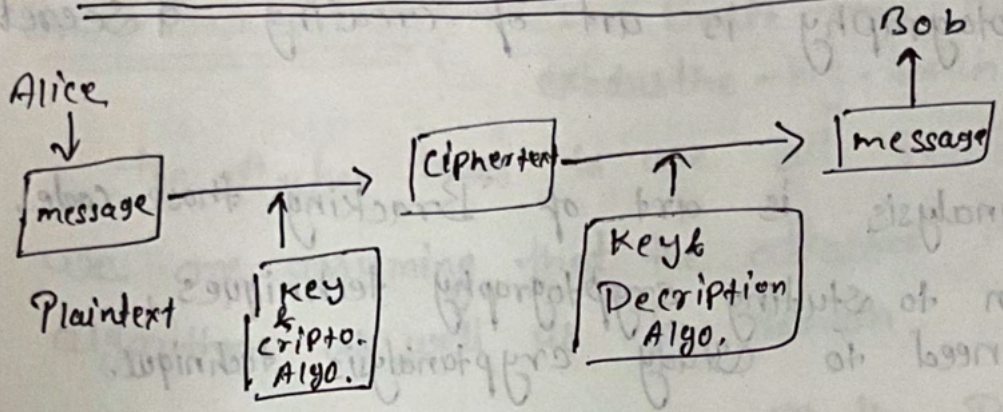
Chapter 3

Traditional Symmetric key ciphers



By using a symmetric key cipher, Alice & Bob have to use same key for Both Encryption & Decryption. Because of this the method is called symmetric.

If there are 'm' person in a group then each person needed m-1 keys to communicate with other person.

In total we need $\frac{m(m-1)}{2}$ keys

Encryption can be thought as locking the Box. & Decryption can be thought as unlocking the Box. In symmetric key encipherment Both locking & unlocking is done By the same key.

Kerckhoff's Principle :- According to this Principle one should always assume that the attacker knows the Encryption & Decryption Algorithm. The Security of message Based on the secrecy of key. In other word gussing the key is too difficult so No need to hide the encrytion & decryption Algorithm.

Cryptanalysis :-

The Cryptography is art of creating a secret code.

&

The Crytanalysis is art of Bracking those code.

In addition to studing cryptography techniques, we also need to study cryptanalysis technique.

This helps us to check the vulnerablity of our cryptography system.

Types of Cryptanalysis Attack :-

4 types of Cryptanalysis Attack.

1. Ciphertext only
2. Known-plaintext
3. Chosen-plaintext
4. Chosen-ciphertext

(1) Ciphertext only :- By using only a ciphertext the Attacker tries to find 'Key' & 'plaintext'.

It is most Probable attack Because the attacker need only cypertext for Attack.

Various Methods are used to impliment ciphertext-only Attack.

① Brute-force-Attack :- In Brute-force-Method or exhaustive-key-search method the attacker tries to use all Possible Key.

we are assuming that the attacker knows the algorithm as well as key domain.

Attacker check every key untill the Plaintext make Sense.

This Attake is Difficult in the past, But it is Easier today using a computer.

To Prevent this attack the number of Possible key Must be very large.

② Statical Attack :- The Attacker can use the inherent characteristics of the Plaintext to launch Statical Attack.

for Example the letter 'E' is most-frequently used in English text. The Attacker finds the most frequent character in the text & Replase with E By finding Such type of pair He is able to find key, By key He is able to find Plain text.

To Prevent this type of attack we should have to hide the characterstic of the language.

③ Pattern Attack :- Some Algorithm may hide the characterstic of the language, but may create some pattern in the cypher. A Attecker may use this Patter to find a key.
So we have to use those algorithm which creates a randomness in the text.

#2 Known Plaintext Attack :- In this type of Attack the Attacker has a access of some plaintext / ciphertext pair. By using this Pairs It can Break the cyphertext.

The plaintext & ciphertext pair collected earlier.
for example :- A Sender Sends a content to network. the Attacker kept this cyphertext. After sometimes the content Become Public. Now the Attacker make a plaintext / cyphertext pair & use this Pair to Break newly coming message.

This Attack is less likely to happen.

#3 Chosen Plaintext Attack :- This Attack is similar to Known-Plaintext attack, the only difference is that the plaintext/ciphertext pair is chosen By the Attacker.

This attack is only happen when Attacker has a access to the sender computer.

By using the sender computer it can create some plaintext/ciphertext Pair & use it to Break upcoming cypher.

#4 Chosen-Ciphertext Attack :- This Attack is similar to Chosen Plaintext attack the only difference is that the attacker tries to create ciphertext/plaintext pair to decrypt the cypher.

This Attack only happen if the attacker have a access to the Receiver computer.

Categories of Traditional Ciphers :-

We can divide traditional Symmetric-key ciphers into two broad categories :-

(1) Substitution Cipher
(2) Transposition Cipher.

(1) Substitution cipher :- In this cipher we replace one character of Plaintext with another character.

If the character (symbol) is alphabate then we replace it with another alphabate.

If the symbol is number then we replace this symbol with another number.

This cipher is further categoriesed in

(a) Monoalphabatic cipher
(b) Polyalphabatic cipher

(a) Monoalphabatic cipher :-

In monolithic substitution, a character in the Plaintext is always changed to the same character in cyphertext.

for Example, If the algorithm says that letter A in the Plaintext is changed to letter D then every letter A is changed to letter D.

that is the relationship blw Plaintext & ciphertext is one to one.

Example :- 'hello' ⇒ KHOOR (It is monolithic)

'hello' ⇒ 'ABNZf (It is Not monolithic)

~~#Add~~ Different types of Monolithic Ciphers :-

(i) Additive Cipher :-

(1) This is also called "Shift cipher"
(2) This is also called "Caesar cipher"

we assign a numerical value to each upper case & Lowercase Alphabatic letter in Z_{26}

Plaintext	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
Ciphertext	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
value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The secret key is also between Sender ~~Alice~~ and Receiver ~~Bob~~ is in Z_{26}.

The Encryption algorithm adds a key to Plaintext.

&

The Decryption algorithm subtract a key from the Ciphertext

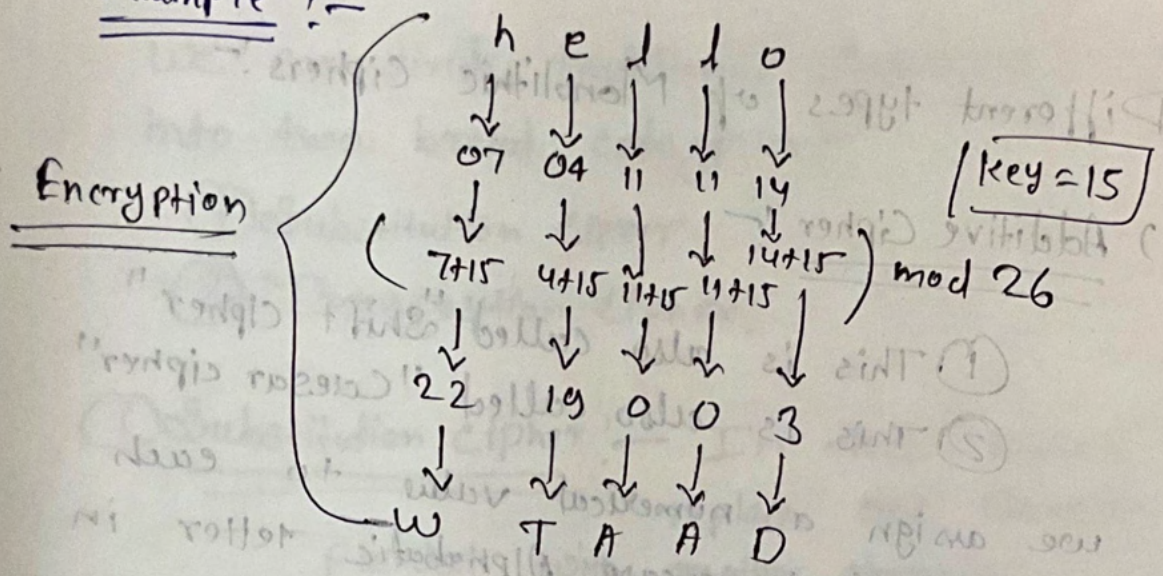
All operations are done in Z_{26}.

$C = (P + K) \bmod 26$ → Send → $P = (C - K) \bmod 26$

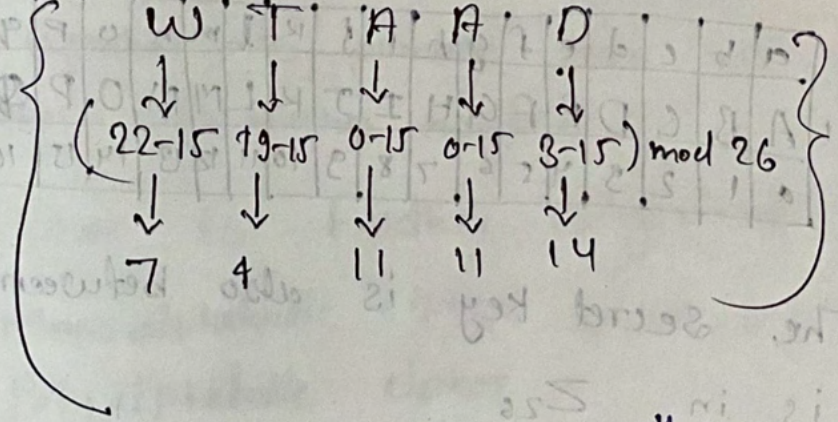
In addative cipher the plaintext, ciphertext, key are integers in Z_{26}.

Example :-

Encryption



Decryption :-



- Encryption algorithm interprited as "shift key character down".
  and Decryption algorithm inperprited as "shift key character up".

Julius Caesar used a Addative cipher to communicate with his officers. & for this addative cipher is also called caesar cipher.

The key used in this is '3'.

#Cryptanlysis of Additive cipher :- Additive cipher is vulnerable to "Ciphertext only Attack" using "Brute-force-attack". the key domain of additive cipher is very small.

Example :- Attacker has "~~HA~~ UVACLYFZLJ BYL"

the attacker try to use

Key	corrosponding Plaintext
1	tuzbkxeykiaxk
2	styajwdxjhzwj
3	rsxzivcwigyvi
4	qrwyhubvhfxuh
5	pqvxgtaugewtg
6	opuwfsztfdvsf
7	notveryseeure.

the Plaintext with key 7 make some sence.

#(ii) Multiplicative cipher :-

Here Encryption means multiplication of Plaintext By a key

& Decryption means mutiplication of ciphertext By a Multiplicative inverse of key.

The operations are in Z_{26}.

for multiplicative inverse the key must belongs to Z_{26}^*.

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

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

Example :- Key Domain of multiplicative cipher.

$Z_{26}^{*} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

we have plaintext "hello" & key = 7.

Encryption

h → (7×7) % 26 → 23 → X
e → (4×7) % 26 → 02 → C
l → (11×7) % 26 → 25 → Z
l → (11×7) % 26 → 25 → Z
o → (14×7) % 26 → 20 → U

Decryption with multiplicative inverse of 7 ⇒ 15

X → (23×15) % 26 → 7 → h
C → (2×15) % 26 → 4 → e
Z → (25×15) % 26 → 11 → l
Z → (25×15) % 26 → 11 → l
U → (20×15) % 26 → 14 → o

(iii) Affine cipher :- It is a combination of additive cipher and Multiplicative cipher.

It uses a pair of keys.

The first key is used with multiplicative cipher & the second key is used with additive cipher.

Both cipher is applied one after another.

$$C = (P \times K_1 + K_2) \bmod 26$$

$$P = ((C - K_2) \times K_1^{-1}) \bmod 26$$

~~One~~ Combination of operation should be reversed on other side..

$T = (P \times K_1) \bmod 26$

$C = (T + K_2) \bmod 26$

$T = (C - K_2) \bmod 26$

$P = (K_1^{-1} \times T) \bmod 26$

K_1^{-1} is multiplicative inverse of K_1

& # $-K_2$ is additive inverse of K_2

~~Note~~

Tips :- The affine cipher uses a pair of keys in which the first key is from Z_{26}^* & the second is from Z_{26}.

The size of key Domain is $26 \times 12 = 312$

Example :- By using affine cipher Encrypt & Decrypt the message "hello". with the key pair (7, 2).

we use 7 for multiplicative key & 2 for additive key.

h → 7	Encryption $((7 \times 7 + 2) \bmod 26)$	→ 25 → z
e → 4	Encryption $((4 \times 7 + 2) \bmod 26)$	→ 4 → e
l → 11	Encryption $((11 \times 7 + 2) \bmod 26)$	→ 1 → B
l → 11	Encryption $((11 \times 7) + 2) \bmod 26$	→ 1 → B
o → 14	Encryption $((14 \times 7 + 2) \bmod 26)$	→ 22 → w

~~No w~~

Now we have to decrypt this message :-

"ZEBBW"

the addative inverse of 2 is 24
& the multiplicative inverse of 7 is 15

Z → Decrept → $((25-2)\times 15) \bmod 26$ → 7 h
E → Decrept → $((4-2)\times 15) \bmod 26$ → 4 e
B → Decrept → $((1-2)\times 15) \bmod 26$ → 11 l
B → Decrept → $((1-2)\times 15) \bmod 26$ → 11 l
W → Decrept → $((22-2)\times 15) \bmod 26$ → 14 o

Note :- The addative cipher is special case of affine cipher with ~~k1=0~~ $K_1=1$

The multiplicative ciper is special case of affine cipher with $K_2=0$

Crytanalysis of Affine Cipher :-

#3 Monoalphabetic Substitution cipher :-

Because, additive, multiplicative, affine ciphers have small key domains, they are vulnerable to Brute force attack. the key independent from the letter being transferred, the same key used for Encryption & decryption. A better solution is to create a mapping b/w each plaintext character & corrosponding cyphertext character.

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

the size of key space for monoalphabetic substitution cipher is 26, The only statical attack is possible.

NOTE :- The Monoalphabatic cipher do not change the frequency of characters in the ciphertext which make the ciphers vulnerable to statical attack.

(b) Polyalphabatic cipher :- In polyalphabatic Substitution each occurrence of a character may have a different Substitution.

The relationship b/w the character in Plaintext & the character in ciphertext is one-to many

for example 'a' could be enciphered as 'D' in the Biginning of the text but as 'N' at the middle.

It has a advantage of hiding a letter frequency.

In this cipher our key is streams of key for each character in plaintext.

In other word we need key $K = \{K_1, K_2, K_3 \ldots\}$ in which K_i used to Encipher the i^{th} character in the plaintext to create the i^{th} character in the Ciphertext.

Types of Polyalphabatic cipher :-

① Autokey cipher :- In this cipher a key is stream of a subkeys, in which each subkey is used to encrypt the corresponding character in the plaintext.

In this cipher the key used is :-
first key is predetermind key at which the sender & receive agreed.
& the second key is first character of the plaintext
the third key is second character of the plaintext.
and so on.

Example :- $c = (p + k) \bmod 26$ $p = (c - k) \bmod 26$

Plaintext :-	a	t	t	a	c	k	i	s	t	o	d	a	y		
p's value :-	00	19	19	0	2	10	8	18	19	14	3	0	24		
Key stream :-	12	0	19	19	0	2	10	8	18	19	14	3	0		
c's value :-	12	19	12	19	2	12	18	0	11	7	17	3	24		
ciphertext :-	M	T	M	T	C	M	S	A	L	H	R	D	Y		

It is addative cypher

Crytanalysis :- It is still vulnerable ~~to~~ because of addative cipher. ~~The~~ This Hides a character.
But the key space (1 to 25) → for first letter. which is very small, so It also vulnerable.

We needed ~~the~~ such algorithm which hides the character. as well as the key Domain is Big.

#2. **Playfair Cipher** :- It is another example of Polyalphabetic cipher. It is used By the british army during world war I.

The Secret key in this cipher is made of 25 alphabet letters arranged in a 5x5 matrix.

letter I & J considered same when encrypting.

Different arrengment of letters in the matrix can create many different keys.

Secret key =

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

Condition

Before encryption, If the two letter in a pair are the same, a bogus letter is inserted Between them to seprate them.

After inserting bogus letters, If the number of Characters in the Plaintext is odd. one extra bogus character is added at the end to make the number of character even.

following Steps for Encryption of Plaintext using Playfair cipher. (After appling above "condition"

Step1 :- A plaintext is devided in pairs of Character.

After deviding the Plaintext to pairs then following 3 Rules are used for encryption :-

Rule1 :- If the two letter in a pair are in the same row of secret key, then the encrypted character for each letter is Next right letter in key

Example :-

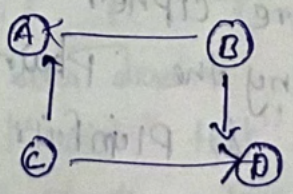
Plainitext = QH	Plaintext = EC
Ciphertext = ME	Ciphertext = CQ.

Rule2 :- If the two letter in a pair are in same column then the corrosponding ciphertext is the character below that character.

Example :-

Plaintext = UV	Plaintext = BT
Ciphertext = MY	Ciphertext = EB

Rule3 :- If the two letters are Not in same row or column of secret key. then the corroponding ciper text is according to this



for AD the cipher will be CB
& for BC the cipher will be AD

Example :-

In given secret key

Plaintext :- EV	Plaintext = Qf
ciphertext :- MO	ciphertext :- GUC

Q message : Jazz

keyword : monarchy

Soln

1. make 5×5 matrix
2. fill keyword in matrix left to right

m	o	n	a	r
c	h	y		

3. fill rest of cell with unique character and fill i/j in one cell

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. take pair of every 2 character
   if pair characters are same then take one from them and make pair with random character

eg 1. Ja zz → in pair both same, it left alone so make pair with 'X'

Ja zx zx

If we have left one character at end so make pair of that with 'X'

eg 2. GR EE T → In pair both are same

GR Ex ET

eg 3. OFF
↓ ↓
OF FX

Encrytion rule:

1. If both character of pair are in same row then cypher is imidate right in that row of each character
2. If both character of pair are in same column then cypher is imidate down in that column of each character

3. If both character of pair are not in same row or same column then form quadirateral
Now problem arrise which corner point we write first
So in pair firstly see first character and see corner point in that row
the see second character and see corner point in that row

eg:. Ja zz
↓ I I
Ja ZX ZX

cypher: Sb uz uz

OFF
↓ ↓
OF FX

hp iv

Decryption Rule

1. If both character of pair are in same row then cypher is imidate left in that row of each character
2. If both character of pair are in same column then cypher is imidate upper in that column each character

3. If both character of pair are not in same row or same column then form quadirateral

Now problem arrise which corner point we write first

So in pair firstly see first character and see corner point in that row

the see second character and see corner point in that row

eg:- Sb uz uz
↓ ↓ ↓
Sb uz uz

Text:- Ja zx zx → If two pair are same and 2nd character in both are x then remove that x from that

so:- Jazz

eg:- hp iv
↓ ↓
hp iv

Text:- OF FX → if last character are X then remove that

so:- OFF

#3 Vigenere Cipher :- This cipher uses a different strategy to create the key stream.

The key stream is made up of repitation of initial secret key of length 'm'.

where $1 \leq m \leq 26$

initial key $= (K_1, K_2, K_3 \ldots K_m)$

Plaintext length $= n$

actual key $= [(K_1, K_2 \ldots K_m)\ (K_1, K_2, \ldots K_1) \ldots\ldots (K_1, K_2, \ldots K_n)]$

↓ the last key varies according to the remaining character.

One Important difference b/w the vigenere cipher & other two poly-alphabetic ciphers, In this the key is created without knowing the Plaintext.

In the vigenere cipher the key is created But in Autokey & Playfair the plaintext is used for generating key.

Example :- Encrypt the message "She is listening" using 6 character key word (PASCAL). the initial key is (15, 0, 18, 2, 0, 11)

Plaintext :-	S	h	e	i	s		i	s	t	e	n	i	n	g
P's values :-	18	7	4	8	18	11	8	18	14	4	13	8	13	6
key stream :-	15	0	18	2	0	11	15	0	18	2	0	11	15	0
c's value :-	7	7	22	10	18	22	23	18	11	6	13	19	2	6

* This cipher can be seen as combination of 'm' addative ciphers.

or

We can say addative cipher is a special case of vigenere ~~ciper~~ cipher.

where $m = 1$

Cryptanalysis of vigenere ciphers :-

The cryptanalysis here consists of two parts :

1. finding the length of the key
2. finding key itself.

(1) Several methods have been devised to find the length of key. One method is "Kasiski test". this Method is usefull in finding the length of the key.

(2) After the length of the key has been found, the cryptanlysis devide the ciphertext into m different pieces & applies the method used to cryptanalysis the addative cipher.

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 :

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

eg :- plain text :- weare discoveredsaveyourself

Key :- deceptive

Soln :-

plain text :- weare discoveredsaveyourself

Key :- deceptivedeceptivedeceptivedeceptive

Encrytion

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

Decryption

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

AutoKey System

1. The periodic nature of the keyword can be eliminated by using a non-repeating keyword that is as long as message itself
2. Vigenere proposed autokey system in which a keyword is concatenated with the plaintext itself to provide a running key.

eg :- Plain text :- wearediscoveredsaveyourself
Key :- deceptive

Sol^n

Plain text :- wearediscoveredsaveyourself
Key :- deceptivewearediscoverdsav

Encryption

Key	3	4	2	4	15	19	8	21	4	22	4	0	17	
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	
CT	25	8	2	21	19	22	16	13	6	10	25	4	8	

Decryption

Key	3	4	2	4	15	19	8	21	4	22	4	0	17	
CT	25	8	2	21	19	22	16	13	6	10	25	4	8	
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	

#4. **Hill cipher** :- It is different from the other ciphers we read Previously.

All the cipher we read is a type of Stream ciphers But this cipher is a Block cipher. In which the ~~the~~ Plaintext is devided into a equal size blocks.

The Block is encrypted one at a time in such a way that each character in a Blocks ~~cotto~~ contributes to the encryption of other characters in the blocks.

The key in this cipher is a square matrix of mxm in which 'm' is the size of the block. If we call the key matrix 'K'

then

$$K = \begin{bmatrix} K_{11} & K_{12} & \cdots & K_{1m} \\ K_{21} & K_{22} & \cdots & K_{2m} \\ K_{31} & K_{23} & \cdots & K_{3m} \\ \vdots & \vdots & \vdots & \vdots \\ K_{m1} & K_{m2} & \cdots & K_{mm} \end{bmatrix}$$

Encryption using Hill cipher :-

If we say m characters in the Plaintext Block $P_1, P_2, \ldots P_m$

the corresponding character in the ciphertext block are

$C_1, C_2, \ldots C_m$

then

$$C_1 = P_1K_{11} + P_2K_{21} + \cdots P_mK_{m1}$$
$$C_2 = P_1K_{12} + P_2K_{22} + \cdots P_mK_{m2}$$
$$\vdots$$
$$C_m = P_1K_{1m} + P_2K_{2m} \cdots P_mK_{mm}.$$

This shows that each character in block of cipher C_K depends on the all the character of corrosponding Block.

we should have to select key very carefully Because Not all the matrix in Z_{26} have inverse.

> NOTE :- In Hill cipher the key must have multiplicative inverse

Example :- Using Hill cipher encrept the plaintext "code is ready" & also decrept it.

The plaintext can be made 3x4 matrix after adding one bogus character 'z' to last Block.

$$P = \begin{bmatrix} c & o & d & e \\ i & s & r & e \\ a & d & y & z \end{bmatrix} = \begin{bmatrix} 2 & 14 & 3 & 4 \\ 8 & 18 & 17 & 4 \\ 0 & 3 & 24 & 25 \end{bmatrix}$$

Let's take

$$key = \begin{bmatrix} 9 & 7 & 11 & 13 \\ 4 & 7 & 5 & 6 \\ 2 & 21 & 14 & 9 \\ 3 & 23 & 21 & 8 \end{bmatrix}$$

then

$$C = P \times K$$

$$C = \begin{bmatrix} 2 & 14 & 3 & 4 \\ 8 & 18 & 17 & 4 \\ 0 & 3 & 24 & 25 \end{bmatrix} \begin{bmatrix} 9 & 7 & 11 & 13 \\ 4 & 7 & 5 & 6 \\ 2 & 21 & 14 & 9 \\ 3 & 23 & 21 & 8 \end{bmatrix}$$

$$C = \begin{bmatrix} 14 & 7 & 10 & 13 \\ 8 & 7 & 6 & 11 \\ 11 & 8 & 18 & 18 \end{bmatrix}$$

$(2\times9 + 14\times4 + 3\times2 + 4\times3) \bmod 26$

Decription.

$$key^{-1} = \begin{bmatrix} 2 & 15 & 22 & 3 \\ 15 & 0 & 19 & 3 \\ 9 & 9 & 3 & 11 \\ 17 & 0 & 4 & 7 \end{bmatrix}$$

$$P = \begin{bmatrix} 14 & 7 & 10 & 13 \\ 8 & 7 & 6 & 11 \\ 11 & 8 & 18 & 18 \end{bmatrix} \begin{bmatrix} 2 & 15 & 22 & 3 \\ 15 & 0 & 19 & 3 \\ 9 & 9 & 3 & 11 \\ 17 & 0 & 4 & 7 \end{bmatrix}$$

$P =$

$$P = \begin{bmatrix} 2 & 14 & 3 & 4 \\ 8 & 18 & 17 & 4 \\ 0 & 3 & 24 & 25 \end{bmatrix}$$

Cryptanalysis of Hill ciphers :-

The key domain of Hill cipher is very huge.
At first glance it looks that it has $26^{k \times k}$ different keys But the ~~multip~~ inverse of every matrix is Not exist. But also it is very huge.

So :- ① Brute forse Attack is very difficult
② Statical Attack is Not possible.

But known Plaintext attack is Possible.

Hill cypher

plain text :- shortexample

Key :- hill

Soln :-

1. Make Key matrix

h	i
l	l

2x2

7	8
11	11

2x2

2. Make plain text matrix

if Key matrix is 2x2 so plain text matrix is 2x1

4x4 4x1

3x3 3x1

Note :- If we have one character to fill when making plain text matrix then use random character there to fill that 'x'

$$\begin{bmatrix} s \\ h \end{bmatrix}\begin{bmatrix} o \\ r \end{bmatrix}\begin{bmatrix} t \\ e \end{bmatrix}\begin{bmatrix} x \\ a \end{bmatrix}\begin{bmatrix} m \\ p \end{bmatrix}\begin{bmatrix} l \\ e \end{bmatrix}$$

$$\begin{bmatrix} 18 \\ 7 \end{bmatrix}\begin{bmatrix} 14 \\ 17 \end{bmatrix}\begin{bmatrix} 19 \\ 4 \end{bmatrix}\begin{bmatrix} 23 \\ 0 \end{bmatrix}\begin{bmatrix} 12 \\ 15 \end{bmatrix}\begin{bmatrix} 11 \\ 4 \end{bmatrix}$$

$C = KP \bmod 26$

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}\begin{bmatrix} 18 \\ 7 \end{bmatrix} \Rightarrow \begin{bmatrix} 182 \\ 275 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} A \\ P \end{bmatrix}$$

$275/26 \Rightarrow 10.5769$

$10.5769 - 10 \Rightarrow 0.5769$

$0.5769 \times 26 \Rightarrow 15$

$$\begin{bmatrix} A \\ P \end{bmatrix}\begin{bmatrix} A \\ D \end{bmatrix}\begin{bmatrix} J \\ T \end{bmatrix}\begin{bmatrix} F \\ T \end{bmatrix}\begin{bmatrix} W \\ L \end{bmatrix}\begin{bmatrix} F \\ J \end{bmatrix}$$

Ciphertext :- APADJTFTWLFJ

Decryption

Ciphertext :- APADJTFTWLFJ

Key :- hill

1. Make Key matrix

h	i
l	l

2×2

7	8
11	11

2×2

2. Make cypher text matrix

if Key matrix is 2×2 so cypher text matrix is 2×1

4×4 4×1

3×3 3×1

Note:- If we have one character to fill when making plain text matrix then use random character there to fill that 'x'

$$\begin{bmatrix} A \\ P \end{bmatrix} \begin{bmatrix} A \\ D \end{bmatrix} \begin{bmatrix} J \\ T \end{bmatrix} \begin{bmatrix} F \\ T \end{bmatrix} \begin{bmatrix} W \\ L \end{bmatrix} \begin{bmatrix} F \\ J \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 15 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} \begin{bmatrix} 9 \\ 19 \end{bmatrix} \begin{bmatrix} S \\ 19 \end{bmatrix} \begin{bmatrix} 22 \\ 11 \end{bmatrix} \begin{bmatrix} S \\ 9 \end{bmatrix}$$

$$P = CK^{-1} \bmod 26$$

$$K^{-1} = \frac{\text{Adj}\cdot K}{\text{Det}(K)}$$

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

$$7(11) - 8(11)$$
$$77 - 88$$
$$-11$$

$$Adj(A) = \begin{bmatrix} + & - \\ - & + \end{bmatrix} \Rightarrow \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix}$$

$$\frac{1}{-11}\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	24
	1	0		-7	24	

$$-7 \bmod 26$$
$$19$$

$$-19\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} \Rightarrow \begin{bmatrix} -209 & 152 \\ 209 & -133 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 25 & 22 \\ 1 & 22 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 15 \end{bmatrix}\begin{bmatrix} 0 \\ 3 \end{bmatrix}\begin{bmatrix} 9 \\ 19 \end{bmatrix}\begin{bmatrix} 5 \\ 19 \end{bmatrix}\begin{bmatrix} 22 \\ 11 \end{bmatrix}\begin{bmatrix} 5 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 22 \end{bmatrix}\begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} 330 \\ 345 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}$$

similarly

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

$$7(11) - 8(11)$$
$$77 - 88$$
$$-11$$

$$Adj(A) = \begin{bmatrix} + & - \\ - & + \end{bmatrix} \Rightarrow \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix}$$

$$\frac{1}{-11}\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	24
	1	0		-7	24	

$$-7 \bmod 26$$
$$19$$

$$-19\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} \Rightarrow \begin{bmatrix} -209 & 152 \\ 209 & -133 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 25 & 22 \\ 1 & 22 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 15 \end{bmatrix}\begin{bmatrix} 0 \\ 3 \end{bmatrix}\begin{bmatrix} 9 \\ 19 \end{bmatrix}\begin{bmatrix} 5 \\ 19 \end{bmatrix}\begin{bmatrix} 22 \\ 11 \end{bmatrix}\begin{bmatrix} 5 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 22 \end{bmatrix}\begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} 330 \\ 345 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}$$

similarly

$$\begin{bmatrix}18\\7\end{bmatrix}\begin{bmatrix}14\\17\end{bmatrix}\begin{bmatrix}19\\4\end{bmatrix}\begin{bmatrix}23\\0\end{bmatrix}\begin{bmatrix}12\\15\end{bmatrix}\begin{bmatrix}11\\4\end{bmatrix}$$

$$\begin{bmatrix}s\\h\end{bmatrix}\begin{bmatrix}o\\r\end{bmatrix}\begin{bmatrix}t\\e\end{bmatrix}\begin{bmatrix}x\\a\end{bmatrix}\begin{bmatrix}m\\p\end{bmatrix}\begin{bmatrix}l\\e\end{bmatrix}$$

Decrypted text:- Shortexample

#5. One time Pad :—

one of the goal of cryptography is Perfect Secracy. A Study By Shannon has Shown that

Perfect Secracy is can be achieved if each Plaintext symbol is encrypted with a key randomely chosen from a key domain.

for example in key domain (0, 1, 2 --- 25)
if the first character is encrypted using 4 second by 2, third 21 & soon means each character is encrypted rendomly.

Using ~~thing~~ this all types of attack become faild.

This Idea used in cipher is called "one-time-Pad". In this cipher the key length is same as Plaintext.

This is Perfect cipher But Hard to impliment commercialy. Because every time we have to create a new key.

One time pad (vernam cipher)

plain text :- H E L L O
7 4 11 11 14

Key :- b a x y c → its length equals to plain text length
1 0 23 24 2

Add :- 8 4 34 35 16 → mod 26

8 4 8 9 16

Cyphertext :- i e i j q

Decryption :-

Cyphertex :- i e i j q
8 4 8 9 16

Key :- b a x y c
1 0 23 24 2

Sub :- 7 4 -15 -15 14 mod 26

plaintext :- 7 4 11 11 14
H E L L O

Note :- In this method we use one key for one encryption next time we use diff key And length of key is as same as plain text

#5 Rotor cipher :- Although one-time pad cipher are not Practical, one step toward more secured ciper is rotor cipher.

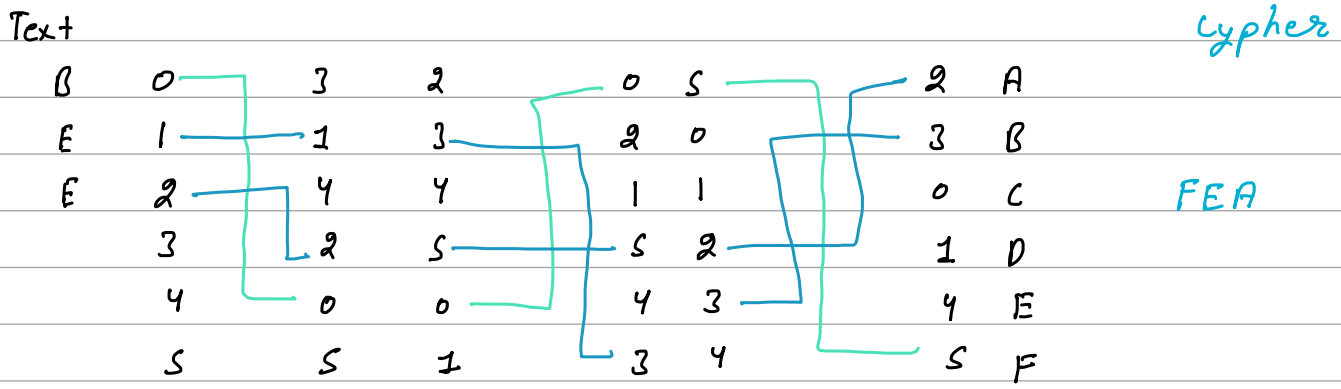
It uses the idea behind the monoalphabetic substitution cipher But change the mapping b/w the plaintext and the ciphertext characters.

After Encryption of Every character the rotors are rotated so that each character in the plain text is mapped to different character in cipher text.

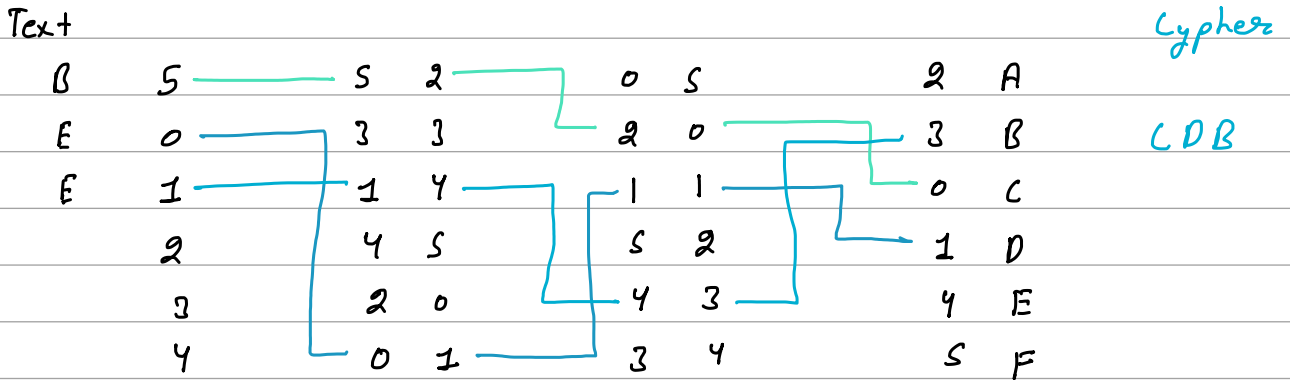
So for this, It is a type of Polyalphabetic cipher.

It prevent all types of attack.

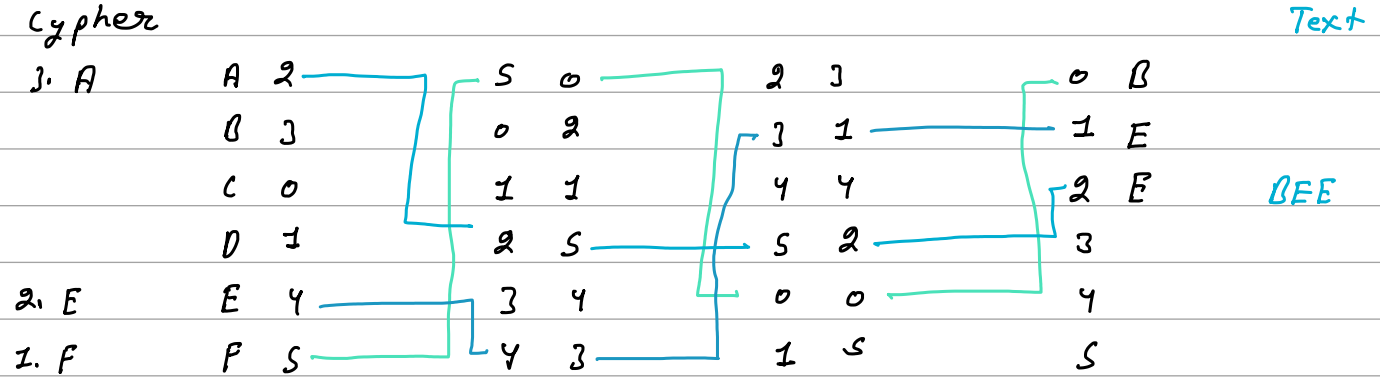
Rotor cipher



Now if we rotate our first rotor



Cypher to plain text (Decryption)



Enigma machine :- It is used in world war 2 By German army.

The component of this machine :-

(1) A Keyboard with 26 keys used for Entering a Plaintext when encrypting and for Entering the ciphertext when decrypting.

(2) A lampboard with 26 lamps that show ciphertext in encrypting & Plaintext in decrypting. (used for Display that which character is typed)

(3) A Plugboard with 26 plugs manually connected By 13 wires, this configuration changed every day to provide different scrambling.

(4) Three wired rotors :- These 3 rotor are choosen daily out of five available rotors.
→ fast
→ medium
→ slow

(5) A reflector :- It is Prewired which relects each character with different character.

(6) Code Book :- This code book Provides settings for every day.

Like :-
① The 3 rotor to be choosen outo of 5 available one.
② order of rotors
③ Settings for Plug board.
④ A three letter code of the day.

Transposition Cipher :-

The transposition cipher does not substitute one symbol for another, instead it changes the location of the symbol.

A symbol in first position in plaintext may appears tenth position of cipher.

A symbol in eight position in plaintext may appears first position in the cipher.

"In other words the transposition cipher reorders the symbols."

Two varients of transposition cipher:-

1. Keyless
2. Keyed.

(1) Keyless Transposition Cipher :-

In past the simple keyless transposition cipher are used, ~~there are of~~ ~~2 type~~

There are 2 method for reordering the character.

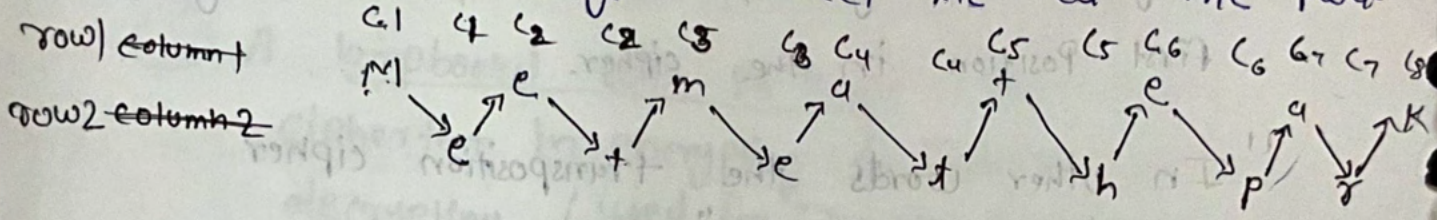
In first method the plaintext is written into a table column by column & then read row by row

In second method the text is written into a table row by row & then transmitted column by column.

Example :- A good Example of keyless transposition cipher using first Method is "rail fence cipher".

In this cipher the plaintext is arrenged column By column in zig-zag pattern. The ciphertext is created By reading row-By-row.

Example :- Encrypt "Meet me at the park"



Ciphertext ⇒ read row-By-row

Mematreaketethpr

Example 2 :- (Second Method) Use Same plaintext "Meet me at the park"

arreng this plaintext in row's & read column By column

	c_1	c_2	c_3	c_4
r_1	M	e	e	t
r_2	m	e	a	t
r_3	h	e	p	
r_4	a	r	K	

ciphertext

MmtaeehreaeKttp

2# Keyed Transposition Ciphers:-

In keyless the ciphers permute the character By using writing a plaintext in one way (row-By-row or column By-column) and reading in another way (column-By-column or row-By-row)

In this the permutation is done on the whole Plaintext to create whole cipher text.

"Another Method is to divide the plaintext into groups of Predetermined size, called blocks. & use a key to Permute the characters in each block separately".

Example :- Encrypt the plaintext :- "enemy attacks tonight".

Deride the plaintext in Block of 5 character

e n e m y
a t t a c
k s t o n
i g h t z

this place is empty so we added a bogus character which is Not Present in the text

Now the key used is

3	1	4	5	2
1	2	3	4	5

Encryption ↓ ↑ Decryption

Cipher text

E E M Y N
T A A C T
T K O N C
H I T Z Y.

the message is EEMYNTAACTTKONCHITZY

the receiver again devide the message in Blocks & decrypt each block seperatly.

Combined Approch :- This approch combined the idea of keyless & keyed transposition cipher.

This is Done is three Steps :-

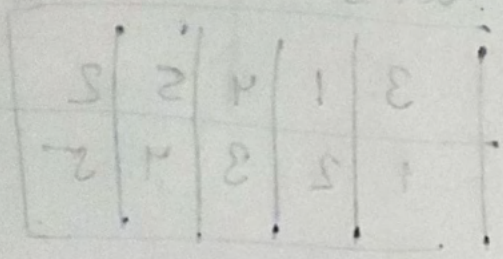
In first step the plaintext is written row By-row ~~to be~~ according to block size &

In second step we use key to reorder the Plaintext.

&In the third step we recad this plaintext column By column.

Example :- we are using privious Example with same key

~~Pla~~ ~~Plaintext~~



Plaintext:- "enemy attacks tonight"

e n e m y
a t t a c
k s t o n
i y h t z

3 1 4 5 2
1 2 3 4 5

E E M Y N
T A A C T
T K O N S
H I T Z G

ETTHEAKIMAOTYCNZNTSG

Decryption key creation using Encryption key:-

given Encryption key =

2	6	3	1	4	7	5
1	2	3	4	5	6	7

key
index

Swap(key, index)

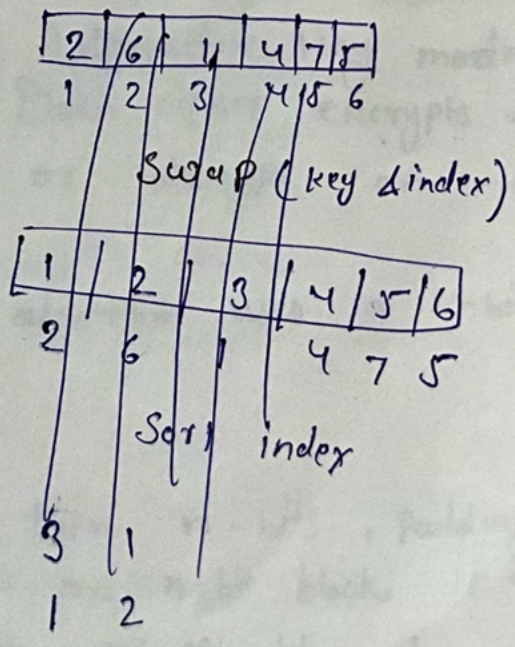
1	2	3	4	5	6	7
2	6	3	1	4	7	5

key
index

Sort (index with key)

4	1	3	5	7	2	6
1	2	3	4	5	6	7

→ Decryption key.



Keyed transposition cipher

Message :- enemyattackstonight

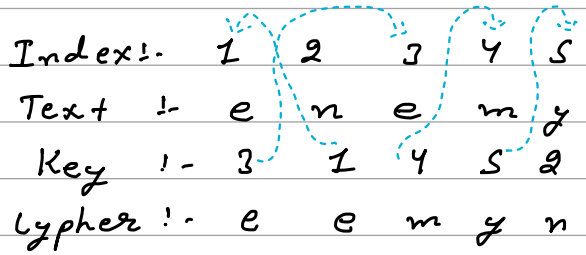
Key :- 31452

Encryption :-

Step 1 :- Make a matrix of plaintext with column size is key size

Index :-	1	2	3	4	5
Key	3	1	4	5	2
Text :-	e	n	e	m	y
	a	t	t	a	c
	K	s	t	o	n
	i	g	h	t	x → this space is filled with random character

Block 1 :-



Note :- firstly we see Key then we go to that index then we fill text of that index below the key that's how our cypher is generated

Similarly

Block 2 :- t a a c t
Block 3 :- t K o n s
Block 4 :- h i t x g

cipher :-

e	e	m	y	n
t	a	a	c	t
t	k	o	n	s
h	i	t	x	g

cipher :- eemyntaactttkonshitxg

Decryption :-

Decryption Key :-

Key :	3	1	4	5	2
Index :	1	2	3	4	5

Swap

Key :	1	2	3	4	5
Index :	3	1	4	5	2

Sort w.r.t Index :-

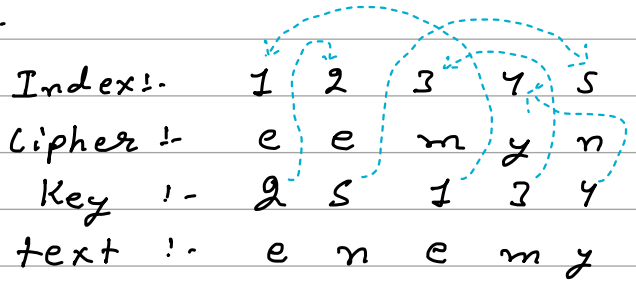
Key :	2	5	1	3	4
Index :	1	2	3	4	5

So our Decryption key is :- 2 5 1 3 4

Step 1 :- Make a matrix of cipher with column size is key size

Index :-	1	2	3	4	5
Key :-	2	5	1	3	4
cipher :-	e	e	m	y	n
	t	a	a	c	t
	t	k	o	n	s
	h	i	t	x	g

Block 1 :-



Index :-	1	2	3	4	5
Cipher :-	e	e	m	y	n
Key :-	2	5	1	3	4
text :-	e	n	e	m	y

Note :- firstly we see Key then we go to that index then we fill text of that index below the key that's how our cypher is generated

similarly :-

Block 1 :	e	n	e	m	y
Block 2 :	a	t	t	a	c
Block 3 :	k	s	t	o	n
Block 4 :	i	g	h	t	x

text :

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	x

plain text :- enemy attacks tonight

Key Matrix :- The key is also represented as a Matrix.

In this Matrix Every row & column has exactly one 1 & rest are 0's

The Decryption key is inverse of Encryption key. this can be achieved By simply transposing the Encryption key.

Example

Key

3	1	4	5	2

Plaintext

$$\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 0 & 19 & 19 & 0 & 2 \\ 10 & 18 & 19 & 14 & 13 \\ 8 & 6 & 7 & 19 & 25 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 4 & 12 & 24 & 13 \\ 19 & 0 & 0 & 2 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 7 & 8 & 19 & 25 & 6 \end{bmatrix}$$

ciphertext

Decryption Key :- 2 5 1 3 4

2	5	1	3	4

cipher

$$\begin{bmatrix} 4 & 4 & 12 & 24 & 13 \\ 19 & 0 & 0 & 2 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 7 & 8 & 19 & 25 & 6 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 13 & 04 & 12 & 24 \\ 0 & 19 & 19 & 0 & 2 \\ 10 & 18 & 19 & 14 & 13 \\ 8 & 6 & 7 & 19 & 25 \end{bmatrix}$$

Text