Chapter 2 (cryptography)

Mathematics of cryptography

Modular Arithmetic, Congruence and Matrices

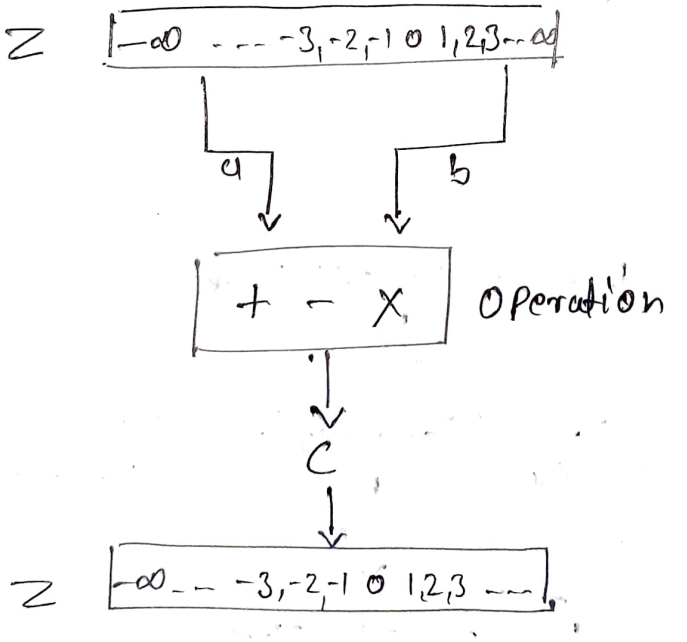
Integer Arithmetic :-

(1) Binary Operations :-

~~The~~ In cryptography there are 8 Binary operations.

they are :-

→ Addition
→ Substraction
→ Multiplication



Integer Division :-

If we devide 'a' by 'n' then we get two integer 'q' and 'r'

the relationship B/w these four integer is

$$a = q \times n + r$$

- a → Dividend
- n → Divisor
- q → Quotient
- r → remainder

The four Number can be anything But In cryptography we impose 2 restrictions :-

1. $n > 0$
2. $r \geq 0$

$-\infty \ldots -3, -2, -1, 0, 1, 2, 3 \ldots \infty$

$\downarrow q$

n (positive) $\longrightarrow a = q \times n + r \longrightarrow r$ (non negative)

$\downarrow q$

$-\infty, -3, -2, -1, 0, 1, 2, 3 \ldots \infty$

Divisibility :-

case1 :- If 'a' is Divisible By 'n' then we write it as

$n \mid a$

case2 :- If 'a' is Not Divisible By 'n' the we write it as

$a \nmid n$

Example :-

for case1 $13 \mid 78$, $7 \mid 98$, $-6 \mid 24$ $4 \mid 44$

for case2 :- ~~$13 \mid 27$~~ $13 + 27$, $7 \nmid 50$ $-6 \nmid 23$

Properties of Divisiblity :-

Property 1 :- If $a \mid 1$, then $a = \pm 1$

Property 2 :- If $a \mid b$, and $b \mid a$ then $a = \pm b$

Property 3 :- If $a \mid b$ and $b \mid c$ then $a \mid c$

Property 4 :- If $a \mid b$ and $a \mid c$ then

$a \mid (mxb + nxc)$

where m & n are arbitary integer.

Property 3 example

$3 \mid 15$ & $15 \mid 45$ then $3 \mid 45$

Property 4 example :-

$3 \mid 15$ & $3 \mid 9$ then

$3 \mid (15 \times 2 + 9 \times 4)$ which means $\boxed{3 \mid 66}$

All ~~Post~~ Divisor :- A positive integer can have more then one divisor.

Example :- 32 has :- 1, 2, 4, 16, 32 as Divisor

facts about Divisor of Positive integer :-

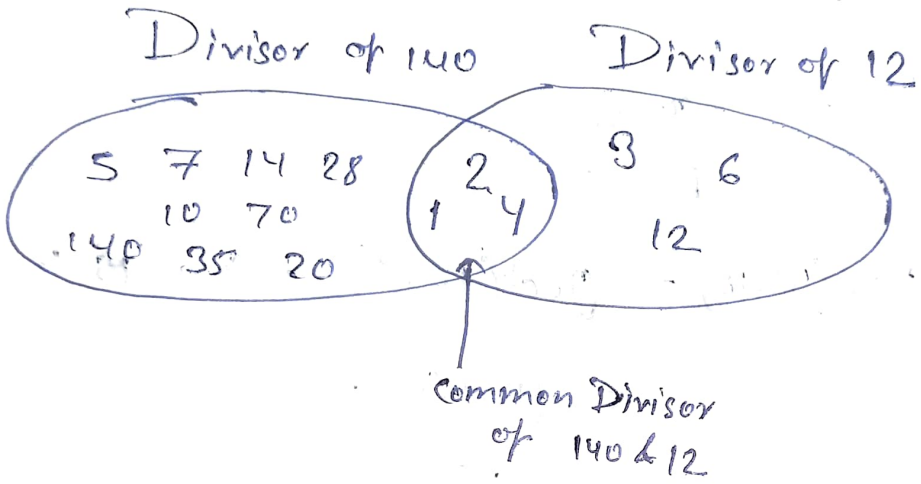
fact 1 :- The integer 1 has only one divisor Itself.

fact 2 :- Any Positive integer has atleast 2 divisor, 1 and itself.

Greatest Common Divisor :- One Integer often needed in cryptography is the "Greatest Common Divisor"

Two Positive integer may have many comman divisors, But only one Greatest common Divisor.

Example :- GCD of 140 & 12



Euclidean Algorithm :- finding the GCD of 2 Positive integer by listing all common divisor is not Practical. when two integer are too large.

The Mathematician named Euclid developed an algorithm for finding the GCD of 2 integers.

The "Euclidean Algorithm" Based on the 2 facts

fact 1 :- $\boxed{gcd(a,0) = a}$

fact 2 :- $\boxed{gcd(a,b) = gcd(b,r)}$ where r is remainder of dividing a by b.

fact1 :- If the second integer is 0, the gcd is first Number.

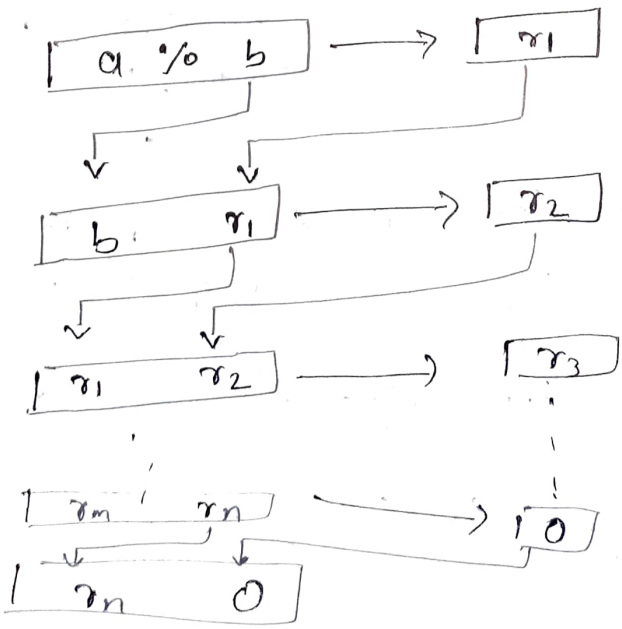
fact2 :- The second fact allow us to change the value of 'a' & 'b' undill 'b' becomes '0'. then we can use the fact 1

Example :- a = 36
b = 10

$$gcd(36,10) = gcd(10,6) = gcd(6,4) = gcd(4,2)$$
$$= gcd(2,0)$$

So our final $gcd(36,10) = 2$

#



r_n is our gcd.

Algorithm :-

```
r1 ← a , r2 ← b , r3
while (r2 != 0)
{
    r3 = r1 % r2;
    r1 = r2
    r2 = r3
}
```

Note :- when GCD is 1 then we can say a & b are **relatively prime**.

Example GCD of (25, 60)

→ a = 25 , b = 60 , r = 25
→ a = 60 , b = 25 , r = 10
→ a = 25 , b = 10 , r = 5
→ a = 10 , b = 5 , r = 0
⇒ **a = 5 , b = 0**

Extended Euclidean Algorithm :-

Given two integer a & b we often need to find other two integers 's & t' such that

$$s \times a + t \times b = gcd(a, b)$$

This Algorithm is same as Euclidean Algorithm we are using 3 sets of variables r's s's & t's

(1) in r's set we have :-

r_1 r_2 & r

all have same value as in Euclidean Algorithm.

(2) in s's set we have :-

$s_1 = 1$ $s_2 = 0$ s

(3) in t's set we have :-

$t_1 = 0$ $t_2 = 1$ t

Algorithm for this :-

$r_1 \leftarrow a$, $r_2 \leftarrow b$

$s_1 \leftarrow 1$, $s_2 \leftarrow 0$

$t_1 \leftarrow 0$, $t_2 \leftarrow 1$

while ($r_2 != 0$)

{

$r = r_1 - q \times r_2$

$r_1 = r_2$

$r_2 = r$

$t = t_1 - q \times t_2$

$t_1 = t_2$

$t_2 = t$

$s = s_1 - q \times s_2$

$s_1 = s_2$

$s_2 = s$

}

$gcd(a,b) \leftarrow r_1$, $s \leftarrow s_1$, $t \leftarrow t_1$

Example :-

$a = 161$, $b = 28$ find $\gcd(a,b)$ & value of s & t.

$$r = r_1 - q \times r_2 \qquad s = s_1 - q \times s_2$$

$$t = t_1 - q \times t_2$$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

GCD = 7 | $s = -1$ | $t = 6$

then

$$161 \times (-1) + 28 \times 6 = 7$$

Example2 :- $a = 17$, $b = 0$, $s_1 = 1, s_2 = 0$, $t_1 = 0, t_2 = 1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

$\gcd(17,0) = 17$ | $s = 1$, | $t = 0$

~~17x0~~

$17 \times 1 + 0 \times 0 = 17$.

Example3 $a = 0$, $b = 45$, $s_1 = 1$, $s_2 = 0$, $t_1 = 0$, $t_2 = 1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		1	0	

gcd = 45 , s = 0 , t = 1

$0 \times 0 + 45 \times 1 = 45$

Linear Diophantine Equations :-

This is the application of "Extended Euclidean algorithm".

we have to find the solution of this equation using the previous algorithm.

the equation is of type $ax + by = c$

we need to find the value of x & y that satisfy the equation.

If $d = \gcd(a, b)$

→ If $d \nmid c$ (c is Not divisible By d) then the equation have ~~infinite~~ no solution

→ If $d \mid c$ (c is divisible By d) then the equation have infinite solution.

In the infinite Number of Solution one is 'Particular' & the rest, are 'general'.

linear Diophantine equation of two variable :-

$ax+by+c$

Particular Solution :-

If $d|c$ then Particular Solution can be found using these steps :-

Step1 :- Reduce the equation By devided Both Side of equation By 'd',
This is possible because 'd' divides a, b, c By assumption.

Step2 :- Solve for 's' & 't' in relation.
$a_1 s + b_1 t = 1$ using Extended Equlidean Algorithm.

Step3 :- Particular Solution founded By

$x_0 = \left(\frac{c}{d}\right) \times s$ | $y_0 = \left(\frac{c}{d}\right) t$

General Solution :-

After finding Particular Solution the general Solution can be found :-

$$x = x_0 + K\left(\frac{b}{d}\right) \qquad y = y_0 - K\left(\frac{a}{d}\right)$$

where K is an integer

Example :- Find the particular and general solutions to the equation.

$$21x + 14y = 35$$

Solution $\quad GCD(21, 14) = 7 = d$

Since $7 \mid 35$ So the equation have Infinite number of solution.

~~So Step1~~ So first we are going to find Particular Solution :-

Step 1 our New equation after deviding Both side By $d = 7$

$$3x + 2y = 5$$

General Solution :-

After finding Particular Solution the general solution can be found :-

$$x = x_0 + K\left(\frac{b}{d}\right) \qquad y = y_0 - K\left(\frac{a}{d}\right)$$

where K is an integer

Example :- Find the particular and general solutions to the equation.

$$21x + 14y = 35$$

Solution $\boxed{GCD(21, 14) = 7 = d}$

Since $7 \mid 35$ So the equation have Infinite number of solution.

~~So Step!~~ So first we are going to find Particular Solution :-

Step 1 our new equation after deviding Both side By $d = 7$

$$3x + 2y = 5$$

Step 2 :- Using Extended Euclidean Algorithm we find s & t such as

$$3s + 2t = 1$$

Using Extended Euclidean algorithm:-

~~$r_1 = 3$ $r_2 = 2$~~

$r_1 = 3$, $r_2 = 2$, r, $s_1 = 1$, $s_2 = 0$, s, $t_1 = 0$, $t_2 = 1$, t

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	3	2	1	1	0	1	0	1	-1
2	2	1	0	0	1	-2	1	-1	3
	1	0		1	-2		-1	3	

So we get $\boxed{s_0 = 1}$ & $\boxed{t = -1}$

So our Particular solution is:-

$$x_0 = \left(\frac{c}{d}\right)s \Rightarrow \left(\frac{35}{7}\right) \times 1 = 5$$

$$y_0 = \left(\frac{c}{d}\right)t \Rightarrow \left(\frac{35}{7}\right)(-1) = -5$$

$\boxed{x_0 = 5}$ $\boxed{y_0 = -5}$

our particular solution is :-

$$x = x_0 + k\left(\frac{b}{d}\right) \qquad y = y_0 - k\left(\frac{a}{d}\right)$$

$$x = 5 + k(2) \qquad y = -5 - k(3)$$

where k is any integer

i.e. k = ..., -1, 0, 1, 2, 3, ...

So our (x, y) = (5, -5) (7, -8), (9, -11) ...

these solution satisfy the original equation

Modular Arithmetic

In division Relationship ($a = q \times n + r$)

we have 2 inputs a & n

& 2 output q & r

But in modular arithmetic we are interested in only r (remainder)

Modulo Operator :-

a mod n

- a → Integer (z)
- mod → operator
- n → modulus
- r → Residue

Integer (z) → a → mod operator → r (non negative)

r: positive

where k is any integer

and k: 0, 1, 2, 3..

So our (x, y) = (5, -5) (7, -8), (9, -11).

these solution satisfy the original equation

Modular Arithmetic

In division Relationship ($a = q \times n + r$)

we have 2 inputs a & n

& 2 output q & r

But in modular arithmetic we are interested in only r (remainder)

Modulo Operator:-

a mod n

- a → Modulus
- n → Residue
- mod → Modulo operator

Integer (z)

↓ a

mod operator

- r → positive
- r (non negative)

Example :- $27 \bmod 5 = 2$

$36 \bmod 12 = 0$

If a is Negative then we add 'n' Continously until $a \geq 0$ $a < 0$

Example (1)

$-18 \bmod 14$

$\downarrow\downarrow$

~~$-4 \bmod 14$~~

$(-18+14) \bmod 14$

$\downarrow\downarrow$

$-4 \bmod 14$

$\downarrow\downarrow$

$(-4+14) \bmod 14$

$\downarrow\downarrow$

$10 \bmod 14$

$\downarrow\downarrow$

$r = 10$

(2) $-7 \bmod 10$

$\downarrow\downarrow$

$(-7+10) \bmod 10$

$\downarrow\downarrow$

$3 \bmod 10$

$\downarrow\downarrow$

$r = 3$

Set of Residues : Z_n

The result of the modulo operation with modulus n is always an integer between 0 and $n-1$.

Or

we can say that the modulo operation creates a set. In modulo arithmetic this set is referred to as the

> Set of least residues modulo n or Z_n

Example :—

$$Z_2 = \{0, 1\}$$

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

$$Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$Z_n = \{0, 1, 2, 3, 4 \ldots\ldots n-1\}$$

Congruence :- ($\equiv$)

Two integers a & b are congruent modulo m iff they have the same remainder when divided by m.

Denoted By

$a \equiv b \pmod m$

a is congruent to b mod m

Note :-

(1) $a \equiv b \pmod m$ means $a \bmod m = b \bmod m$

(2) $a \equiv b \pmod m$ iff m divides $a-b$

Residue classes :- $[a]$ or $[a]_n$ is a set of integers congruent modulo n.

example :-

$n = 5$

then Residue classes

$[0] = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$

$[1] = \{\ldots -14, -9, -4, 1, 6, 11, 16 \ldots\}$

$[2] = \{\ldots -13, -8, -3, 2, 7, 12, 17 \ldots\}$

$[3] = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}$

$[4] = \{\ldots -11, -6, -1, 4, 9, 14, 19 \ldots\}$

Set of least residue = Z_5 $\{0, 1, 2, 3, 4\} = Z_n$

Modulo arithmetic example in daily life is Clock. (It start from 12 instead of 0)
It is mod 12.

Operation on Z_n :- Binary operations are defined for Z_n

1. addition
2. Substraction
3. Multiplication.

After performing these operation Between 2 numbers, the result will be mapped to Z_n using mod n

$(a+b) \bmod n$
$(a-b) \bmod n$
$(a*b) \bmod n$

Properties :-

1. $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
2. $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
3. $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

These Property are helpful when number is too Big. So the addition & multiplication also become too big.

Inverse :-

In cryprography we mainly focus on 2 types of inverse :-

(1) **Additive Inverse** :- It is related to addition operation.

Two numbers 'a' & 'b' are additive inverse of each other

if $a+b \equiv 0 \bmod n$

Example , n=10

a=4

the additive inverse of 4 is 6

Multiplicative Inverse :-

In Z_n, two number a & b are the multiplicative inverse of each other if.

$$a \times b = 1 \bmod n$$

Note :- 'a' has multiplicative inverse in Z_n if $\gcd(a,n) = 1$, or 'a' & 'n' are relatively Prime.

Example :- The multiplicative inverse of '8' in Z_{10}

There is No number in Z_{10} such that it when it is multiplied to 8 ~~leaves~~ remainder ~~→~~ '1'. & after multiply the modulo 10 become 1.

Note :- The multiplicative inverse of a number exist only when ~~the~~ 'n' & 'a' are relatively prime.

Example :-

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

3 pairs (1,1) (3,7) (9,9) has a multiplicative inverse in Z_n

$(1*1) \bmod 10 = 1$
$(3*7) \bmod 10 = 1$
$(9*9) \bmod 10 = 1$

0, 2, 4, 5, 6, 8 do Not have multiplicative inverse.

Finding Multiplicative inverse using Extended Euclidean Algorithm :-

The Extended Euclidean Algorithm finds the multiplicative inverse of 'b' in Z_n

when n & b are given & $\boxed{\gcd(n, b) = 1}$

The multiplicative inverse of 'b' is 't' after it mapped to Z_n. (means after $\boxed{t \bmod n}$ ↓ multiplicative inverse.)

Example (1) find multiplicative inverse of 11 in Z_6

~~r_1 r_2~~

$r_1 = n$, $r_2 = b$, r,
$t_1 = 0$, $t_2 = 1$, t

$\boxed{r = r_1 - q \times r_2}$
$\boxed{t = t_1 - q \times t_2}$

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	26
	1	0		-7	26	

$\gcd = r_1 = 1$

$t_1 = -7 \bmod 26 = 19$

So the multiplicative inverse of
is 19

Example 8 :- Multiplicative inverse of 23 in Z_{100}

$b = 23 \quad n = 100$

$r_1 = 100, \quad r_2 = 23, \quad r$

$t_1 = 0, \quad t_2 = 1, \quad t$

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

gcd = 1 means Multiplicative inverse exist

$t = -13$

$-13 \bmod 100 = 87$ is the multiplicative inverse of 23.

$(87 \times 23) \bmod 100 = (2001) \bmod 100 = 1$

So the multiplicative inverse of is 19

Example 8 :- Multiplicative inverse of 23 in Z_{100}

$b = 23 \quad n = 100$

$r_1 = 100, \quad r_2 = 23, \quad r$

$t_1 = 0, \quad t_2 = 1, \quad t$

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

gcd = 1 means Multiplicative inverse exist

$t = -13$

$-13 \bmod 100 = 87$ is the multiplicative inverse of 23.

$(87 \times 23) \bmod 100 = (2001) \bmod 100 = 1$

Examples :- Multiplicative inverse of 12 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	2
6	12	2	0	1	-2	13
	2	0		-2	13	

$\gcd(12,26) = 2 \neq 1$ so

there is No multiplicative inverse of 12

Addition table for Z_{10}

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

In addition each no. has an inverse.

Multiplication table for Z_{10}

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

But in case of multiplication it is Not Possible

Different set for addition and Multiplication :-

If the operation is addition the Z_n be the set of possible key because each element in Z_n have a inverse.

On other hand when the operation is multiplication the Z_n can not be a set of possible key. Because some of the elements has a inverse.

Because of this we need another set Z_n^* in This set contains all the element of Z_n such that ~~it has~~ each element of Z_n^* has a multiplicative inverse.

Note :- we need Z_n when addative inverse are needed.
we need Z_n^* when multiplicative inverse is needed.

$Z_6 = \{0,1,2,3,4,5\}$, $Z_6^* = \{1,5\}$
$Z_7 = \{0,1,2,3,4,5,6\}$, $Z_7^* = \{1,2,3,4,5,6\}$
$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ $Z_{10}^* = \{1,3,7,9\}$

We have two more set Z_p & Z_p^*

Z_p is same as Z_n - But p is prime number only.
→ It contains 0 → n-1

Z_p^* contain 1 — n-1 In this set all the numers has a calculative as well as Multiplicative inverse.

Example

$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

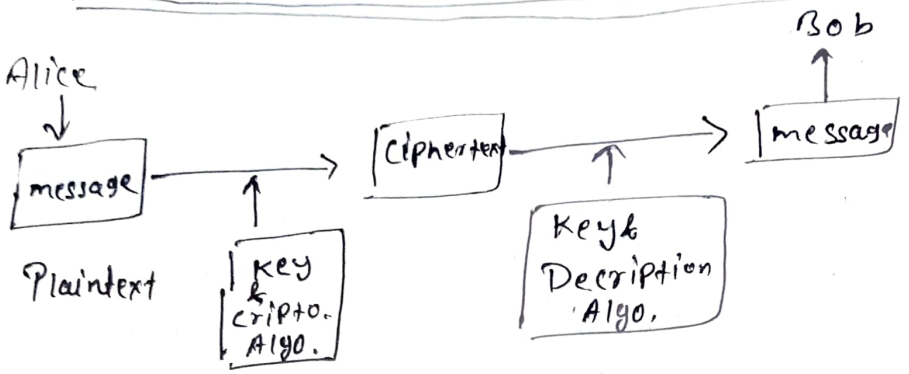
Residue Matrix :- Matrix with all elements are in Z_n.

All operations are same as integer matrix only addition is that all operations ~~is~~ are done in modular arithmetic.

this Matrix has Multiplicative inverse only if $\boxed{\gcd(\det(A), n) = 1}$

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 b/w plaintext & ciphertext is

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 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 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

h	e	l	l	o
↓	↓	↓	↓	↓
07	04	11	11	14
↓	↓	↓	↓	↓
(7+15	4+15	11+15	11+15	14+15) mod 26
↓	↓	↓	↓	↓
22	19	0	0	3
↓	↓	↓	↓	↓
W	T	A	A	D

Key = 15

Decryption :-

W	T	A	A	D
↓	↓	↓	↓	↓
(22-15	19-15	0-15	0-15	3-15) mod 26
↓	↓	↓	↓	↓
7	4	11	11	14

- 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. So for this addative cipher is also called casear cipher.

The key used in this is '3'.

Cryptanlysis 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 "~~HA~~ UVACLYFZL~~J~~ BYL"

the attacker try to use,

Key	corrosponding Plaintext
1	tuzbKXeykiaxK
2	styajwdxjhzwj
3	rsxzivcwjgyvi
4	qrwyhubvhfxuh
5	pqvxgtaugewtg
6	opuwfszftfdvsf
7	notverysecure.

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.

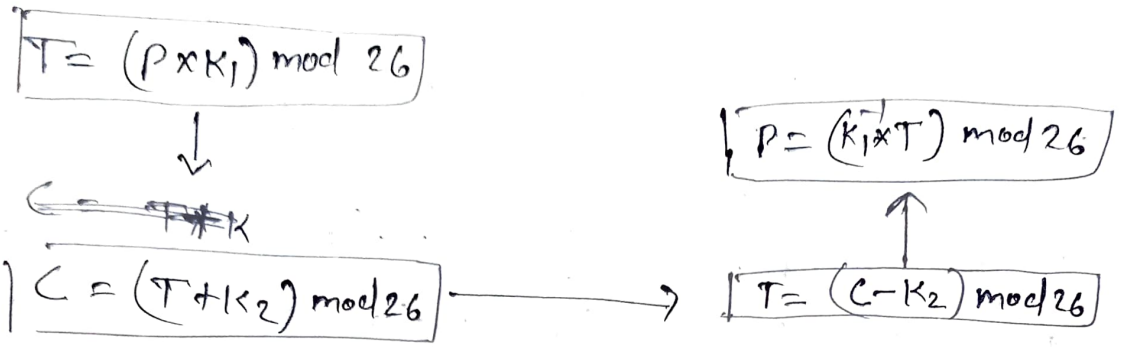
The first key is used with multiplicative cipher & the second key is used with additive cipher.

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.



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 $((7 \times 7 + 2) \bmod 26) \rightarrow 25 \rightarrow z$

e → 4 Encryption $((4 \times 7 + 2) \bmod 26) \rightarrow 4 \rightarrow e$

l → 11 Encryption $((11 \times 7 + 2) \bmod 26) \rightarrow 1 \rightarrow B$

l → 11 Encryption $((11 \times 7) + 2) \bmod 26 \rightarrow 1 \rightarrow B$

o → 14 Encryption $((14 \times 7 + 2) \bmod 26) \rightarrow 22 \rightarrow w$

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

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	Y	L	K	H	V	I	J	M	P	Z	S	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 a 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:-

Plaintext :- a t t a c k i s t o 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~~ o 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 :- In It is another example of Polyalphabudic cipher It is used By the british army during world war I.

The Secret key in this cipher is meade of 25 alphabet letters arranged in a 5X5 matrix.

letter I & J considered same when encrypting.

Different arrengyment 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 addded 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:-

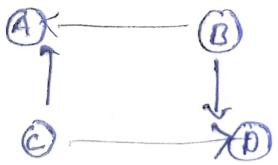
Plainitext = GH	Plaintext = EC
Ciphertext = ME	Ciphertext = CG.

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 or 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 = GF
ciphertext :- MO	Ciphertext :- OUC

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

The key stream is made up of repitition 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 $= [(K_1, K_2 \ldots K_m)\ (K_1, K_2, \ldots K_3) \ldots (K_1, K_2, \ldots K_n)]$

↓

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 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'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' additive ciphers.

or

We can say additive 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 additive cipher.

#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 ~~coffee~~ 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

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

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 :- Unsing 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.

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

$$P = \begin{bmatrix} C \\ 14 & 7 & 10 & 13 \\ 8 & 7 & 6 & 11 \\ 11 & 8 & 18 & 18 \end{bmatrix} \begin{bmatrix} K^{-1} \\ 2 & 15 & 22 & 3 \\ 15 & 0 & 19 & 3 \\ 9 & 9 & 3 & 11 \\ 17 & 0 & 4 & 7 \end{bmatrix}$$

$P =$

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

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 force Attack is very difficult
(2) Statical Attack is Not possible.

But known Plaintext attack is Possible.

#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.

#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 monoalphabatic Substitution cipher But change the mapping b/w the plaintext and the ciphertext characters..

After Encryption of Erery character the roters 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.

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 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

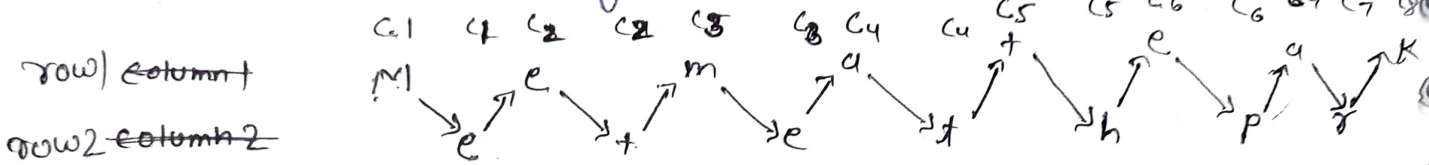
In second Method the ~~text~~ is written into a table row by row & then transmitted column By column.

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

Memateaketethpr

Example 2 :- (Second Method) Use same plaintext "Meet me at the park" arrenge this plaintext By column in row's & read column

	c1	c2	c3	c4
r1	M	e	e	t
r2	m	e	a	t
r3	h	e	p	
r4	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

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

the message is EEMYNTANCTTKONCHITZY

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 Plain text.

& In the third step we read 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

ETTHEAKIMAOTYCNZINTSG

Decryption key creation using Encryption key :-

given Encryption key =

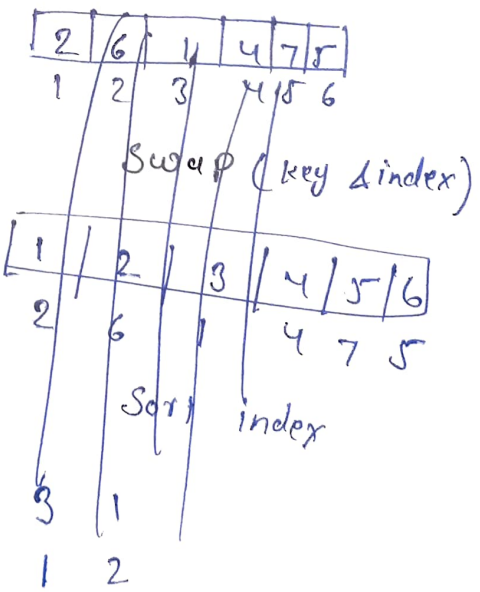
2	6	3	1	4	7	5	key
1	2	3	4	5	6	7	index

Swap(key, index)

1	2	3	4	5	6	7	key
2	6	3	1	4	7	5	index

Sort (index) with key)

4	1	3	5	7	2	6	→ Decryption key
1	2	3	4	5	6	7	



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

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

key

$$\begin{bmatrix} 3 & 1 & 4 & 5 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$=$

ciphertext

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