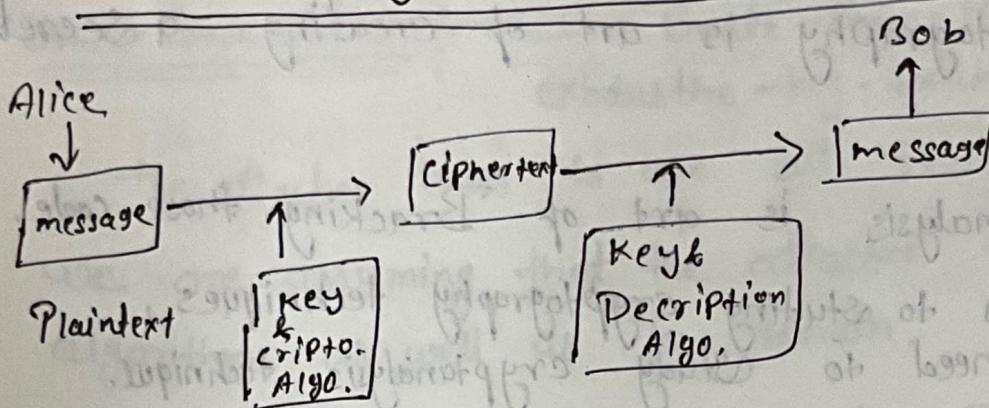


Chapter 3

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 guessing the key is too difficult so No need to hide the encryption & decryption Algorithm.

Cryptanalysis :-

2 part

The cryptography is art of creating a secret code.

&

The cryptanalysis is art of Bracking those code.

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

This helps us to check the vulnerability 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 cyperntext for Attack.

Various Methods are used to implement 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 until the Plaintext make sense.

This Attack 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 Statistical Attack! — The Attacker can use the inherent characteristics of the Plaintext to launch Statistical Attack.

for Example the letter 'E' is most-frequently used in English text. The Attacker finds the most frequent character in the text & Replace 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 characteristic of the language.

③ Pattern Attack! — Some Algorithm may hide the characteristic of the language, but may create some pattern in the cypher. A Attacker may use this pattern to find a key.

So we have to use those algorithm which creates a randomness in the text.

④ #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 / ciphertext pair & use this pair to ~~Break~~ 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 Ciphers.

① Substitution Cipher — In this cipher we replace one character of Plaintext with another character.

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

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

This cipher is further categorised in

(a) Monoalphabetic cipher

(b) Polyalphabetic cipher

④ Monoalphabetic 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 b/w Plaintext & cyphertext is one to one.

Example :- 'hello' \Rightarrow 'KHOOR' (It is monolithic)
 'hello' \Rightarrow '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 Alphabetic 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 ~~Alice~~ and ~~Bob~~ Sender and Receiver
 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 additive cipher the Plaintext, ciphertext, Key are integers in \mathbb{Z}_{26} .

Example :-

Encryption

$$\begin{array}{c}
 h \ e \ l \ l \ o \\
 \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
 07 \ 04 \ 11 \ 11 \ 14 \\
 \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
 7+15 \ 4+15 \ 11+15 \ 11+15 \ 14+15 \\
 \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
 22 \ 19 \ 0 \ 0 \ 3 \\
 \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
 w \ T \ A \ A \ D
 \end{array}
 \quad \boxed{\text{Key} = 15}$$

Decryption

$$\begin{array}{c}
 w \ i \ t \ : \ A \ : \ A \ : \ D \\
 \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
 22-15 \ 19-15 \ 0-15 \ 0-15 \ 3-15 \\
 \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
 7 \ 4 \ 11 \ 11 \ 14
 \end{array}$$

• Encryption algorithm interpreted as "Shift key character down".

and Decryption algorithm interpreted as "Shift key character up".

Julius Caesar used a Additive cipher to communicate with his officers. For this additive cipher is also called Caesar cipher.

The key used in this is '3'.

Cryptanalysis of Additive cipher :- Additive cipher is vulnerable to

"Ciphertext only Attack" using "Brute-force attacks".
the key domain of additive cipher is very small.

Example :- Attacker has - ~~UVACLYFZLT BYZ~~ UVACLYFZLT BYZ

the attacker try to use

Key corresponding Plaintext

1 fuzbkxeykianK

2 styajwodxjhzwi

3 osxzivewig yvi

4 qswyghubvhfxuh

5 Pqrxgtaugenty

6 opuwfszffdlvsf

7 notverysecure.

the Plaintext with Key 7 make some sense.

#(ii) Multiplicative cipher :-

Here Encryption means multiplication of Plaintext

By a key

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

The operations are in \mathbb{Z}_{26} ,

for multiplicative inverse the key must belongs to

$$\mathbb{Z}_{26}^*$$

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

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

Example 1 → key Domain of multiplicative cipher.

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

we have plaintext "hello" & key = 7.

Encryption	h	$\rightarrow (7 \times 7) \mod 26 \rightarrow 23 \rightarrow x$
	e	$\rightarrow (1 \times 7) \mod 26 \rightarrow 02 \rightarrow c$
	l	$\rightarrow (11 \times 7) \mod 26 \rightarrow 25 \rightarrow z$
	l	$\rightarrow (4 \times 7) \mod 26 \rightarrow 25 \rightarrow z$
	o	$\rightarrow (14 \times 7) \mod 26 \rightarrow 20 \rightarrow u$
Decryption with multiplicative inverse of 7 $\Rightarrow 15$	x	$\rightarrow (23 \times 15) \mod 26 \rightarrow 7 \rightarrow h$
	c	$\rightarrow (2 \times 15) \mod 26 \rightarrow 4 \rightarrow e$
	z	$\rightarrow (25 \times 15) \mod 26 \rightarrow 11 \rightarrow l$
	z	$\rightarrow (25 \times 15) \mod 26 \rightarrow 11 \rightarrow l$
	u	$\rightarrow (20 \times 15) \mod 26 \rightarrow 14 \rightarrow o$

(ii) 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.

$$C = (P \times k_1 + k_2) \mod 26$$

$$P = ((C - k_2) \times k_1^{-1}) \mod 26$$

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

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



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

$$\leftarrow T \times K$$

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

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

~~#~~ K_1^{-1} is multiplicative inverse of K_1

~~#~~ $-K_2$ is additive inverse of K_2

~~#~~ 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.

$$h \rightarrow 7$$

$$\text{Encryption } ((7 \times 7 + 2) \bmod 26) \rightarrow 25 \rightarrow z$$

$$e \rightarrow 4$$

$$\text{Encryption } ((4 \times 7 + 2) \bmod 26) \rightarrow 4 \rightarrow e$$

$$l \rightarrow 11$$

$$\text{Encryption } ((11 \times 7 + 2) \bmod 26) \rightarrow 1 \rightarrow b$$

$$l \rightarrow 11$$

$$\text{Encryption } ((11 \times 7 + 2) \bmod 26) \rightarrow 1 \rightarrow b$$

$$o \rightarrow 14$$

$$\text{Encryption } ((14 \times 7 + 2) \bmod 26) \rightarrow 22 \rightarrow w$$

~~Note~~ Now we have to decrypt this message
"ZEBBW"

the additive inverse of 2 is 24
& the multiplicative inverse of 7 is 15.

$$\begin{aligned} Z &\rightarrow \text{Decrypt} \rightarrow ((25-2) \times 15) \bmod 26 \rightarrow 7 \cdot h \\ E &\rightarrow \text{Decrypt} \rightarrow ((4-2) \times 15) \bmod 26 \rightarrow 4 \cdot e \\ B &\rightarrow \text{Decrypt} \rightarrow ((1-2) \times 15) \bmod 26 \rightarrow 4 \cdot f \\ B &\rightarrow \text{Decrypt} \rightarrow ((1-2) \times 15) \bmod 26 \rightarrow 11 \cdot g \\ W &\rightarrow \text{Decrypt} \rightarrow ((22-2) \times 15) \bmod 26 \rightarrow 14 \cdot o \end{aligned}$$

Note → The additive cipher is special case of affine cipher with $k_1=0$

The multiplicative cipher is special case of affine cipher with $k_2=0$

Cryptanalysis of Affine Cipher

so we have to do a lot of calculations to find out the key. So it is not a good idea to use this cipher.

So, we can say that monoalphabetic ciphers are not secure. They are vulnerable to frequency analysis. If we know the frequency of letters in the plaintext, we can easily break the cipher. For example, if we know that 'E' is the most frequent letter in the plaintext, we can assume that it is mapped to 'M' in the ciphertext. This is because 'M' is the most frequent letter in the English language. Similarly, we can assume that 'T' is mapped to 'Z', 'A' to 'B', 'B' to 'C', and so on. This is called a frequency attack.

Monalphabetic Substitution cipher: Because, additive, multiplicative, affine ciphers have small key domains, they are vulnerable to Brute force attack. The key is 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 & corresponding Ciphertext 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	G	Y	L	K	H	V	I	M	P	Z	S	W		

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

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

(b) Polyalphabetic cipher In Polyalphabetic 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 Beginning 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 ~~which~~ for each character in plaintext.

~~We~~ In other word we need key $K = \{K_1, K_2, K_3, \dots\}$ 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 Polyalphabetic 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 pre determined key at which the Sender & receiver agreed.

& the second key is first character of the plaintext
the third key is second character of the plaintext.
and so on.

Example:-

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

Plaintext :- a t t a c k i s t o o d a y

p's value :- 0 19 19 0 2 10 8 18 19 14 3 0 24

Key stream :- 12 0 19 2 10 8 18 19 14 3 0 24

c's value :- 12 19 92 19 2 12 18 0 11 7 R 0 7

Ciphertext :- M T M T C M S A L H R D Y

It is additive cipher

Cryptanalysis! It is still vulnerable to a because of additive cipher. This hides a character.

But the key space (1 to 25) which is very small, so it is also vulnerable.

We needed 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 arrangement of letters in the matrix can create many different keys.

Secret key =

I	C	D	B	A
Q	M	H	G	C
U	R	N	I	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 separate 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 applying above "condition")

Step1 :- A plaintext is divided in pairs of characters.

After dividing the Plaintext to pairs then following 3 Rules are used for encryption?

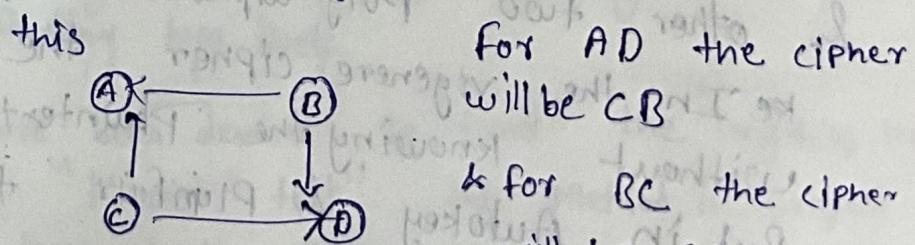
Rule 1 :- If the two letter in a pair are in the same row of secret key, then the encrypted character for each letter is next right letter in key

Example:-
Plaintext = GH | Plaintext = EL
Ciphertext = ME | Ciphertext = CG.

Rule 2 :- If the two letter in a pair are in same column then the corresponding ciphertext is the character below that character.

Example:-
Plaintext = UV | Plaintext = BT
Ciphertext = NY | Ciphertext = BB

Rule 3 :- If the two letters are Not in Same row or column of secret key, then the corresponding cipher text is according to



Example :- In given secret key

Plaintext :- EV | Plaintext = QF
Ciphertext = MO | Ciphertext = QUC

Ø message : Jazz

Keyword : monarchy

Sol^m

1. make 5×5 matrix

2. fill Keyword in matrix left to right

m	o	n	a	r
c	h	z		

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

m	o	n	a	r
c	h	z	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

4. take pair of every 2 character

if pair characters are same then take one from them
and make pair with random character

in pair both same

eg 1. $\overline{J} \overline{a} \quad \overline{z} \overline{z} \rightarrow$ it left alone so make pair with 'x'
 $\downarrow \quad \overline{\overline{J} \overline{I}}$
 $J a \quad z x \quad z x$

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

In pair both are same



eg 2. $\overline{G} \overline{R} \quad \overline{E} \quad \overline{E} \quad T$
 $\downarrow \quad \downarrow \quad \downarrow$
 $G R \quad E X \quad E T$

Eg 3. $\begin{array}{c} OFF \\ \overline{J} \quad \overline{J} \\ OF \quad FX \end{array}$

Encryption rule:

1. If both character of pair are in same row then cypher is immediate right in that row of each character
2. If both character of pair are in same column then cypher is immediate down in that column of each character
3. If both character of pair are not in same row or same column then form quadrilateral
Now problem arise which corner point we write first
So in pair firstly see first character and see corner point in that row
then see second character and see corner point in that row

Eg: $\begin{array}{cc} Ja & zz \\ \overline{J} & \overline{J} \quad \overline{J} \\ Ja & zx \quad zx \end{array}$ $\begin{array}{c} OFF \\ \overline{J} \quad \overline{J} \\ OF \quad FX \end{array}$

Cypher: Sb uz uz hp iv

Decryption Rule

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

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

Now problem arise 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:- $\begin{array}{ccc} S & b & u \\ \downarrow & \downarrow & \downarrow \\ S & b & u \\ u & z & z \end{array}$

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

so:- Ja zz

Eg:- hpi v
 $\begin{array}{cc} \downarrow & \downarrow \\ h & p \\ h & i \\ p & i \\ v & v \end{array}$

Text:- OF FX \rightarrow 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 repetition of initial secret key of length 'm'.
where $1 \leq m \leq 26$

$$\text{initial key} = (k_1, k_2, k_3, \dots, k_m)$$

Plaintext length = n
actual key = $(k_1, k_2, \dots, k_m) (k_1, k_2, \dots, k_m) \dots (k_1, k_2, \dots, k_n)$

↓
the last key varies according to the remaining character.

One important difference b/w the Vigenere cipher

& other two poly-alphabetic ciphers, ~~in this case~~ In the Vigenere cipher the key is created without knowing the Plaintext.

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 value :-	7 7 22 10 18 22	23 18 11 6 13 19	2 6

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

Or

We can say, additive cipher is a special case of Vigenere cipher.

Where $m=1$

Cryptanalysis of Vigenere cipher:-

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 useful in finding the length of the key.

② After the length of the key has been found, the cryptanalysis divide the ciphertext into m different pieces & applies the method used to cryptanalysis the additive 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:

$$p_i = (c_i - k_{i \bmod m}) \bmod 26$$

e.g:- plaintext :- wearediscoveredaveyourself
Key :- deceptive

Soln :-

plaintext :- wearediscoveredaveyourself
Key :- deceptive *deceptive* *deceptive* *deceptive* *deceptive*

Encryption

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.

e.g:- Plain text :- wearediscoveredsaveyourself
Key :- deceptive

Solⁿ

Plain text :- wearediscoveredsaveyourself
Key :- deceptivewearediscoveredsav

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 divided into equal size blocks.

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

The key in this cipher is a square matrix of $m \times m$ in which 'm' is the size of the block.

If we call the key matrix 'K' then

$$K = \begin{bmatrix} K_{11} & K_{12} & \cdots & K_{1m} \\ K_{21} & K_{22} & \cdots & K_{2m} \\ K_{31} & K_{32} & \cdots & K_{3m} \\ \vdots & \vdots & \ddots & \vdots \\ K_{m1} & K_{m2} & \cdots & K_{mm} \end{bmatrix}$$

Encryption using Hill cipher

If we say m characters in the plaintext Block P_1, P_2, \dots, P_m

the corresponding character in the ciphertext block are

$$C_1, C_2, \dots, C_m$$

then

$$C_1 = P_1 K_{11} + P_2 K_{21} + \dots + P_m K_{m1}$$

$$C_2 = P_1 K_{12} + P_2 K_{22} + \dots + P_m K_{m2}$$

:

$$C_m = P_1 K_{1m} + P_2 K_{2m} + \dots + P_m K_{mm}$$

$$C_m = P_1 K_{1m} + P_2 K_{2m} + \dots + P_m K_{mm}$$

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

We should have to select key very carefully because ^{Not} all the matrix in Z_{26} ~~do~~ have inverse.

NOTE !— In Hill cipher the key must have multiplicative inverse

Example !— Using Hill cipher encrypt the plaintext "Code is ready" & also decrypt it.

The ~~#~~ plaintext can be made 3×4 matrix after adding one bogus character "Z" to last block.

$$\textcircled{O} P = \begin{bmatrix} C & O & D & E \\ I & S & R & E \\ A & D & Y & Z \end{bmatrix} = \begin{bmatrix} 2 & 14 & 3 & 4 \\ 8 & 18 & 17 & 4 \\ 0 & 3 & 24 & 25 \end{bmatrix}$$

Let's take

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

then

$$C = P \times K$$

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

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

$(2 \times 9 + 14 \times 4 + 3 \times 2 + 4 \times 3) \mod 26$

Description.

$$\text{key} = \begin{bmatrix} 2 & 15 & 22 & 3 \\ 15 & 0 & 19 & 3 \\ 9 & 9 & 3 & 0 \\ 17 & 10 & 4 & 7 \end{bmatrix}$$

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

$$P =$$

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

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 ~~will~~ inverse of every matrix is not exist. But also it is very huge.

So:- ① Brute force Attack is very difficult

② Statical Attack is Not possible.

But Known Plaintext attack is Possible.

Hill cipher

plain text :- short example

key :- hill

Sol:-

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

4x1

3x3

4x1

3x1

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

$\begin{bmatrix} 8 \\ h \end{bmatrix} \begin{bmatrix} 0 \\ r \end{bmatrix} \begin{bmatrix} t \\ e \end{bmatrix} \begin{bmatrix} x \\ a \end{bmatrix} \begin{bmatrix} m \\ p \end{bmatrix} \begin{bmatrix} l \\ e \end{bmatrix}$

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

$$C = KP \bmod 26$$

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

$$275 / 26 \Rightarrow 10 \cdot 5769$$

$$10 \cdot 5769 - 10 \Rightarrow 0 \cdot 5769$$

$$0 \cdot 5769 \times 26 \Rightarrow 15$$

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

Ciphertext :- APADJTFWLFT

Decryption

Ciphertext :- APADJTFWLFB
Key :- hill

1. Make key matrix

h	i
l	l

7	8
11	11

2. Make cipher text matrix

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

4×1

3×3

4×1

3×1

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

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

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

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

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

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

$$\begin{aligned} 7(11) - 8(11) \\ 77 - 88 \\ -11 \end{aligned}$$

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

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

$$\begin{array}{ccccccccc} 2 & x_1 & x_2 & x_3 & x_1 & x_2 & x \\ 2 & 26 & 11 & 4 & 0 & 1 & -2 \\ 2 & 11 & 4 & 3 & 1 & -2 & 5 \\ 1 & 4 & 3 & 1 & -2 & 5 & -7 \\ 3 & 3 & 1 & 0 & 5 & -7 & 24 \\ 1 & 0 & & & -7 & 24 & \end{array}$$

$$-7 \bmod 26$$

$$19$$

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

$$\Rightarrow \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

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

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} 330 \\ 245 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}$$

similarly

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

$$\begin{aligned} 7(11) - 8(11) \\ 77 - 88 \\ -11 \end{aligned}$$

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

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

$$\begin{array}{ccccccccc} 2 & x_1 & x_2 & x_3 & x_1 & x_2 & x \\ 2 & 26 & 11 & 4 & 0 & 1 & -2 \\ 2 & 11 & 4 & 3 & 1 & -2 & 5 \\ 1 & 4 & 3 & 1 & -2 & 5 & -7 \\ 3 & 3 & 1 & 0 & 5 & -7 & 24 \\ 1 & 0 & & & -7 & 24 & \end{array}$$

$$-7 \bmod 26$$

$$19$$

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

$$\Rightarrow \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

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

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} 330 \\ 245 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}$$

similarly

$$\begin{bmatrix} 18 \\ 7 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \begin{bmatrix} 19 \\ 4 \end{bmatrix} \begin{bmatrix} 23 \\ 0 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix}$$
$$\begin{bmatrix} 8 \\ h \end{bmatrix} \begin{bmatrix} 0 \\ r \end{bmatrix} \begin{bmatrix} t \\ e \end{bmatrix} \begin{bmatrix} x \\ a \end{bmatrix} \begin{bmatrix} m \\ p \end{bmatrix} \begin{bmatrix} l \\ e \end{bmatrix}$$

Decrypted text:- short example

#5. One time Pad :-

one of the goal of cryptography is Perfect Secrecy. A Study By Shannon has shown that

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

for example in key domain $(0, 1, 2, \dots, 25)$ if the first character is encrypted using 4 second by 2, third is 21 & so on means each character is encrypted randomly.

Using this all types of attack become failed.

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 Implement commercially. 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
1 0 23 24 2 length

Add :- 8 4 34 35 16 → mod 26

8 4 8 9 16

Cyphertext :- i e i j g

Decryption :-

Cyphertext :- i e i j g
8 4 8 9 16

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

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

plain text :- 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 ciphers are not practical, one step toward more secured cipher 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.

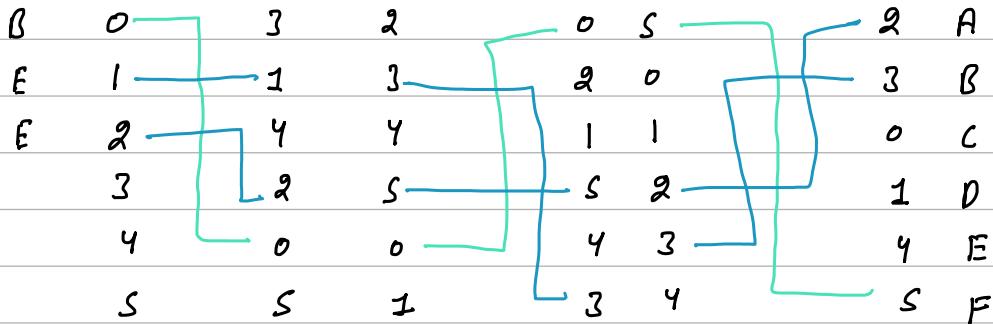
So for this, It is a type of Polyalphabetic cipher.

It prevent all types of attack.

Rotor cipher

Text

Cypher



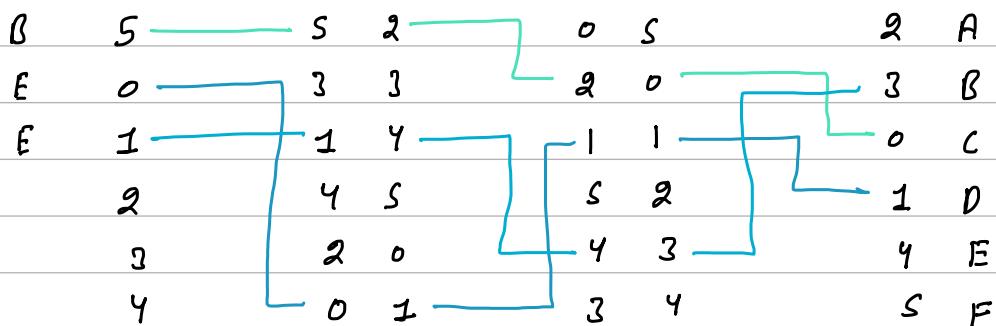
FEA

Fast Rotor Medium Rotor Slow Rotor

Now if we rotate our first rotor

Text

Cypher



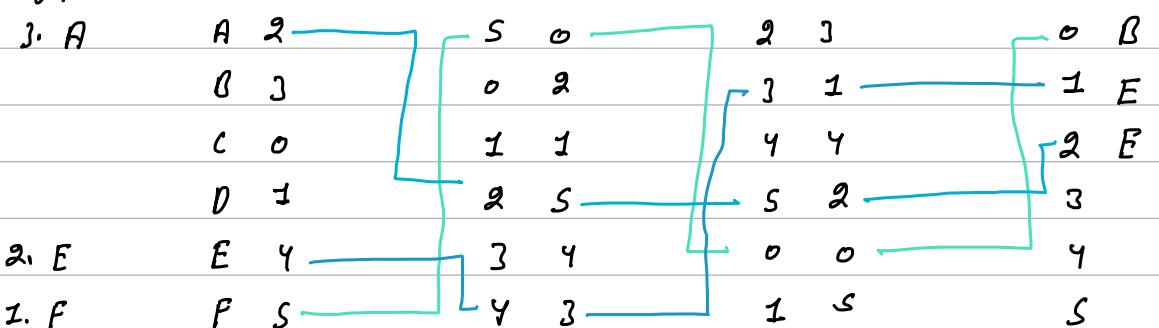
CDB

Fast Rotor Medium Rotor Slow Rotor

Cypher to plain text (Decryption)

Cypher

Text



BEE

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 with 13 wires, this configuration changed every day to provide different scrambling.

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

⑤ A reflector :- It is prewired for each character which reflects with different

⑥ Code Book :- This code book provides settings for every day.

Like:-

① The 3 rotors to be chosen out of 5 available one.

② Order of rotors

③ Settings for plugboard.

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 appear tenth Position of cipher.

A symbol in eight Position in Plaintext may appear first Position in the cipher.

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

Two variants 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
character.

In first method the
table column by column

for reordering the

Plaintext is written into a
& then read row by row

In Second Method the
table row by row &
By column.

text is written into a
& then transmitted column

Example 1 → A good example of keyless transposition cipher using first Method is

"rail fence cipher".

In this cipher the plaintext is arranged in column by column in zig-zag pattern.

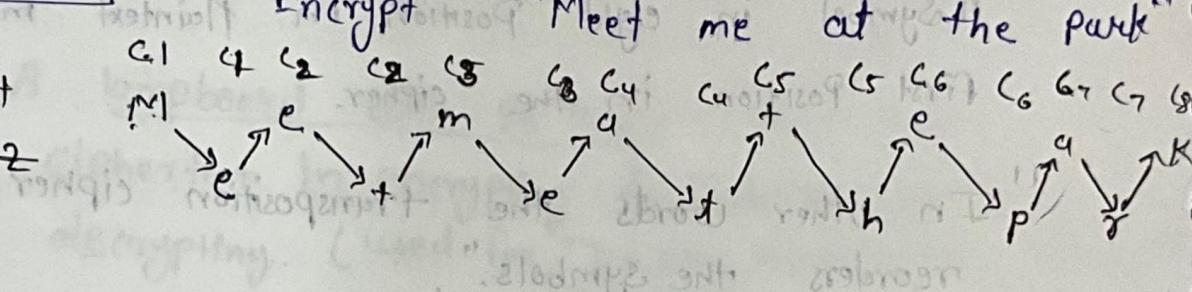
The ciphertext is created by reading row-by-row.

Example 1 →

Encrypting "Meet me at the park"

row1 column1

row2 column2



Ciphertext ⇒ read row-by-row

MemateaketethPr

Example 2 → (Second Method) Use Same plaintext

"Meet me at ^{the} park"

arranging this plaintext in row's & read column by column

	C ₁	C ₂	C ₃	C ₄	C ₅	C ₆	C ₇	C ₈
R ₁	M	e	e	t				
R ₂	m	e	a	t	h			
R ₃	#	b	e	p				
R ₄	a	r	K					

ciphertext

MintaeehreakeKtP

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".

Divide the plaintext in Block of 5 character

e n e m i

a t t a c

k s + o n

i g h + (Z)

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

Now the key used is

Encryption



3	1	4	5	2
1	2	3	4	5

Decryption



Ciphertext

E E M Y N
T A A C T

T K O N C

H I T Z Y

the message is

EE M Y N T A A C T T K O N C H I T Z Y

the receiver again divide the message in blocks & decrypt each block separately.

Combined Approach! — This approach combined the idea of keyless & keyed transposition cipher.

This is Done in three steps!

In first step the plaintext is written row by row according to block size &

In second step we use key to reorder the plaintext.

In the third step we read this plaintext column by column.

Example! — we are using previous Example with same key

~~Plaintext~~

S	Z	P	I	E
R	M	B	S	T

Plaintext:- "enemy attacks tonight"

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

Step 1: [2 6 3 1 4 7 5]

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

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)

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

Swap(key, index)

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

Sort 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 :- enemyattacktonight

Key :- 31452

Encryption :-

Step 1:- Make a matrix of plain text 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	8	t	o	n
	:	g	h	+	x → this space is filled with random character

Block 1 :-

Index :-	1	2	3	4	5
Text :-	e	n	e	m	y
Key :-	3	1	4	5	2
Cypher :-	e	e	m	y	n

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 + x g

cipher :- e e m z n
t a a c t
t k o n s
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

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 1 - 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 z 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	s	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 cipher 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 attackstonight

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

The 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

Plaintext	<u>key</u>	ciphertext
$\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 0 & 19 & 19 & 0 & 2 \\ 10 & 18 & 19 & 14 & 13 \\ 8 & 6 & 7 & 19 & 25 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 & 1 & 4 & 5 & 2 \end{bmatrix}$	$\begin{bmatrix} 4 & 4 & 12 & 24 & 13 \\ 19 & 0 & 0 & 2 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 7 & 8 & 19 & 25 & 6 \end{bmatrix}$

Decryption Key : - 2 5 1 3 4

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