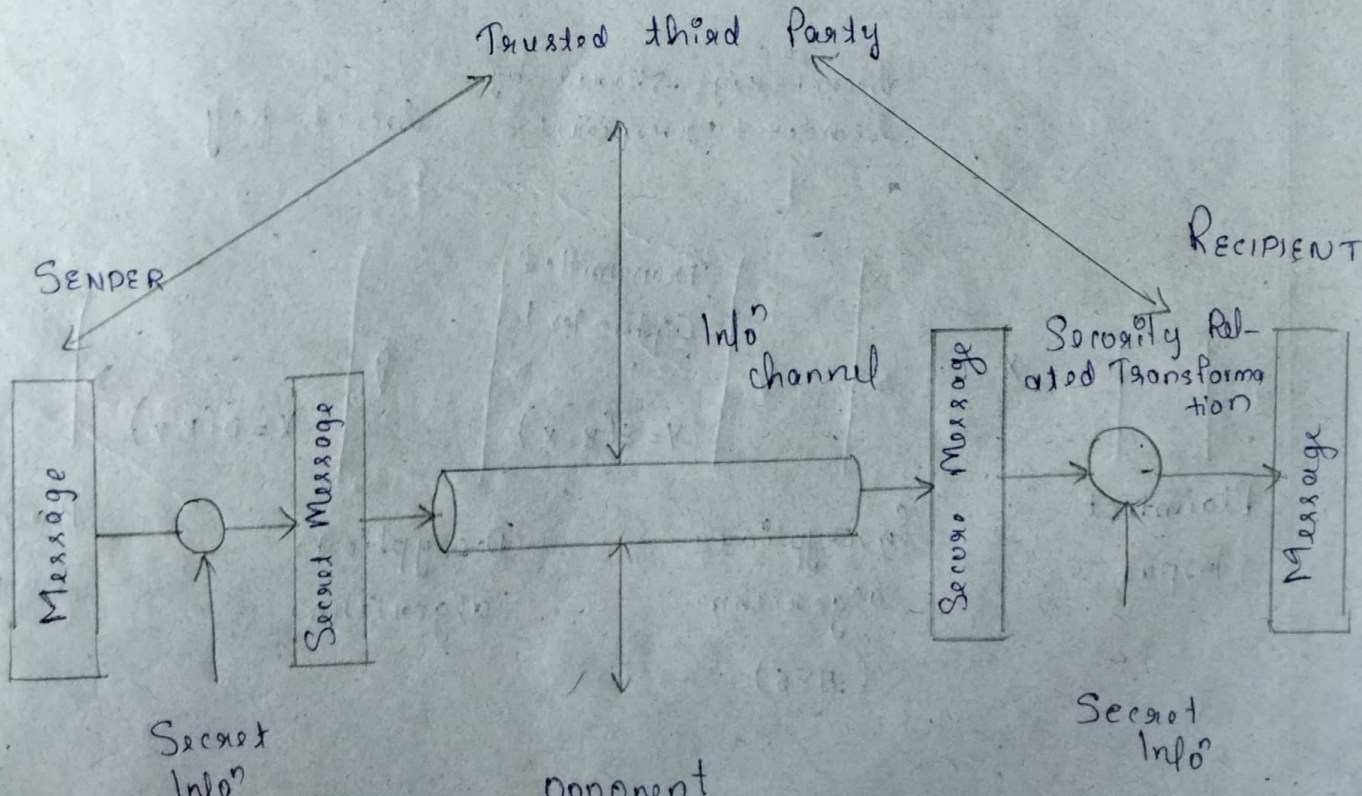
① Smurf attack : a previously exploited Dos attack in which a malicious actor utilizes the broadcast address of vulnerable n/w by sending spoofed packets, resulting in the flooding of a targeted IP address.

② Ping flood : This simple Dos attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings that it is able to respond to efficiently, Dos can occur. This attack can also be used as a DDos attack.

③ Ping of death : Often conflated with a ping flood attack, a ping of death attack involves sending a mal-formed packets to a targeted machine, resulting in deleterious behavior such as s/m crash.

NETWORK SECURITY MODEL



There are four basic tasks in designing a particular Security Services :

① Design an algorithm for performing the security related transformation. The algo. should be such that an opponent cannot defeat its purpose.

② Generate the Secret info^{n} to be used with the algo.

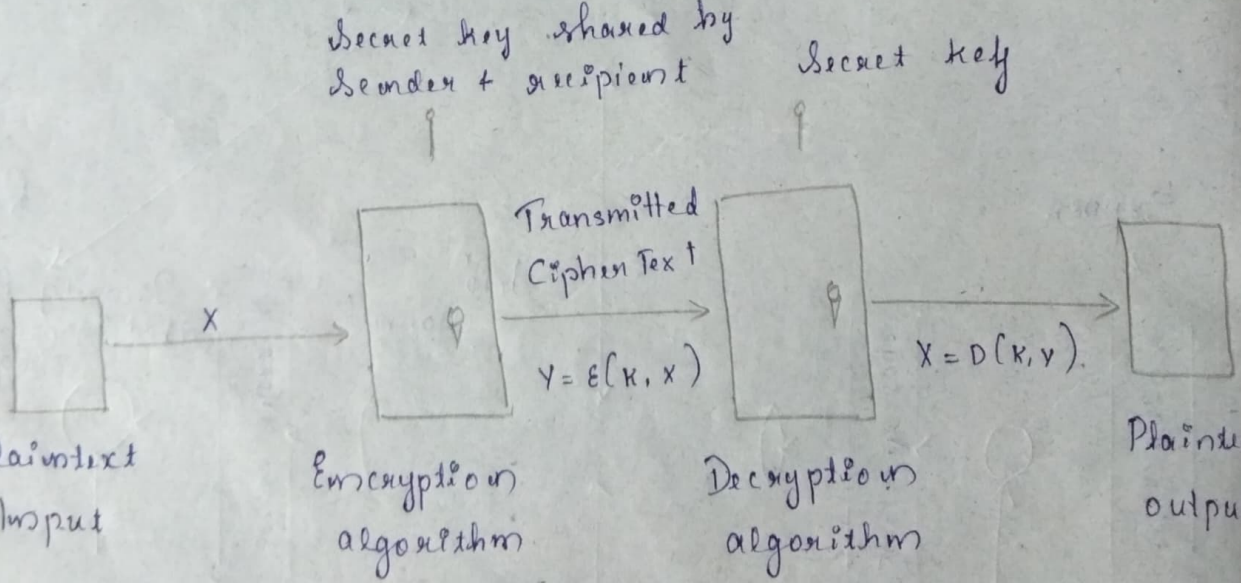
③ Develop methods for the distribution & sharing of the Secret info^{n}.

④ Specify a protocol to be used by the two principles that makes the use of the Security algo^{m} & the Secret info^{n} to achieve a particular Security Service.

13/01/21

Classical Encryption Technique

① SYMMETRIC CIPHER MODEL



- Plaintext : Original intelligence message or data that is fed into the algorithm as input.

- Encryption algorith : It performs various substitution & transformations on the P.T

- Secret key : The Secret key is ~~the~~ also the i/p to the encryption algorithm. The key is a value independent of P.T & of the algorithm. The algorithm will produce a different o/p depending on the specific key being used at a time.

- Cipher text : This is the scrambled message produced as o/p. It depends on the P.T & Secret key. For a given message, two different keys will produce two different C.T. The C.T is an apparently random stream of data & is unintelligible.

- Decryption algorithm : This is essentially the encryption algorithm run in reverse. It takes the C.T & the Secret key & produce the original P.T

Requirements for Secure use of conventional Encryption

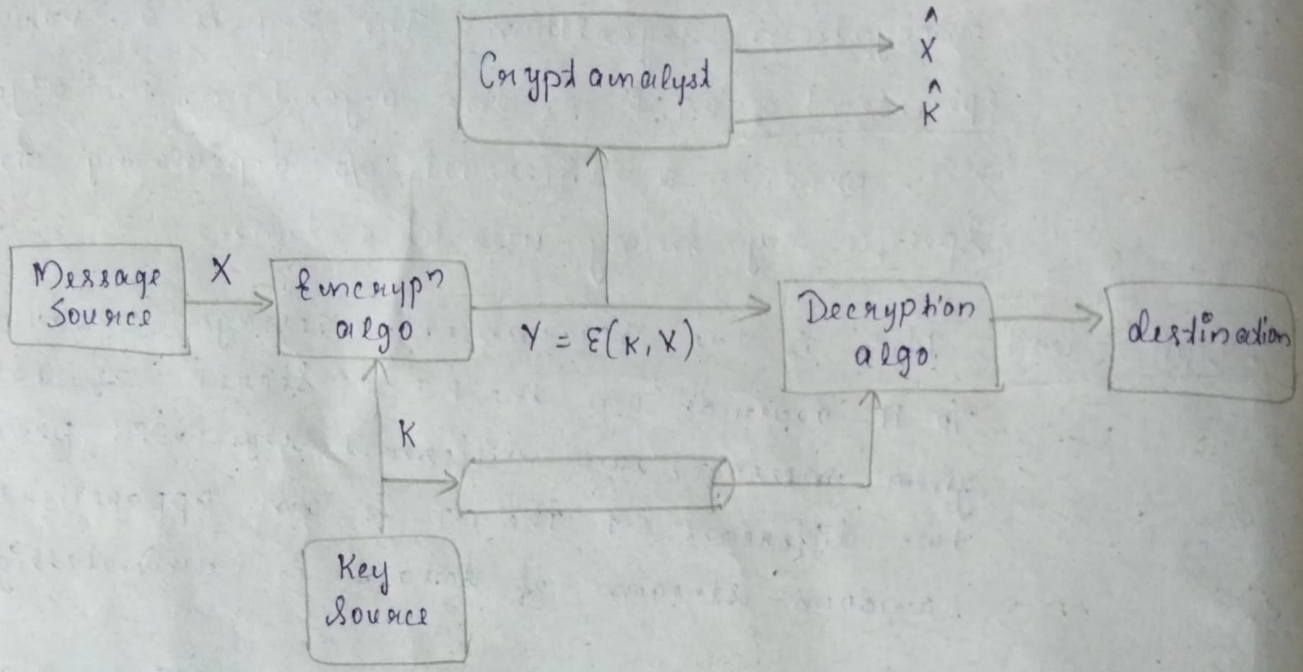
① Strong encryption algorithm : Algo. to be such that an opponent who knows the algorithm & has access to one or more C.T would be unable to decipher the C.T or figure out the key.

② The opponent should be unable to decrypt C.T or discover the key even if he or she is in possession of a no. of C.T together with the P.T that produced each C.T

③ Sender & receiver must have obtained copies of the Secret key in a secure fashion & must keep the key

Secure. If someone can discover the key & knows the algo., all communication using this key is readable.

Modes of Symmetric Cryptosystem



Characteristics of Cryptographic Systems

① Type of operations used for transforming PT to CT.
② The No. of keys used
③ Way in which P.T is processed

① Substitution, in which each element in P.T is mapped into another element &

Transposition, in which elements in the P.T are rearranged.

Fundamental requirement is that no info^n is lost

② If both Sender & receiver use the same key, the system is referred to as Symmetric, Single-key, Secret-key

If the sender & receiver use different keys ⟶ asymmetric, two-key or public-key encryption.

③ A block cipher processes the i/p one block of elements at a time, producing o/p block for each i/p block.

A stream cipher processes the i/p element continously, producing o/p one element at a time, as it goes along.

Cryptanalysis and Brute-force Attack

* Cryptanalysis :

> Cryptanalytic attacks rely on the nature of algo & some knowledge of general characteristics of PT or even some sample PT-CT pairs.

> This type of attacks exploit the char. of the algo. to attempt to deduce a specific PT or to deduce the key being used.

* Brute-force attack :

> The attacker tries every possible key on a piece of CT until an intelligible translation into PT is obtained. On average, half of the possible key

② SUBSTITUTION TECHNIQUES

• A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

• Two basic building blocks of all encryption techniques include

- SUBSTITUTION TECH^{n}
- TRANSPOSITION TECH^{n}

Types of Substitution technique include:

1) Caesar cipher
2) Monoalphabetic cipher
3) Playfair cipher
4) Hill cipher
5) Polyalphabetic cipher
6) One time pad

* Caesar cipher

- It involves ~~involves~~ replacing each ~~of~~ letter of the alphabet with the letter standing three places further down the alphabet

- PT: meet me after the toga party
- CT: PHHW PH DIWHU WKH WRJD SDUWD

- General caesar algorithm

Encryption: $C = E(K, P) = (p + K) \bmod 26$

Decryption: $P = D(K, C) = (C - K) \bmod 26$

Characteristics used for brute force Cryptanalysis:

1) Encryption & Decryption algorithms are known
2) There are only 25 keys to try.
3) Language of the P.T is known & easily recognisable

* Monoalphabetic Cipher

- A Permutation of a finite set of element S is an ordered sequence of all elements of S, with each element appearing exactly once.

- If $S = \{a, b, c\}$, there are six permutations of S
  abc, acb, bac, bca, cab, cba

- In general, there are $n!$ permutations
- Since it uses single cipher alphabet, it is another line of attack
- If the cryptanalyst knows the nature of P.T, then the analyst can exploit the regularities of the language.

* Playfair Cipher

- The best-known multiple-letter encryption cipher is playfair
- It treats digrams in the P.T as single unit & translates these units into C.T diagrams
- (PT) diagrams ⟶ (CT) diagrams
- Eg: Keyword 'MONARCHY'

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

Here a matrix is constructed by filling the letters of the keyword from left to right & from top to bottom.

- PT is encrypted two letters at a time, according to the following rules:

① Repeating P.T letters that are in the same pair are separated with a filler letter, (eg: x), so that balloon would be treated as ba lx lo on

② Two P.T that fall in the same row of matrix are replaced by the letter to the right, with the first element of the row circularly following the last.

Eg: ar is encrypted as RM

③ Two P.T letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.

Eg: mu is encrypted as CM

④ Otherwise, different, each PT in a pair is replaced by the letter that lies in its own row & column occupied by other P.T

Eg: hs becomes BT

ea becomes IM or JM

~~* Hill Cipher~~

Question:

Q. Keyword is 'WELCOME' & plain text is 'meet me'. Using playfair cipher as substitution cipher, convert 'meet me' to corresponding C.T

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

meet me → me et me

→ aw oq aw //

* Hill Cipher

We define the inverse M^{-1} of a square matrix M by the equation $M(M^{-1}) = M^{-1}M = I$

↓

Square Identity Matrix

- more secure

Eg: $A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$ $A^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

$\det(A) = \begin{vmatrix} 5 & 8 \\ 17 & 3 \end{vmatrix} = 15 - 136$

$= -121 \bmod 26 = 9$

$= -9 \bmod 26 = 3$

Inverse of $A = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = \begin{pmatrix} 9 & -24 \\ -51 & 15 \end{pmatrix}$

Eg: kw = hill

C.T = APAD = $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$

kw matrix = $\begin{bmatrix} h & i \\ l & l \end{bmatrix}$

= ~~-121~~ starting from 0

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

$|K| = (7 \times 11) - (8 \times 11)$

$= -11 \quad (-11 + 26)$

$K = 15 \bmod 26$

$K K^{-1} = 1 \bmod 26$

$15 x = 1 \bmod 26$

$\frac{15x1}{26} = 1 \; x$

$\frac{15x7}{26} = 1 \; x$

$15 \times 7 = 105 = 1 \bmod 26$

Multiplicative Inverse

$Adj(K) = Adj \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

Eg: $A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$

$A^{-1} = (\det A)^{-1} (-1)^{i+j} (D_{ji})$

$\det(A) = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} = 15 - 136 = -121 \bmod 26$

$= a \bmod b = (a - b) \times \text{floor}(a/b)$

$= -121 - 26 \times (-4)$

$= -121 + 104 = 9$

$\therefore -121 \bmod 26 = 9$

$(\det A)^{-1} = 9^{-1} \bmod 26$

$= 3$

$A^{-1} \bmod 26 = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3\begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

$A A^{-1} = \begin{pmatrix} (5 \times 9) + (8 \times 1) & (5 \times 2) + (8 \times 15) \\ (17 \times 9) + (3 \times 1) & (17 \times 2) + (3 \times 15) \end{pmatrix}$

$= \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$C = PK \bmod 26$.

Hill System can be expressed as:

$C = E(K, P) = PK \bmod 26$

$P = D(K, C) = CK^{-1} \bmod 26 = \underbrace{PKK^{-1}}_{CT} = P$.

* Polyalphabetic Cipher

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the P.T message.

- Features:

* A set of related monoalphabetic substitution rules is used
* A key determines which particular rule is chosen for a given transformation.

- Vigenere Cipher

. Polyalphabetic ciphers.
. It consists of the 26 Caesar ciphers with shifts of 0 through 25.
. Each cipher is denoted by a key letter.
. Assume a sequence of PT letters, $P = p0, p1, p2, c, pn-1$ & a key consisting of the sequence of letters $K = k0, k1, k2, c, km-1$.
. The sequence of C.T letters $C = C0, C1, C2, c, Cn-1$ is calculated as follows:

$C = C_0, C_1, C_2 \ldots C_{n-1}$

$= E(K, P)$

$= E[(K_0, K_1 \cdots K_{m-1})(P_0, P_1, \ldots P_{n-1})]$

$= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26 \ldots (p_{m-1} + k_{m-1}) \bmod$

$= (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26 \ldots (p_{2m-1} + k_{m-1}) \bmod$

Eg: Key : deceptive deceptive deceptive

P.T : wearediscoveredsaveyourself

C.T : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Encryption : $C_i = (p_i + k_i \bmod m) \bmod 26$

Decryption : $p_i = (C_i - k_i \bmod m) \bmod 26$

• The periodic nature of the keyword can be eliminated by using a non repeating keyword that is as long as the message itself.

• Vigenere proposed an autokey system, in which a keyword is concatenated with the P.T itself to provide a running key.

Eg: key : deceptive we are ~~sav~~ discoveredsav

P.T : we are discovedsaveyourself

C.T : ZICVTWQNGKZEIIGASXSTSLVVWLA

- Vernam Cipher

> The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as P.T & has no statistical relationship to it.

> The system can be expressed as:

$$C_i = P_i \oplus K_i$$
$$P_i = C_i \oplus K_i$$

where, P_i = i^{th} binary digit of P.T

K_i = i^{th} binary digit of key

Hill cipher Example

Keyword = hill $= \begin{bmatrix} h & i \\ l & l \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

CT = APAD $= \begin{bmatrix} A & P \\ A & D \end{bmatrix} = \begin{bmatrix} 0 & 15 \\ 0 & 3 \end{bmatrix}$

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

$|K| = (7 \times 11) - (8 \times 11) = \underline{\underline{-11}}$

$-11 + 26 = 15 //$

$K = 15 \bmod 26$

$K K^{-1} = 1 \bmod 26$

$K = 15$ then $15 \times x = 1 \bmod 26$

$$\frac{15 \times x}{26} = 1$$

$\Rightarrow x = (7) \rightarrow$ multiplicative Inverse

$15 \times 7 = 1 \bmod 26$

$$A^{-1} = \frac{\text{Adj. } A}{|A|}$$

$= \text{Adj } A \times |A|^{-1} \bmod n$

We know $K = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

$$\text{Adj}(K) = \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} = \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix}$$

If a square matrix A has a non-zero determinant, the inverse of the matrix is computed by

$$[A^{-1}]_{ij} = (\det A)^{-1} (-1)^{i+j} (D_{ji})$$

$$K^{-1} = \frac{Adj\ K}{|K|}$$

$$= 7\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \bmod 26$$

$$C = PK \bmod 26$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ P \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 15 \end{pmatrix}$$

$$= \begin{pmatrix} 25\times 0 + 22\times 15 \\ 1\times 0 + 23\times 15 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 18 \\ 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} S \\ L \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ D \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

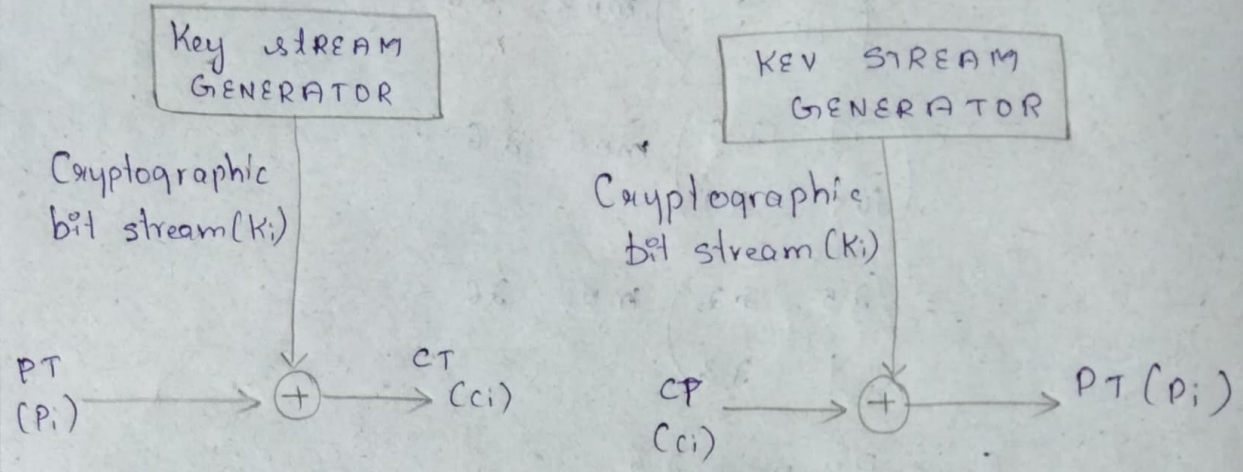
$$= \begin{pmatrix} 25\times 0 + 22\times 3 \\ 1\times 0 + 23\times 3 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 66 \\ 69 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ R \end{pmatrix}$$

P.T = SLOR

c_i = i^{th} binary digit of CT

$\oplus$ = exclusive or (XOR) operation.



> The essence of this technique is the means of construction of the key.

* One Time Pad

- Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated
- Each new message requires a new key of the same length as the new message,
- Such a scheme, One time pad, is unbreakable.

We now show two different decryptions using two different keys.

→ CT : ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
Key : pxlmvmsydofuyrYzwc tnlebnecvgdupathfzzlmnyih
PT : mr mustard with the candlestick in the hall

→ CT : ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
Key : mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
PT : miss Scarlet with the knife in the library.

• Suppose that a cryptanalyst had managed to find these two keys. Two plausible P.T are produced.

• If the actual key were produced in a truly random fashion, then the cryptanalyst cannot say that one of the two keys is more likely than the other.

• The security of one pad is entirely due to the randomness of the key.

• Two fundamental difficulties :

1) There is the practical problem of making large quantities of random keys

2) Problem of key distribution & protection.

Monoalphabetic Vs Polyalphabetic Cipher

* Monoalphabetic cipher is one where each symbol in P.T is mapped to a fixed symbol in C.T	* Polyalphabetic cipher is any cipher based on substitution, using multiple sub^{n} alphabets.
* The r/t ship b/w a character in the P.T & characters in CT is one to one	* The r/tship b/w a char in P.T & char in C.T is one-to-many.
* Each alphabetic char of P.T is mapped onto unique alphabetic character of a C.T	* Each alphabetic char of P.T can be mapped onto 'm' alphabetic char of C.T
* A stream cipher is a mono-alphabetic cipher if the value of key does not depend on the position of the P.T character in the P.T stream.	* A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of P.T. char in the P.T stream.

* Simple Sub^{n} Cipher	* Multiple Sub^{n} Cipher
* Monoalphabetic cipher is described as a sub^{n} cipher in which some fixed mappings from P.T to cipher letters across the entire text are used	* It is described as a sub^{n} cipher in which P.T letters in diff positions are enciphered using different crypto alphabets
* It is not that strong as compared to polyalphabetic cipher.	* It is stronger.

TRANSPOSITION TECHNIQUE

- Transposition technique is an encryption method which is achieved by performing permutation over the plain text.
- Mapping P.T into C.T using transposition technique is called transposition cipher.

Transposition Techniques

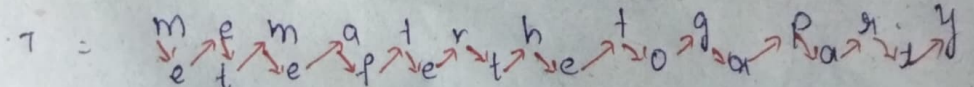
① RAIL FENCE TRANSPOSITION

The steps to obtain C.T using this technique is as follow:

Step1 : P.T is written as a sequence of diagonals.

Step2 : To obtain C.T, the text is read as a sequence of rows.

Eg: P.T = "meet me after the toga party"

C.T = 

= MEMATRHTGPRYETEFETEOAAT

. A more complex scheme is to write the message in rectangle, row by row, & read the message off, col. by col., but permute the order of the columns. The order of the columns then becomes key to the algorithm.

Key : 4 3 1 2 5 6 7

PT : a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

CT : TTNAAPTMTSUOAODWCOIXKNLYPETZ