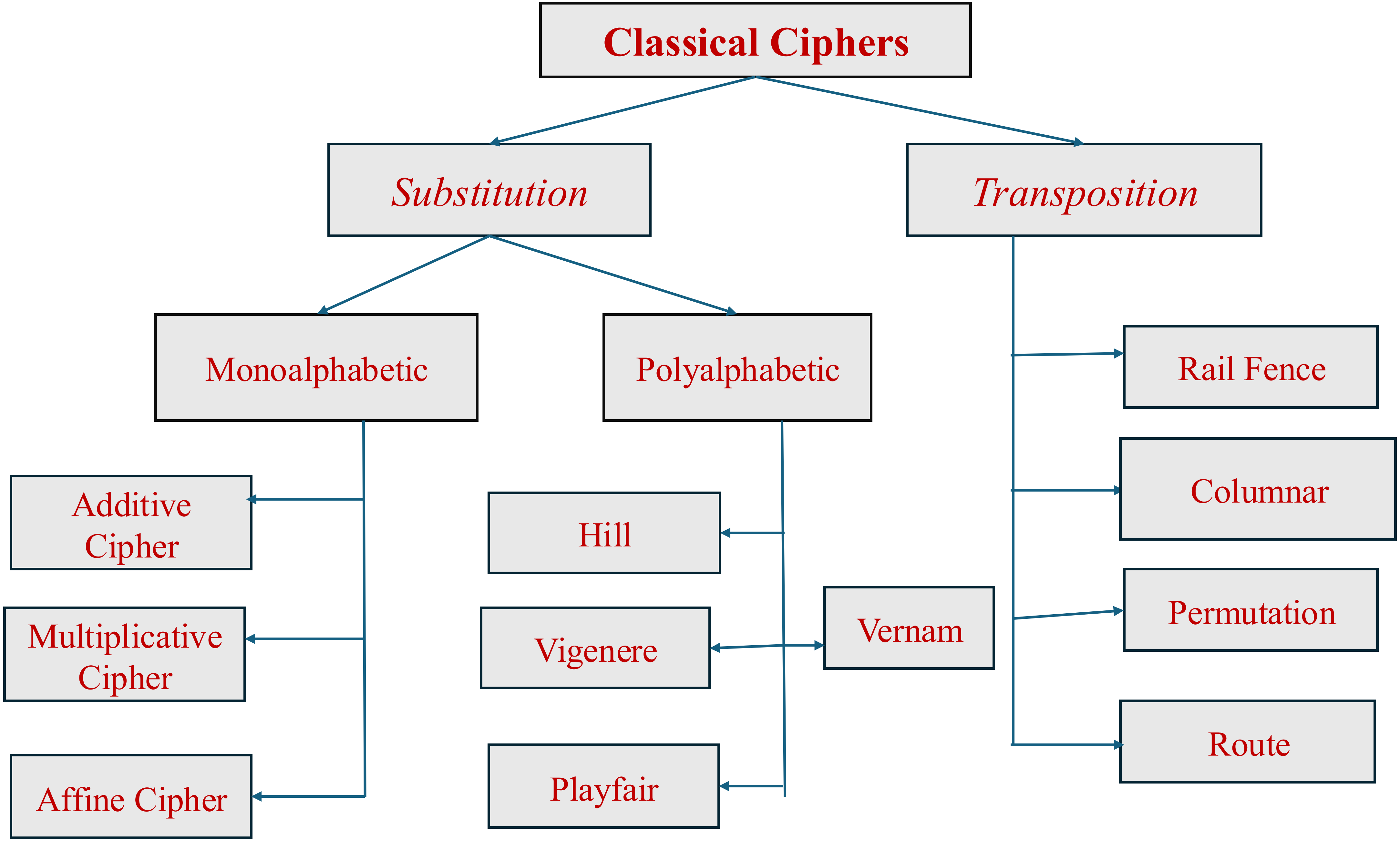
Chosen Plaintext Attack



Chosen Ciphertext Attack



HIERARCHY OF CLASSICAL CIPHERS



Classical Ciphers

Substitution

Transposition

Monoalphabetic

Polyalphabetic

Additive Cipher

Multiplicative Cipher

Affine Cipher

Hill

Vigenere

Vernam

Playfair

Rail Fence

Columnar

Permutation

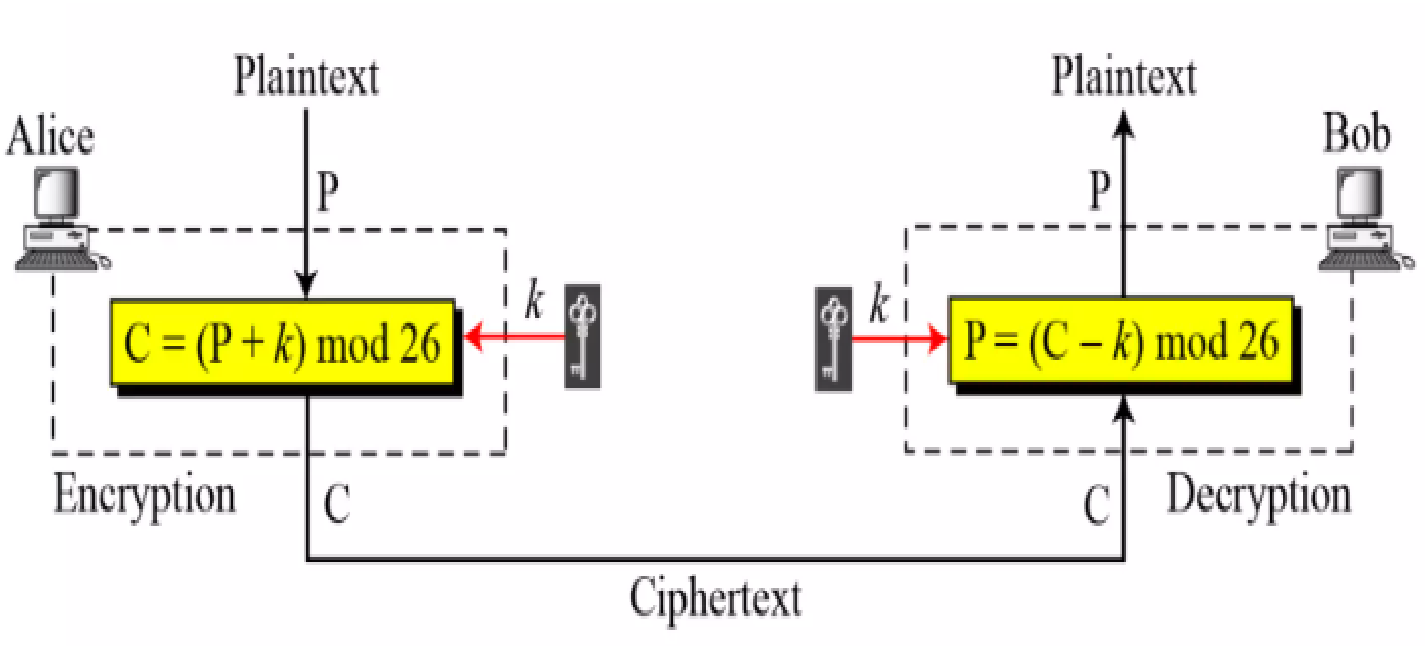
Route

Default Numerical Values

Character	Numerical Equivalent	Character	Numerical Equivalent
a	0	n	13
b	1	o	14
c	2	p	15
d	3	q	16
e	4	r	17
f	5	s	18
g	6	t	19
h	7	u	20
i	8	v	21
j	9	w	22
k	10	x	23
l	11	y	24
m	12	z	25

ADDITIVE CIPHER

Additive Cipher

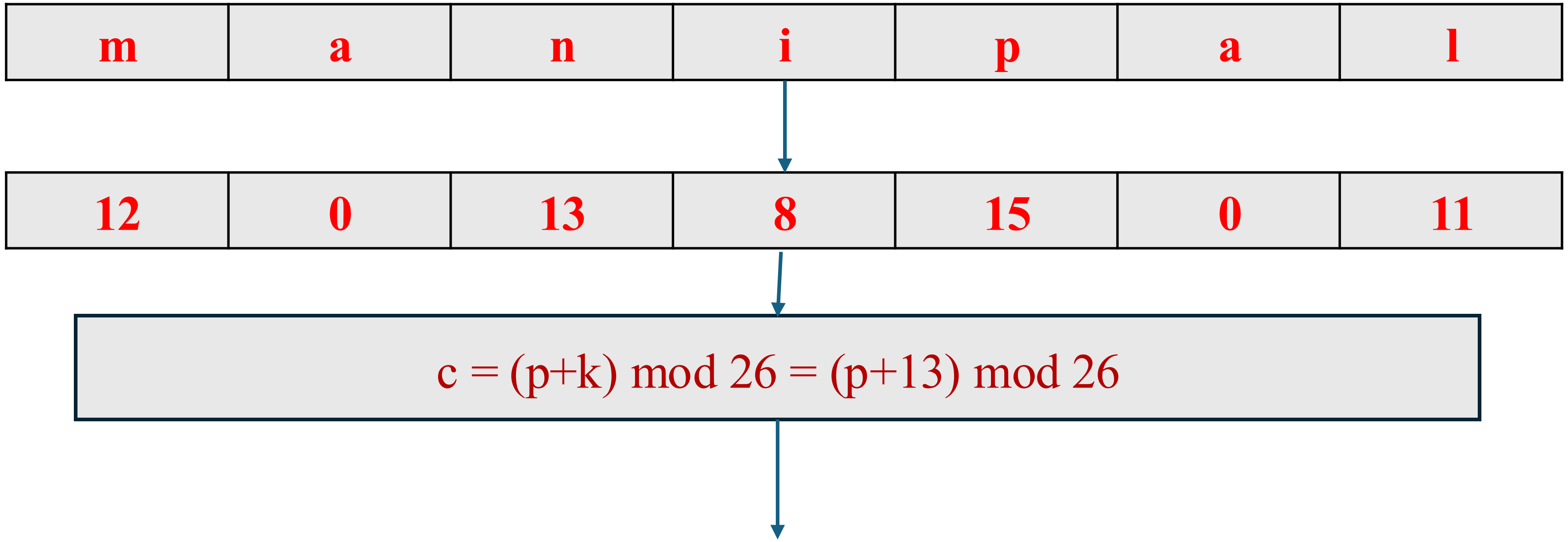


- Also called as Shift cipher.
- Here the key, PT and CT are in Z_{26}.

Example 1

Encrypt the message “**manipal**” using key = 13, and additive cipher in Z_{26}. Assume that the alphabets are case-insensitive and use the default numerical equivalents.

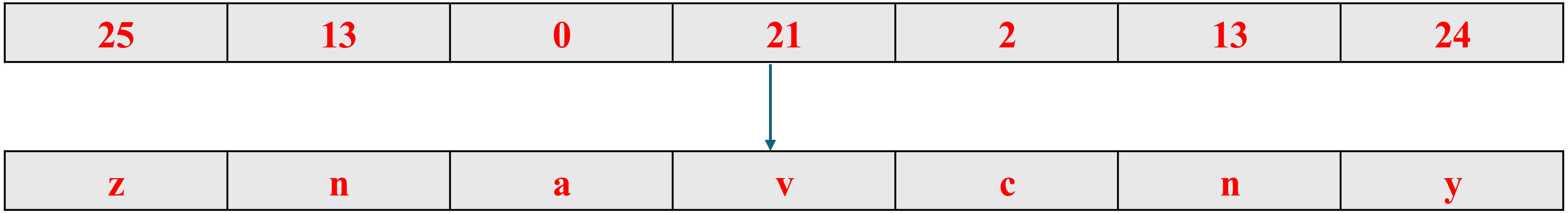
Solution:-



m	a	n	i	p	a	l
12	0	13	8	15	0	11

$c = (p+k) \bmod 26 = (p+13) \bmod 26$

Example 1 (Contd..)



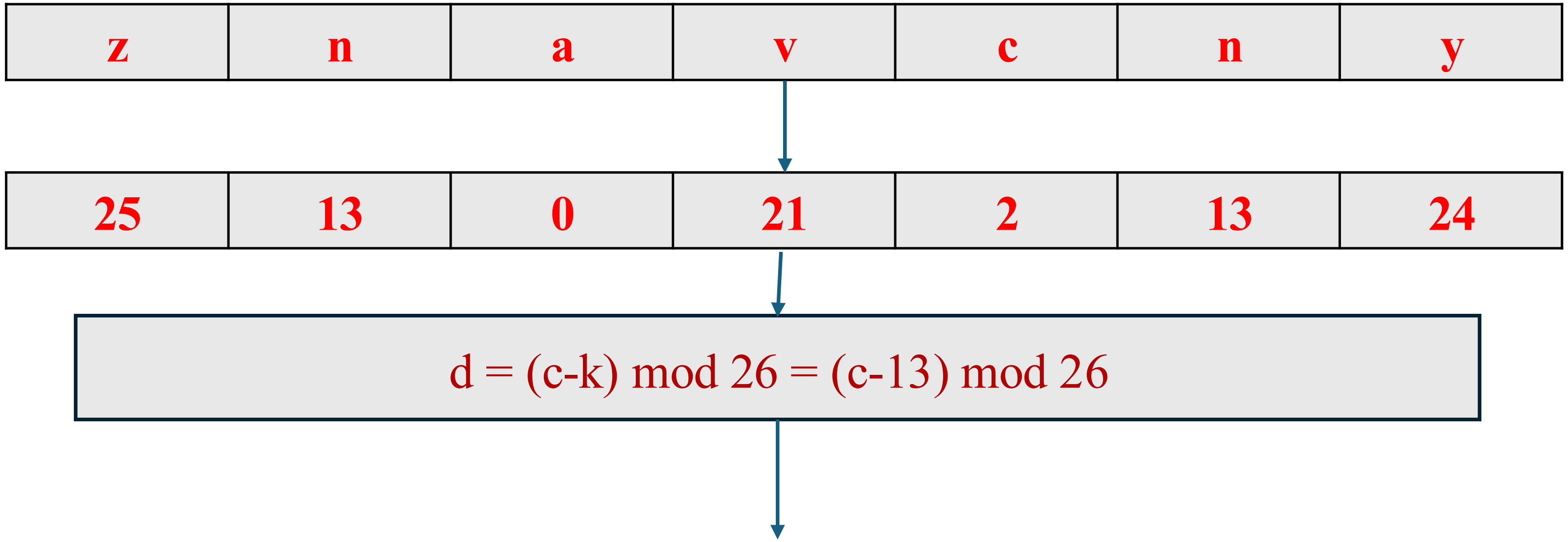
25	13	0	21	2	13	24
z	n	a	v	c	n	y

- Therefore, the encrypted message is “**znavcny**”.

Example 2

Decrypt the message “**znavcny**” using key = 13, and additive cipher in Z_{26}. Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-



z	n	a	v	c	n	y
25	13	0	21	2	13	24

d = (c-k) mod 26 = (c-13) mod 26

Example 2 (Contd..)

12	0	13	8	15	0	11
m	a	n	i	p	a	l

- Therefore, the decrypted message is “**manipal**”.

Example 3

Assume that Additive cipher is used with some special characters with their corresponding numerical equivalents as displayed in the table below. Assume that the alphabets which are used are case-insensitive and use the default numerical equivalents. Decrypt the ciphertext “**>d@$d>>h$d@w**” using key = 23.

Special Characters	Numerical Equivalents
?	26
>	27
<	28
@	29
#	30
$	31
!	32

Example 3 (Solution)

- > (27) → {d = (c-23) mod 33} → 4 (e)
- d (3) → {d = (c-23) mod 33} → 13 (n)
- @ (29) → {d = (c-23) mod 33} → 6 (g)
- $ (31) → {d = (c-23) mod 33} → 8 (i)
- d (3) → {d = (c-23) mod 33} → 13 (n)
- > (27) → {d = (c-23) mod 33} → 4 (e)
- > (27) → {d = (c-23) mod 33} → 4 (e)

Example 3 (Solution)

- h (7) → {d = (c-23) mod 33} → 17 (r)
- $ (31) → {d = (c-23) mod 33} → 8 (i)
- d (3) → {d = (c-23) mod 33} → 13 (n)
- @ (29) → {d = (c-23) mod 33} → 6 (g)
- w (22) → {d = (c-23) mod 33} → 32 (!)

- Therefore, the decrypted text is “**engineering!**”

Digrams on Additive Ciphers

- Pairs of alphabets or characters are encrypted or decrypted.
- Most commonly used digrams in plaintexts are ‘th’, ‘he’, ‘in’, etc.
- c = (p+k) mod 676, when only alphabets are used by ignoring the case.
- d = (c-k) mod 676, when only alphabets are used by ignoring the case.

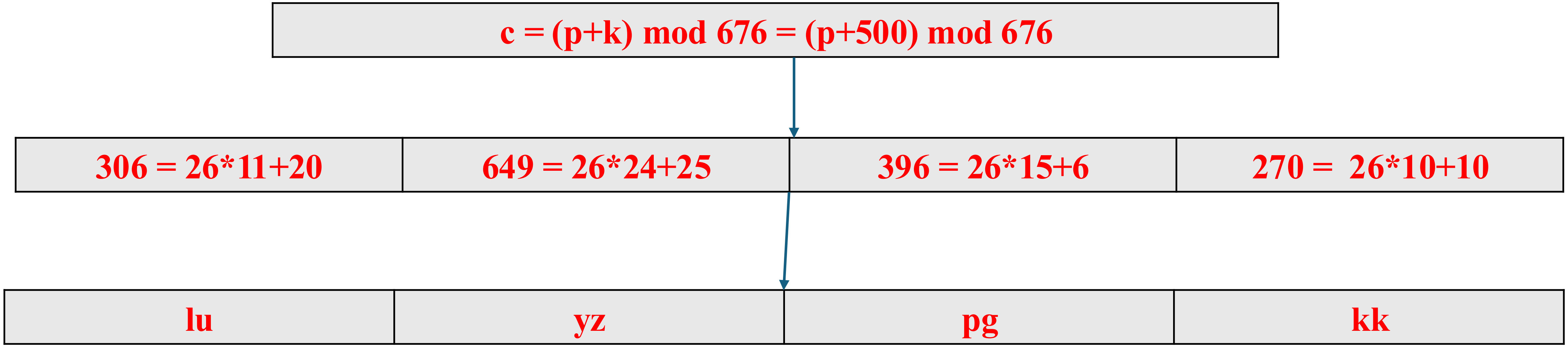
Additive Cipher with digram (Example 1)

Encrypt the message “**software**” using key = 500, and additive cipher using digrams. Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-

so	**ft**	**wa**	**re**
26*18+14 = 482	**26*5+19 = 149**	**26*22+0 = 572**	**26*17+4 = 446**

Additive Cipher with digram (Example 1) (Contd..)



c = (p+k) mod 676 = (p+500) mod 676

306 = 26*11+20	**649 = 26*24+25**	**396 = 26*15+6**	**270 = 26*10+10**
lu	**yz**	**pg**	**kk**

- The ciphertext is “**luyzpgkk**”.

Additive Cipher with digram (Example 2)

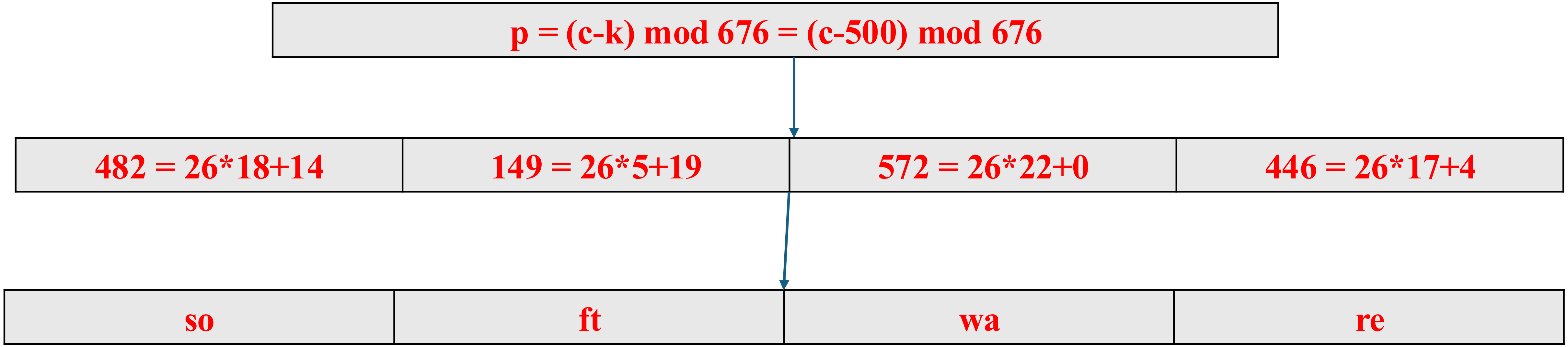
Decrypt the message “**luyzpgkk**” using key = 500, and additive cipher using digrams. Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-

lu	**yz**	**pg**	**kk**

26*11+20 = 306	**26*24+25 = 649**	**26*15+6 = 396**	**26*10+10 = 270**

Additive Cipher with digram (Example 2) (Contd..)



p = (c-k) mod 676 = (c-500) mod 676

482 = 26*18+14	149 = 26*5+19	572 = 26*22+0	446 = 26*17+4
so	ft	wa	re

- The decrypted text is “**software**”.

Caesar Cipher

- c = (p+3) mod 26
- d = (c-3) mod 26
- Ciphertext corresponding to the plaintext “udupi” is “xgxsl”
- Plaintext corresponding to the ciphertext “pdqlsdo” is “manipal”.
- However, Caesar cipher is generalized as additive cipher to use key of any value.

Pros and Cons of Additive Cipher

- Simple to understand, and Easy to implement.
- Demands negligible computational resources.

- Highly vulnerable to BFA.
- Vulnerable to Statistical attack.

HILL CIPHER

Hill Cipher

- Developed by Lester Hill in 1929.
- Uses concepts of Linear Algebra.
- C = P * K (mod 26), where P is of order m*n, and K is of order n*n.
- D = C * K^{-1} (mod 26)
- Note:- K is an invertible matrix, and GCD(det(K), 26) = 1

Example 1

- Encrypt the plaintext "**engineer**" using Hill Cipher with the key matrix displayed below. Assume that only alphabets are used for encryption/decryption, by ignoring the case.

K = $\begin{bmatrix} 5 & 6 \\ 3 & 9 \end{bmatrix}$

Solution:-

- P = $\begin{bmatrix} e & n \\ g & i \\ n & e \\ e & r \end{bmatrix} = \begin{bmatrix} 4 & 13 \\ 6 & 8 \\ 13 & 4 \\ 4 & 17 \end{bmatrix}$

- C = P*K (mod 26)

Example 1 (Contd..)

- $C = \begin{bmatrix} 4 & 13 \\ 6 & 8 \\ 13 & 4 \\ 4 & 17 \end{bmatrix} * \begin{bmatrix} 5 & 6 \\ 3 & 9 \end{bmatrix} \pmod{26} = \begin{bmatrix} 59 & 141 \\ 54 & 108 \\ 77 & 114 \\ 71 & 177 \end{bmatrix} \pmod{26}$

- $C = \begin{bmatrix} 7 & 11 \\ 2 & 4 \\ 25 & 10 \\ 19 & 21 \end{bmatrix} = \begin{bmatrix} \mathbf{h} & \mathbf{l} \\ \mathbf{c} & \mathbf{e} \\ \mathbf{z} & \mathbf{k} \\ \mathbf{t} & \mathbf{v} \end{bmatrix}$

- Therefore, the ciphertext is “**hlcezktv**”.

Example 2

- Decrypt the ciphertext "**hlcezktv**" using Hill Cipher with the key matrix displayed below. Assume that only alphabets are used for encryption/decryption, by ignoring the case.

$$K = \begin{bmatrix} 5 & 6 \\ 3 & 9 \end{bmatrix}$$

Solution:-

- det(K) = 27

- $C = \begin{bmatrix} h & l \\ c & e \\ z & k \\ t & v \end{bmatrix} = \begin{bmatrix} 7 & 11 \\ 2 & 4 \\ 25 & 10 \\ 19 & 21 \end{bmatrix}$

Example 2 (Contd..)

- $K^{-1} = \begin{bmatrix} 9 & -6 \\ -3 & 5 \end{bmatrix} * 27^{-1} \pmod{26}$

q	a	b	r	u1	u2	u
1	27	26	1	1	0	1
26	26	1	0	0	1	-26
	1	0		1	-26	

- $K^{-1} = \begin{bmatrix} 9 & -6 \\ -3 & 5 \end{bmatrix} * 1 \pmod{26} = \begin{bmatrix} 9 & 20 \\ 23 & 5 \end{bmatrix}$

Example 2 (Contd..)

- $D = C*K^{-1} \pmod{26} = \begin{bmatrix} 7 & 11 \\ 2 & 4 \\ 25 & 10 \\ 19 & 21 \end{bmatrix} * \begin{bmatrix} 9 & 20 \\ 23 & 5 \end{bmatrix} \pmod{26}$
- $D = \begin{bmatrix} 316 & 195 \\ 110 & 60 \\ 455 & 550 \\ 654 & 485 \end{bmatrix} \pmod{26} = \begin{bmatrix} 4 & 13 \\ 6 & 8 \\ 13 & 4 \\ 4 & 17 \end{bmatrix} = \begin{bmatrix} \mathbf{e} & \mathbf{n} \\ \mathbf{g} & \mathbf{i} \\ \mathbf{n} & \mathbf{e} \\ \mathbf{e} & \mathbf{r} \end{bmatrix}$
- Therefore, the decrypted text is "**engineer**".

Example 3

- Decrypt the ciphertext “**rrlmwbkaspdh**” using Hill Cipher with the key matrix displayed below. Assume that only alphabets are used for encryption/decryption, by ignoring the case.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Solution:-

$$C = \begin{bmatrix} r & r & l \\ m & w & b \\ k & a & s \\ p & d & h \end{bmatrix} = \begin{bmatrix} 17 & 17 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \\ 15 & 3 & 7 \end{bmatrix}$$

Example 3 (Contd..)

- $K^{-1} = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} * (-939)^{-1} \pmod{26}$

- $K^{-1} = \begin{bmatrix} -300 & 313 & -267 \\ 357 & -313 & 252 \\ -6 & 0 & 51 \end{bmatrix} * (939)^{-1} \pmod{26}$

- $K^{-1} = \begin{bmatrix} -300 & 313 & -267 \\ 357 & -313 & 252 \\ -6 & 0 & 51 \end{bmatrix} * 9 \pmod{26} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$

Example 3 (Contd..)

- D = C * K^{-1} (mod 26) = $\begin{bmatrix} 17 & 17 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \\ 15 & 3 & 7 \end{bmatrix} * \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$ (mod 26)

- D = $\begin{bmatrix} 587 & 442 & 544 \\ 402 & 482 & 329 \\ 472 & 90 & 456 \\ 273 & 186 & 362 \end{bmatrix}$ (mod 26) = $\begin{bmatrix} 15 & 0 & 24 \\ 12 & 14 & 17 \\ 4 & 12 & 14 \\ 13 & 4 & 24 \end{bmatrix} = \begin{bmatrix} p & a & y \\ m & o & r \\ e & m & o \\ n & e & y \end{bmatrix}$

- Therefore, the decrypted text is "**paymoremoney**".

Pros and Cons of Hill Cipher

- Simple and Easy to understand and implement with prior knowledge of linear algebra.
- More resistant to statistical attack than that for any other monoalphabetic ciphers.
- Use of matrices adds an additional level of security.

- Limited key size and key space if 2*2 matrix is used as the key.
- Poor efficiency for encrypting and decrypting data using large key matrices.

VIGENERE CIPHER

Vigenere Cipher

- The length of the key is made equal to that of the plaintext or ciphertext if its not the case already.
- $c_i = (p_i + k_{i \text{ mod } m}) \text{ mod } 26$
- $p_i = (c_i - k_{i \text{ mod } m}) \text{ mod } 26$
- Typically, m is lesser than the length of plaintext or ciphertext.

Example 1

- Encrypt the plaintext "**karnataka**" using Vigenere Cipher and the key "**hello**". Assume that the encryption/decryption is done using only alphabets by ignoring the case.

Solution:-

PT	**k** **(10)**	**a** **(0)**	**r** **(17)**	**n** **(13)**	**a** **(0)**	**t** **(19)**	**a** **(0)**	**k** **(10)**	**a** **(0)**

+

Key	**h** **(7)**	**e** **(4)**	**l** **(11)**	**l** **(11)**	**o** **(14)**	**h** **(7)**	**e** **(4)**	**l** **(11)**	**l** **(11)**

(mod 26) =

Example 1 (Contd..)

CT	**17** **(r)**	**4** **(e)**	**2** **(c)**	**24** **(y)**	**14** **(o)**	**0** **(a)**	**4** **(e)**	**21** **(v)**	**11** **(l)**

- Therefore, the ciphertext is “**recyoaevl**”.

Example 2

- Decrypt the ciphertext “**recyoaevl**” using Vigenere Cipher and the key “**hello**”. Assume that the encryption/decryption is done using only alphabets by ignoring the case.

Solution:-

CT	**r** **(17)**	**e** **(4)**	**c** **(2)**	**y** **(24)**	**o** **(14)**	**a** **(0)**	**e** **(4)**	**v** **(21)**	**l** **(11)**

-

Key	**h** **(7)**	**e** **(4)**	**l** **(11)**	**l** **(11)**	**o** **(14)**	**h** **(7)**	**e** **(4)**	**l** **(11)**	**l** **(11)**

(mod 26) =

Example 2 (Contd..)

PT	**10** **(k)**	**0** **(a)**	**17** **(r)**	**13** **(n)**	**0** **(a)**	**19** **(t)**	**0** **(a)**	**10** **(k)**	**0** **(a)**

- Therefore, the decrypted text is “**karnataka**”.

Example 3

- Decrypt the ciphertext “**yitpiyxugubnmtf**” using Vigenere Cipher and the key “**manipal**”. Assume that the encryption/decryption is done using only alphabets by ignoring the case.

Solution:-

CT	y (24)	i (8)	t (19)	p (15)	i (8)	y (24)	x (23)	u (20)	g (6)	u (20)	b (1)	n (13)	m (12)	t (19)	f (5)

-

Key	m (12)	a (0)	n (13)	i (8)	p (15)	a (0)	l (11)	m (12)	a (0)	n (13)	i (8)	p (15)	a (0)	l (11)	m (12)

(mod 26) =

Example 3 (Contd..)

PT	**12** **(m)**	**8** **(i)**	**6** **(g)**	**7** **(h)**	**19** **(t)**	**24** **(y)**	**12** **(m)**	**8** **(i)**	**6** **(g)**	**7** **(h)**	**19** **(t)**	**24** **(y)**	**12** **(m)**	**8** **(i)**	**19** **(t)**

- Therefore, the decrypted text is “**mightymightymit**”.

Pros and Cons of Vigenere Cipher

- Simple to understand and easy to implement.
- More resistant to statistical attack and pattern attack when compared to that of monoalphabetic ciphers.
- When the PT is long, the cipher is resistant to BFA if the key is long enough.

- Vulnerable to BFA if PT is extremely short.
- Vulnerable to statistical attack if key length is significantly lesser than that of the plaintext.
- Vulnerable to pattern attack if key length is significantly lesser than that of the plaintext.

PLAYFAIR CIPHER

Playfair Cipher

- Invented by Charles Wheatstone in the year 1854.
- Encrypts or decrypts digrams.
- Key is a 5*5 matrix with all the alphabets (letters i and j are considered as a single entry appropriately) arranged row-wise.

Generation of key matrix from key

- Initially the alphabets of the key are arranged row-wise in a 5*5 matrix, by removing duplicates from the key.
- Rest of the vacancies of the matrix are filled with remaining alphabets.

Generation of key matrix from key (Example 1)

- Consider that the key is “UDUPI”.
- The corresponding key matrix will be:-

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

Generation of key matrix from key (Example 2)

- Consider that the key is “JAIPUR”.
- The corresponding key matrix will be:-

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

Steps for Processing Plaintexts

- Plaintext is processed as each digram at a time.
- Plaintext is modified (if necessary) to make sure that no digram has a duplicate alphabet (by replacing a duplicate alphabet by x).
- Plaintext is modified (if necessary) to make sure that no alphabet is left unpaired (by adding x to the last alphabet of the original plaintext to make it form a digraph).
- FEVER ➔ FEVERX
- SHEEP ➔ SHEXEP
- TEAM ➔ TEAM

Steps for Encrypting a Plaintext

- If both the alphabets of a digram are in the same row, then each alphabet is replaced by the alphabet immediately towards its right, in the row by considering right rotation.
- If both the alphabets of a digram are in the same column, then each alphabet is replaced by the alphabet immediately below it in the column by considering top-bottom rotation.
- Else, in a digram each alphabet is replaced by the alphabet which is in the same row but in the column of the other alphabet of the digraph.

Steps for Decrypting a Ciphertext

- If both the alphabets of a digram are in the same row, then each alphabet is replaced by the alphabet immediately towards its left, in the row by considering left rotation.
- If both the alphabets of a digram are in the same column, then each alphabet is replaced by the alphabet immediately above it in the column by considering bottom-top rotation.
- Else, in a digraph each alphabet is replaced by the alphabet which is in the same row but in the column of the other alphabet of the digram.

Example 1

- Encrypt the plaintext “CHENNAI” using the key “MANGALORE”.

Solution:-

- Key matrix:-

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

- Modified PT = CHENNAIX

Example 1 (Contd..)

- CH → EK
- EN → HE
- NA → GN
- IX → HY

- Therefore, the ciphertext is “**EKHEGNHY**”.

Example 2

- Decrypt the ciphertext “EKHEGNHY” using the key “MANGALORE”.

Solution:-

- Key matrix:-

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

- Modified CT = EKHEGNHY

Example 2 (Contd..)

- EK → CH
- HE → EN
- GN → NA
- HY → IX

- The decrypted text is “**CHENNAIX**”.
- Therefore, the final decrypted text is “**CHENNAI”.**

Example 3

- Encrypt the plaintext “HELLOINDIA” using the key “PLAYFAIR”.

Solution:-

- Key matrix:-

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

- Modified PT = HELXLOINDIAX

Example 3 (Contd..)

- HE → KG
- LX → YV
- LO → RV
- IN → EU
- DI → IR
- AX → YW

- Therefore, the ciphertext is “KGYVRVEUIR”.

Example 4

- Decrypt the ciphertext “LGXNDODENPDSAU” using the key “PRINCIPLESOFCRYPTOGRAPHY”.

Solution:-

- Key matrix:-

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

- Modified CT = LGXNDODENPDSAU

Example 4 (Contd..)

- LG ➔ SY
- XN ➔ MX
- DO ➔ ME
- DE ➔ TR
- NP ➔ IC
- DS ➔ KE
- AU ➔ YX

- The decrypted text is “SYMXMETRICKEYX”.
- Therefore, the final decrypted text is “SYMMETRICKEY”.

Story time

1. BSSBKQBSFRSW, key: History

2. BINBZTNBKNDMQDRW, key: Dawn

3. IDXWQFBSMXBQZOGQWEFCIZQG , key : Dawn

Pros and Cons of Playfair Cipher

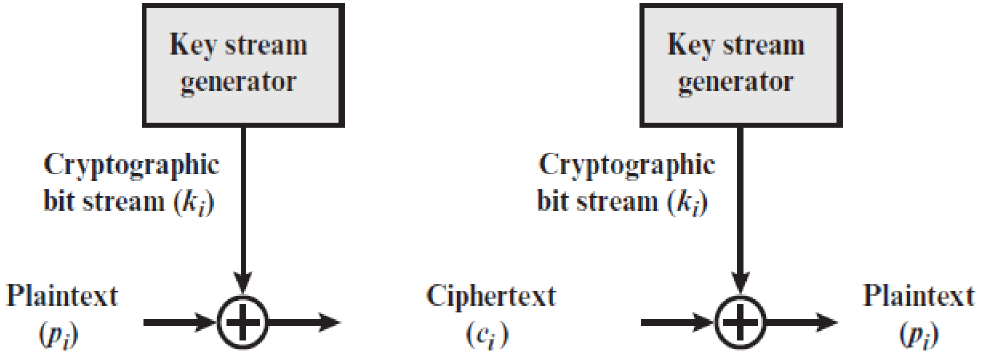
- Simple to understand and easy to implement when the plaintext length is even and when the original digrams don’t have duplicate alphabets.
- BFA on the cipher is almost impossible.
- Resistant to statistical and pattern attacks when the plaintexts are short.
- Key Management is easy.

- Implementation gets complicated when the plaintext length is odd, or the original digrams have duplicate alphabets.
- Vulnerable to statistical and pattern attacks when the plaintexts are long (> 1000 characters).

VERNAM CIPHER

Vernam Cipher

- Introduced by Gilbert Vernam in 1918.
- Length of the plaintext = Length of the key.
- More resistant to statistical attack when compared to Vigenere cipher.
- Initially, the algorithm was proposed with repeating phrases in the key.



One Time Pad

- Improved version of Vernam Cipher.
- Length of the key (random) = Length of the plaintext
- The key is discarded after every session.
- Produces a random ciphertext.
- Statistical attack becomes almost impossible.

One Time Pad (Examples)

- Encryption of “**cryptography**” using the key “**zabbcgvikjyx**” is “**brzqvubzkyfv**” (using only alphabets by ignoring the case).
- Encryption of “**cryptography**” using the key “**aghhqztuypfr**” is “**cxfwjnzlyemp**” (using only alphabets by ignoring the case).
- Encryption of “**operatingsystems**” using the key “**xgpuukrxfepsrxal**” is “**lvtludzklwnkkbmd**” (using only alphabets by ignoring the case).

Disadvantages of using One Time Pad

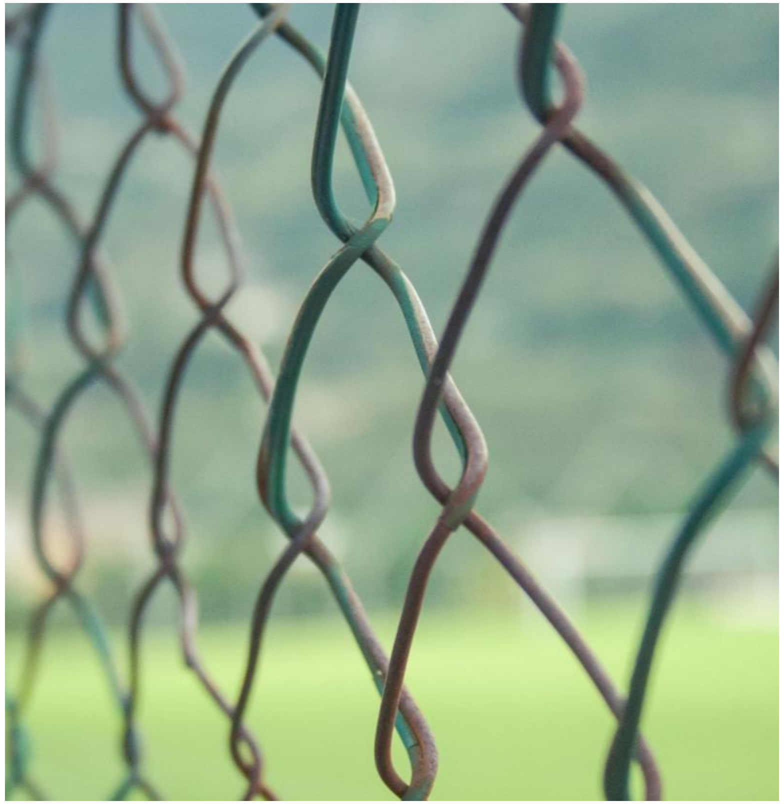
- Generation of large random key for every session, when the plaintext is huge.
- Key Management becomes harder.
- Most probably its used for only low bandwidth channels.

RAIL FENCE CIPHER

Rail Fence Cipher

- Encryption:- The plaintext characters are written as a sequence of diagonals in a table based on the depth (Number of rows = depth) in a zig-zag manner. The ciphertext is obtained by reading the characters in the Rail Fence table, row-wise.

- Decryption:- Create a blank table with rows equal to the depth and columns equal to the length of the ciphertext. Enter the first ciphertext character in the top-left cell, then move diagonally down to the last row and back up to the first row, placing the next character in the corresponding column when you return to the top. Continue this process, leaving blank spaces as needed until all characters are placed. Fill any remaining blank spaces row-wise with the remaining ciphertext characters. To decrypt, read the ciphertext characters diagonally in a zig-zag pattern.



Example 1

- Encrypt the plaintext “KANNIYAKUMARI” using Rail fence cipher with a depth of 2.

Solution:-

K		N		I		A		U		A		I
	A		N		Y		K		M		R	

- The ciphertext is “KNIAUAIANYKMR”.

Example 2

- Decrypt the ciphertext “KNIAUAIANYKMR” using Rail fence cipher with a depth of 2.

Solution:-

- Iteration 1:-

K		N		I		A		U		A		I
	_		_		_		_		_		_	

Example 2 (Contd..)

- Iteration 2:-

K		N		I		A		U		A		I
	A		N		Y		K		M		R	

- Therefore, the decrypted text is “KANNIYAKUMARI”.

Example 3

- Encrypt the plaintext “COMPUTERNETWORKS” using Rail Fence cipher with a depth of 3.

Solution:-

C				U				N				O			
	O		P		T		R		E		W		R		S
		M				E				T				K	

- The ciphertext is “CUNOOPTREWRSMETK”.

Example 4

- Decrypt the ciphertext "CUNOOPTREWRSMETK" using Rail fence cipher with a depth of 3.

Solution:-

- Iteration 1:-

C				U				N				O			
	_		_		_		_		_		_		_		_
		_				_				_				_	

Example 4 (Contd..)

- Iteration 2:-

C				U				N				O			
	O		P		T		R		E		W		R		S
		M				E				T				K	

- Therefore, the decrypted text is “COMPUTERNETWORKS”.

Example 5

- Decrypt the ciphertext “MLRAAUESNPNVIYIIT” using Rail fence cipher with a depth of 4.

Solution:-

- Iteration 1:-

M						L						R				
	_				_		_				_		_			
		_		_				_		_				_		_
			_						_						_	

Example 5 (Contd..)

- Iteration 2:-

M						L						R				
	A				A		U				E		S			
		N		P				N		V				I		Y
			I						I						T	

- The decrypted text is “MANIPALUNIVERSITY”.

Pros and Cons of Rail Fence Cipher

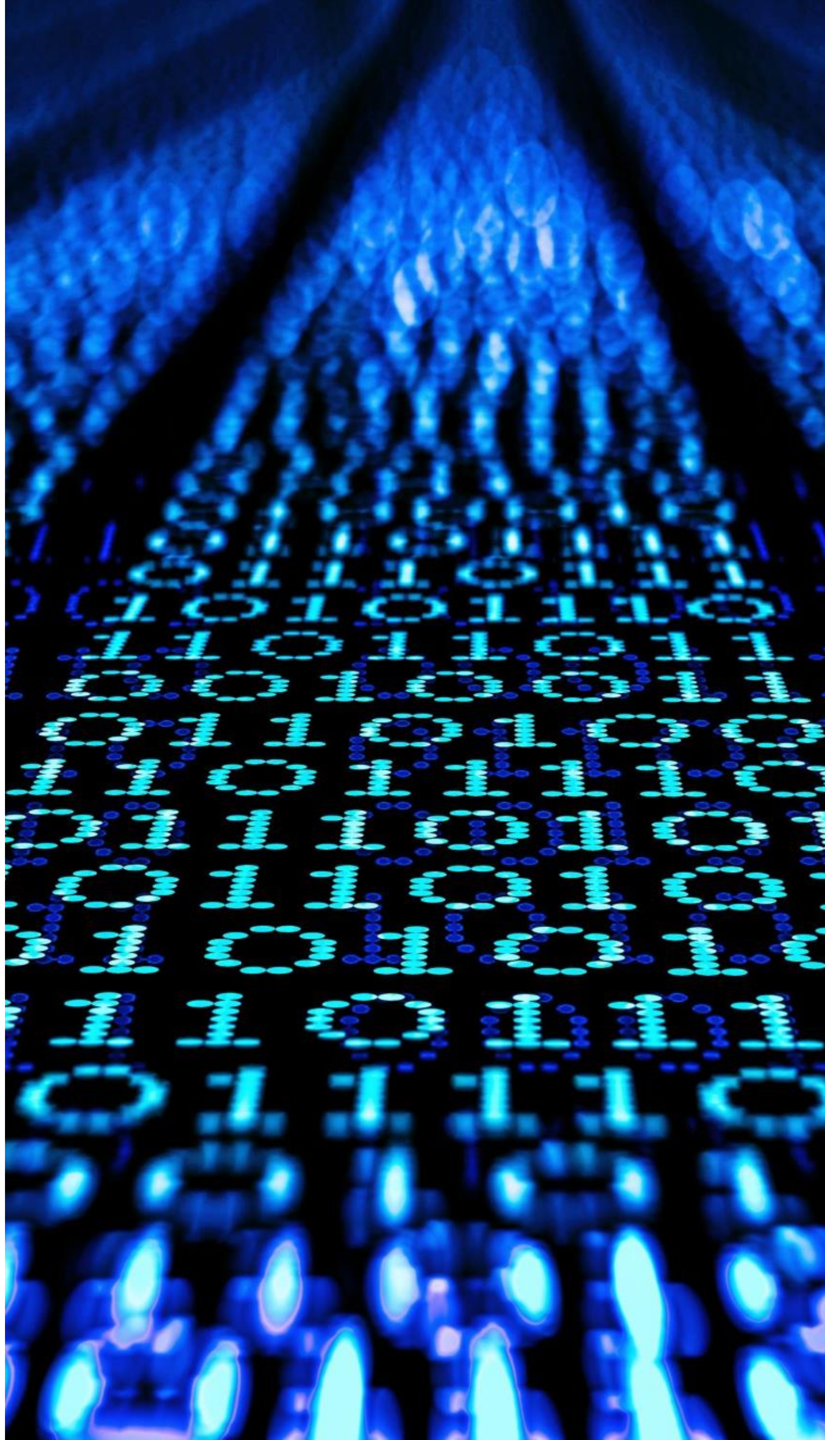
- Simple to understand and easy to implement.
- Has got low computation cost.

- Vulnerable to Statistical attack.
- Vulnerable to Pattern attack.
- Vulnerable to BFA.

COLUMNAR CIPHER

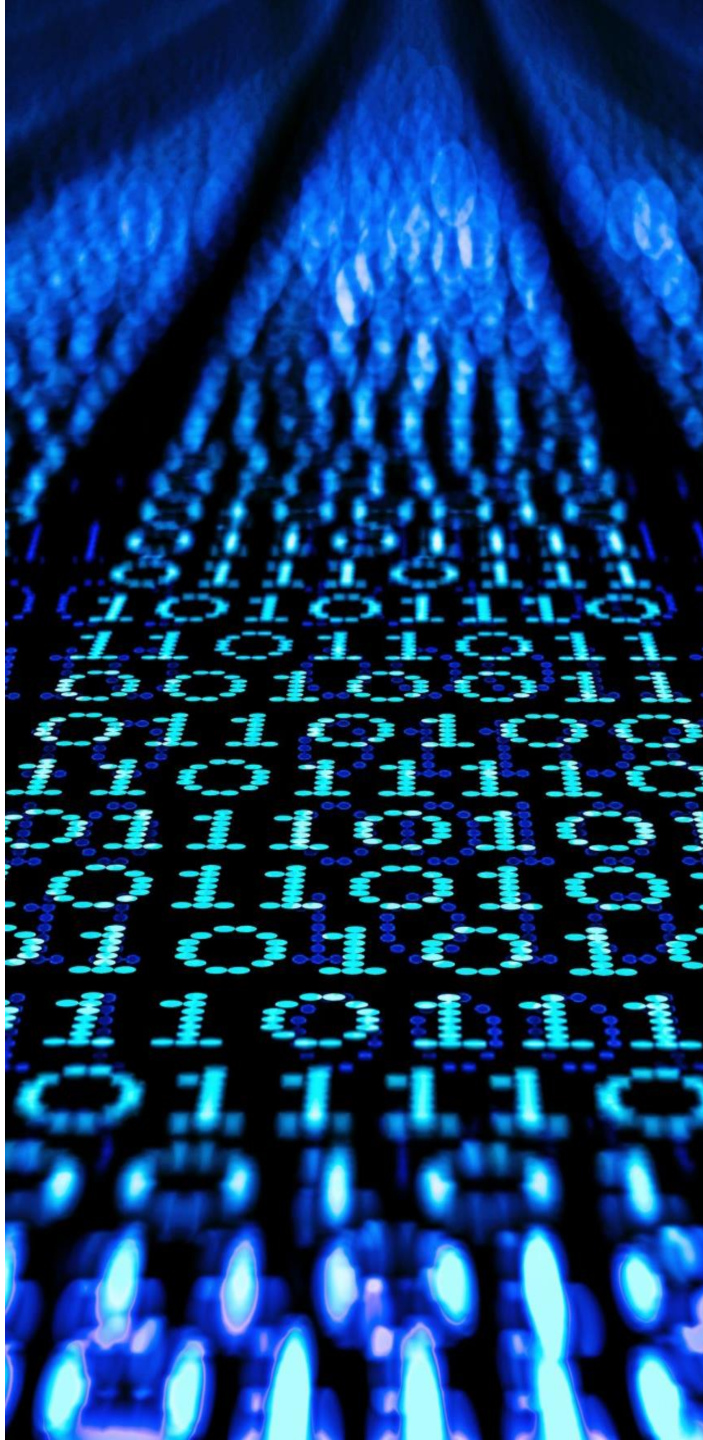
Columnar Cipher

- Provides grid-based encryption and decryption.
- The plaintext is written row-wise, and the ciphertext is generated by reading the plaintext characters column-wise.
- The ciphertext is written column-wise in a certain order, and the decrypted text is generated by reading the ciphertext characters row-wise.
- The key contains a sequence of numbers representing the order of columns.
- Multiple stages can be used to enhance the security.



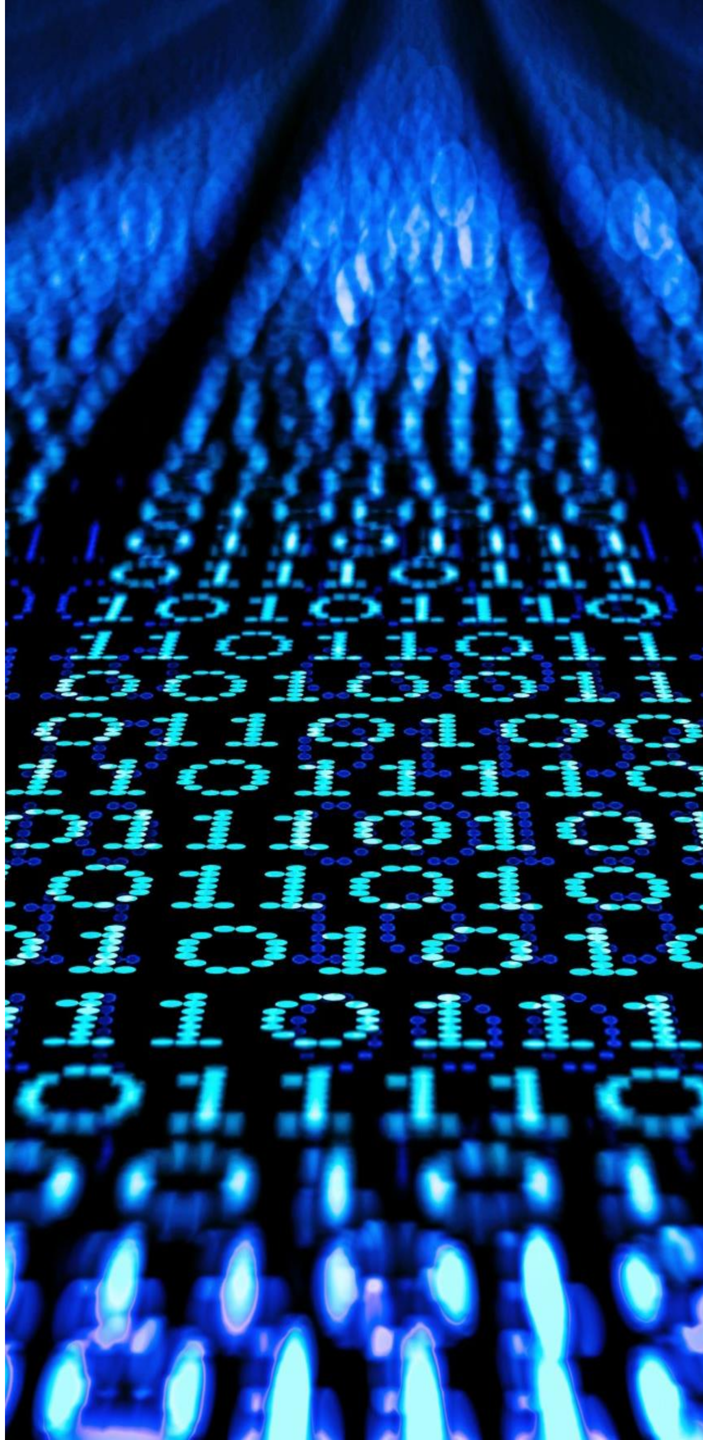
Processing the key

- The key could either be represented as a sequence of numbers or as a text.
- If the key is a text, then the text is converted into a sequence of numbers according their alphabetical order in the text.
- The length of the key = number of columns.
- Assume that the key is ‘4 2 1 3 5’. This indicates that the grid consists of 5 columns.
- If the key is ‘hello’, then the corresponding sequence of numbers for the key would be ‘2 1 3 4 5’.



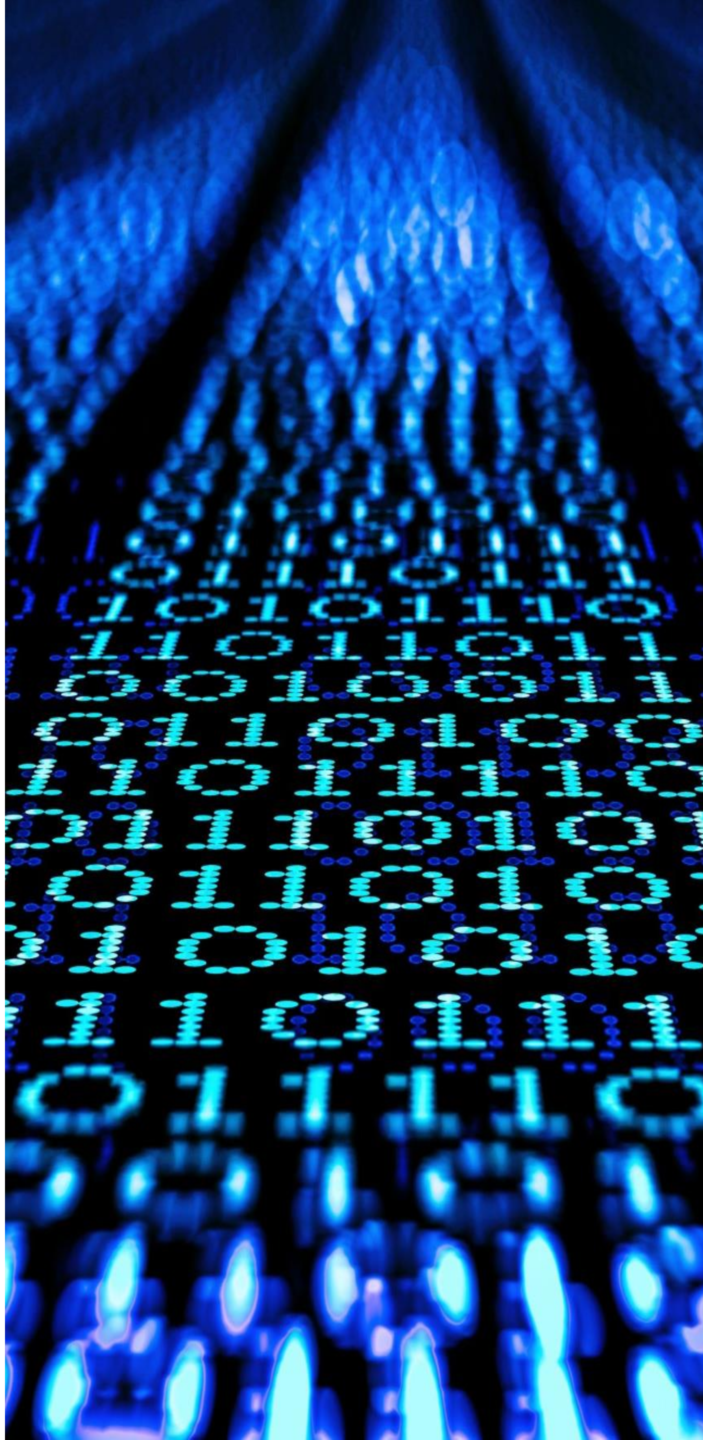
Steps for Encryption

- Number of Rows = Ceil(Length(PT)/Number of Columns)
- Fill the grid row-wise with plaintext characters (At the end, fill any vacancy with ‘x’).
- Obtain the ciphertext, by reading the plaintext characters column-wise according to sequence of numbers.
- For example, a key having a sequence ‘3 1 2’ indicates that the grid has 3 columns. Moreover, during CT calculation, the second column is read first, third column is read second, and the first column is read third.



Steps for Decryption

- Number of Rows = Length(CT)/Number of Columns
- Fill the grid column-wise with the Ciphertext characters according to sequence of numbers in the key.
- Obtain the Plaintext by reading the Ciphertext characters row-wise.
- For example, if the key has a sequence ‘3 1 2’, then the second column is filled first, third column is filled second, and the first column is filled third.



Example 1

- Encrypt the plaintext “GOCORONAGO” using single stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”

G	O	C	O	R
O	N	A	G	O

- Therefore, the Ciphertext is “ONGOCAOGRO”.

Example 2

- Decrypt the Ciphertext “ONGOCAOGRO” using single stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”
- IT1:-

	O			
	N			

Example 2 (Contd..)

- IT2:-

G	O			
O	N			

- IT3:-

G	O	C	O	R
O	N	A	G	O

- Therefore, the decrypted text is “GOCORONAGO”.

Example 3

- Encrypt the plaintext “GOCORONAGO” using double stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”

G	O	C	O	R
O	N	A	G	O

- CT after first stage encryption:- “ONGOCAOGRO”.

Example 3 (Contd..)

- Now encrypt “ONGOCAOGRO”.

2	1	3	4	5
O	N	G	O	C
A	O	G	R	O

- Therefore, the final Ciphertext is “NOOAGGORCO”.

Example 4

- Decrypt the Ciphertext “NOOAGGORCO” using double stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”

O	N	G	O	C
A	O	G	R	O

- Decrypted text after first stage decryption:- “ONGOCAOGRO”.

Example 4 (Contd..)

- Now decrypt “ONGOCAOGRO” again.

2	1	3	4	5
G	O	C	O	R
O	N	A	G	O

- Hence, the final decrypted text is “GOCORONAGO”.

Example 5

- Decrypt the Ciphertext “CALONAIXACEIEIEMUMHXAHXADFXYRPODTNG” using double stage columnar transposition with key “MANIPAL”.

Solution:-

- “MANIPAL” →

5	1	6	3	7	2	4

Example 5 (Contd..)

5	1	6	3	7	2	4
A	C	F	E	O	A	M
H	A	X	I	D	I	U
X	L	Y	E	T	X	M
A	O	R	I	N	A	H
D	N	P	E	G	C	X

- The decrypted text after first stage decryption:- “ACFEOAMHAXIDIUXLYETXMAORINAHDNPEGCX”.

Example 5 (Contd..)

- Now decrypt “ACFEOAMHAXIDIUXLYETXMAORINAHDNPEGCX” again.

5	1	6	3	7	2	4
M	A	N	I	P	A	L
A	C	A	D	E	M	Y
O	F	H	I	G	H	E
R	E	D	U	C	A	T
I	O	N	X	X	X	X

- The decrypted text after second stage decryption:- “MANIPALACADEMYOFHIGHEREDUCATIONXXXX”.

- Hence, truncating the 4 ‘X’s at the end, the decrypted text is “MANIPALACADEMYOFHIGHEREDUCATION”.

Pros and Cons of Columnar Transposition Cipher

- Simple to understand and straight forward to implement for short texts.
- Efficient for short texts.
- At times more resistant to statistical attack when compared to substitution attack.

- Highly vulnerable to Pattern analysis attack, when a short key is used, with a single stage transposition.
- Decrypting long ciphertexts could produce errors, if not implemented properly.