Transposition Cipher :-

A transposition cipher changes the order of characters in the plaintext. A symbol in the first position of the plaintext may appear in the ~~tenth~~ 10th position of the ciphertext. A symbol in the 8th position may appear in the first position of the ciphertext. That means, a transposition cipher reorders (transposes) the symbols. Transposition cipher is divided into two categories:

```
                 Transposition
                    Cipher
          ┌───────────┴───────────┐
          ↓                       ↓
       Keyless                  Keyed
    Transposition           Transposition
       Cipher                   Cipher
```

1) Keyless Transposition Ciphers

Simple transposition ciphers. It is keyless. There are two methods for permutation of characters.

In the first method, the plaintext is written in a table column by column and then transmitted row by row.

Eg:-

Plain text: Meet Me At Park

The plaintext is arranged in two lines in ~~zig~~ zigzag pattern

```
m ↘   ↗ e ↘   ↗ m ↘   ↗ a ↘   ↗ p ↘   ↗ r ↘
    e       t       e       t       a       k   { ( M e e t m e a t p a r k )
```

~~The~~

The ciphertext is created reading the pattern row by row.

Ciphertext : memapretetak

In the second method, the text is written into the table row by row and then transmitted column by column.

Eg:-

plaintext: Meet Me At park

The plaintext is arranged in row by row.

m e e t
m e a t
p a r k

Then the ciphertext is created reading the pattern column by column.

ciphertext: mmpeeaeartk tk

2) Keyed Transposition Cipher

In this method plaintext is divided into groups of predetermined size called blocks and then use a key to permute the characters in each block seperately.

Eg:-

Plaintext: Enemy Attacks At Night

The key used for encryption and decryption is a permutation key it shows how the characters are permuted. Here plaintext is divided into groups of 5 characters. Adding a bogus character at the end ~~of~~ to make the last character to the same size as the others. For this message assume that the following table as key for encryption and decryption.

Encryption ↓

3	1	4	5	2
1	2	3	4	3

↑ Decryption

Plaintext: Enemy Attack ksatn lghtz

Encryption: 1 2 3 4 5

e n e m y → eemyn
a t t a c → taact
k s a t n → aktns
i q h t z → hitzq

ciphertext: eemyntaactaktnshitzq

3) Combining two Approaches

Here encryption or decryption is done in 3 steps:

① The text is written into a table row by row.
② The permutation is done by reordering the columns.
③ The new table is read column by column.

The first and third steps provide a keyless global reordering; the second step provides a blockwise keyed reordering. These types of ciphers are often referred to as keyed columnar transposition ciphers ~~at~~ or just columnar transposition ciphers.

Eg:

Plaintext: Enemy Attacks at Nightz

Encryption: 1 2 3 4 5

e n e m y ⇐ Written by row by row
a t t a c
k s a t n
i q h t z

Encryption ↓

3	1	4	5	2
1	2	3	4	5

then

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

⇒ Read by column by column

∴ Ciphertext: etaheakimattycnzntsq

Decryption: ~~a~~ ~~2~~ ~~3~~

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

⇐ Written by column by column

1	2	3	4	5
2	5	1	3	4

↑ Decryption

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

⇒ Read ~~by~~ row by row

Plaintext: enemy attacks at night

Streams And Block Ciphers :-

The symmetric Ciphers are divided into two categories, Stream ciphers and Block ciphers. These two methods are used for converting plaintext into ciphertext. Block ciphers convert the plaintext into ciphertext by dropping plaintext's block at a time. While stream ciphers converts the plaintext into ciphertext by taking one symbol at a time.

1) Stream Cipher

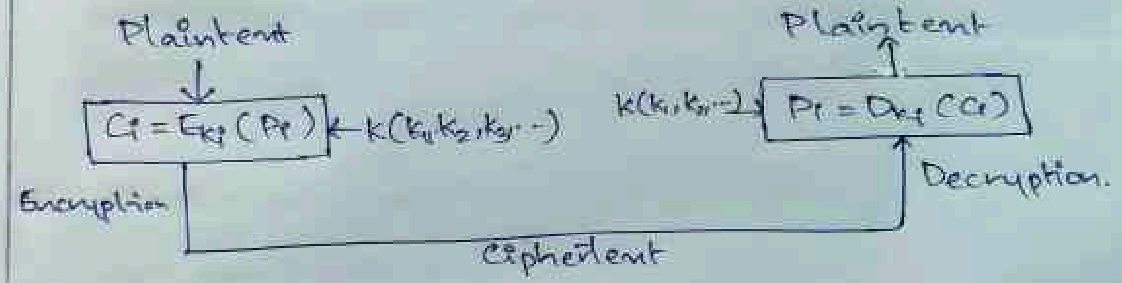
Encryption and decryption are done on one symbol at a time. Here we've a plain text stream P, a ciphertext stream C and a key stream K. General form

$P = P_1P_2P_3 \cdots$ $C = C_1C_2C_3 \cdots$ $k = (k_1, k_2, k_3, \cdots)$

Encryption: $C_i = E_{k_i}(P_i)$ Decryption: $P_i = D_{k_i}(C_i)$

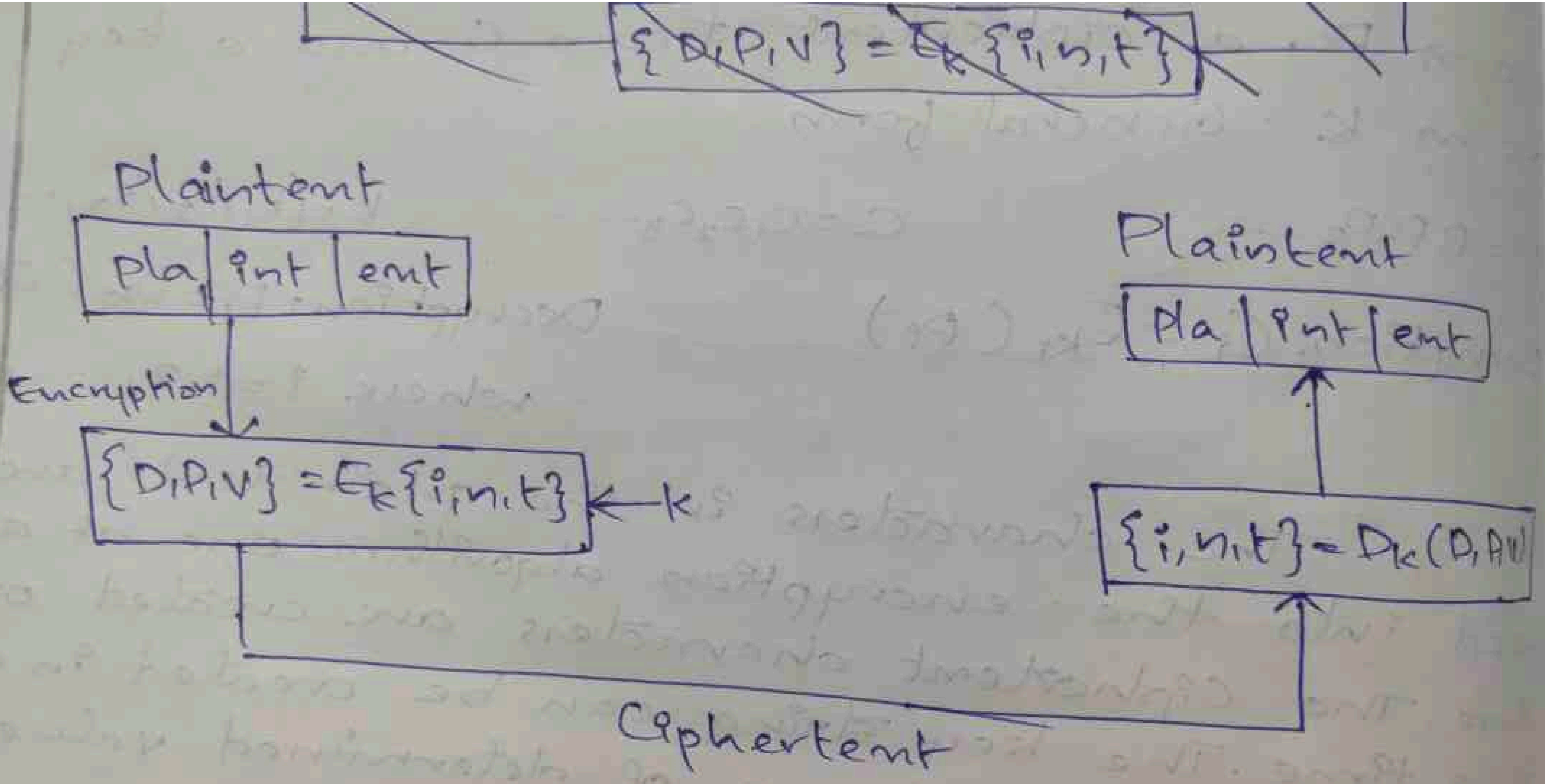
where $i = 1, 2, \cdots$

The characters in the plain text are feed into the encryption algorithm one at a time. The ciphertext characters are created one at a time. The key string can be created in many ways. It may be stream of determined values. It may be one value at a time using an algorithm. The values may depend on the plaintext or ciphertext characters. And may be also depends on the precious key values.



2) Block Cipher

A group of plaintext symbols of size m(m>1) are encrypted together creating a group of ciphertext of same size. In a block cipher a single key is used to encrypt the whole block even if the key is made of multiple values. In a block cipher a ciphertext block depends on the whole plaintext block.


~~{D,P,V} = Ek{i,n,t}~~
Plaintent
pla
int
ent
Encryption
{D,P,V} = Ek{i,n,t}
k
Ciphertent
{i,n,t} = Dk(D,P,V)
Plaintent
Pla
int
ent