Selective - Field confidentiality : — Confidentiality of selected field of user data

Traffic flow confidentiality — Protection of information that observed by traffic flow.

Data Integrity : Assurance that the data received are exactly as sent by an authorized entity.

(i) connection Integrity with recovery.
(ii) connection Integrity without recovery.
(iii) Selective field connection Integrity.
(iv) connectionless Integrity.
(v) Selective field connectionless Integrity.

Non Repudiation:

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

(i) Non repudiation, origin → Assurance of source
(ii) Non repudiation, Destination → Assurance of Receiver.

Classical Encryption Techniques:

Types of ciphers: 1. Symmetric cipher technique → single key used
2. Asymmetric cipher technique → Different keys are used

Symmetric ciphers: (conventional Encryption / secret key / single key).

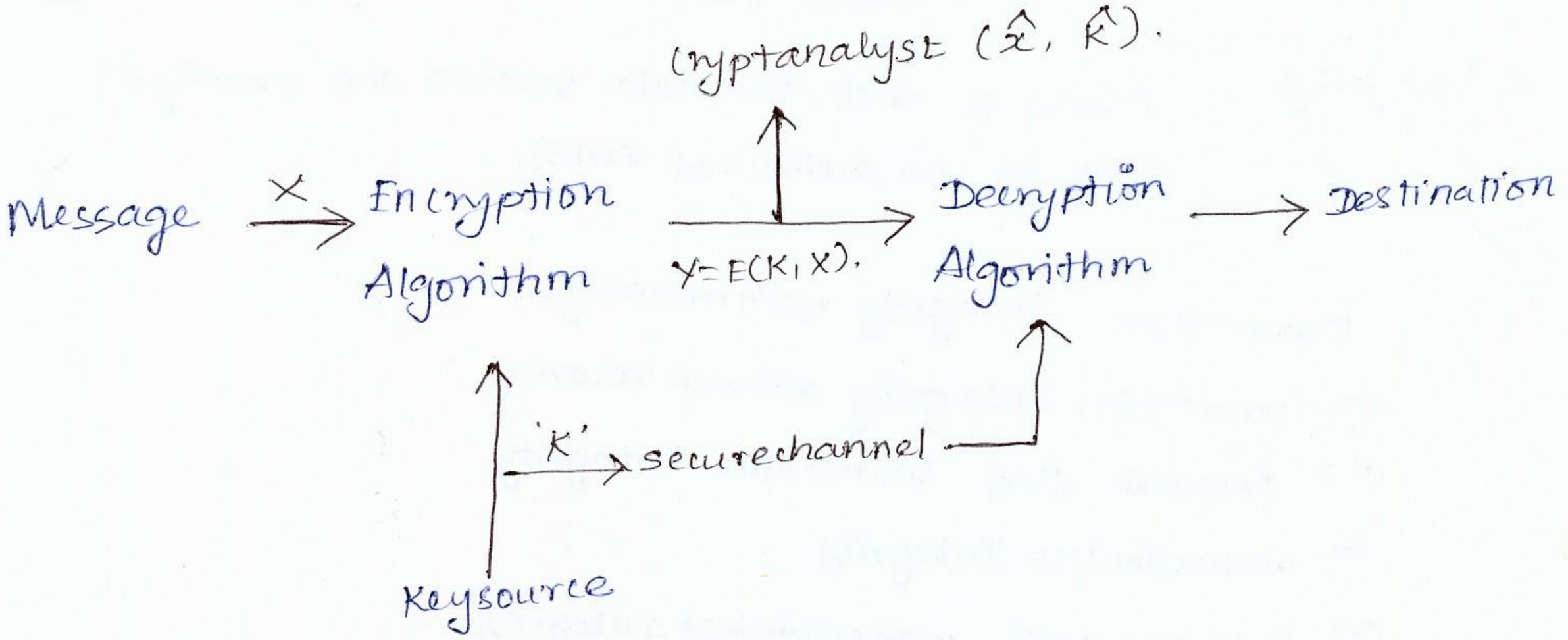
plain text → Original message.

Encryption Algorithm → Various substitution and Transposition Technique.

Secret Key → Key used for Encryption / Decryption Algorithm.

ciphertext → Encrypted message (or) scrambled message.

Decryption → ciphertext converted into original message.



Types:

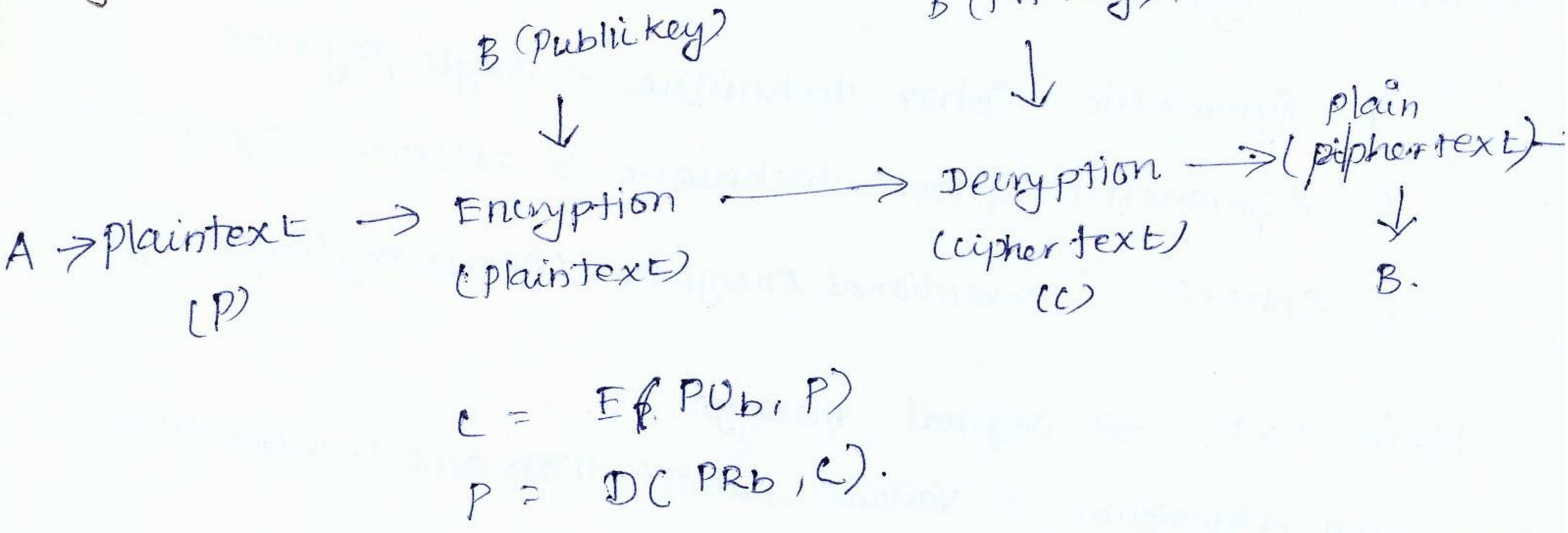
(i) Block cipher → Encrypts a block of plaintext at a time

(ii) Stream cipher → Encrypts data one bit (or one byte at a time.

Eg: DES, AES

Eg: RC4.

Asymmetric ciphers:



$C = E(PU_b, P)$

$P = D(PR_b, C)$.

Cryptanalysis And Brute-Force Attack:

Cryptanalysis → Nature of algorithm, some sample plaintext-ciphertext pairs.
→ By this attack find plaintext (or) key.

Brute-force Attack → Tries every possible keys on a ciphertext until plaintext is obtained

Classical Encryption Technique:

(i) Substitution Technique. → letters of plaintext are replaced by other letters.
- Caesar ciphers
- Monoalphabetic ciphers
- Polyalphabetic ciphers.
  → Vigenere cipher.
- Playfair cipher
- Hill cipher
- One-Time pad.

(ii) Transposition Technique. (rail fence) (permutation).
↳ Rearranging letter order.

(iii) ROTOR Machines

(iv) Steganography.

Substitution Technique:

Caesar cipher:

Involves replacing each letter of the alphabet with the letter standing 'k' places further down the alphabet.

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

$P = D(K, C) = (E - K) \bmod 26.$

a	b	. . .	z
0	1	. . . . .	25

Example:

K = 3 plaintext : Meet Me.

P =	M	e	e	t	m	e
	↓	↓	↓	↓	↓	↓
C = F + P =	P	h	h	W	P	h

Dis Advantages:

(i) Encryption and Decryption Algorithm known

(ii) There are possible only 25 keys to try.

(iii) Language of plaintext is known.

MonoAlphabetic ciphers:

Permutation ⇒ finite set of elements 'S' is an ordered sequence of all the elements of 'S' with each element exactly appearing once.

→ Shuffle the letters arbitrarily.

→ Each plaintext letter maps to a different random ciphertext letter.

→ Here key is 26 letters long.

Plain : 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.

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

plaintext : H e l l o

ciphertext : J F S S H

Advantages:

- Guessing key value is difficult ∵ 26! possible ways.

Disadvantages:

- Monoalphatic substitution ciphers do not change relative letter frequencies.
- Human languages are redundant

Eg: Most common letter in English → E'
followed by T, R, N, I, O, A, S.

Fairly used letters → Z, J, K, Q, X.

Playfair Key Matrix:

(i) 5 x 5 matrix of letters based on a keyword
(ii) Fill in letters of keyword
(iii) Fill rest of matrix with other letters.

Eg: Using the 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.

(i) If a pair is repeated letter, insert filler like 'x'

(ii) If both letters fall in the same row, replace each with letter to right (wrapping back to start from end).

(iii) If both letters fall in the same column, replace each with letter below to it (again wrapping to top from bottom).

(iv) Otherwise each letter is replaced by the letter in the same row and in the same column of the other letter of the pair.

Advantages:

(i) Security much improved over monoalphabetic since it have $26 \times 26 = 676$ entry diagram should have to try.

(ii) monoalphabetic 26 vs playfair 676.

DisAdvantages:

(i) It can be broken, given a few hundred letters of ciphertext are generally sufficient.

(ii) Leaves much of plaintext language intact.

Example:

Encrypt the plaintext "Hello" using the following key.

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.

Plain text : hello

Step 1:

he ll o

↓ Repeated word so insert 'x'

Step 2: he lx lo.

he → ec

lx → qz

lo → Bx.

Step 3: hello → ecqzBx.

Hill cipher:

In hill cipher, the key is a square matrix. of size $m \times m$ in which m is the size of the block. The substitution is determined by m linear equations in which each character is assigned a numerical value.

For $m = 3$, the system can be

$$C_1 = (K_{11} P_1 + K_{12} P_2 + K_{13} P_3) \bmod 26$$
$$C_2 = (K_{21} P_1 + K_{22} P_2 + K_{23} P_3) \bmod 26$$
$$C_3 = (K_{31} P_1 + K_{32} P_2 + K_{33} P_3) \bmod 26.$$

This can be represented as,

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \bmod 26.$$

OR

$$C = KP \bmod 26.$$

Example:

Encrypt the plaintext "Pay More Money"

by using the encryption key $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

Step:

Numeric value of plaintext character are assigned.

0	1	2	3	4	5	6	7	8	9
a	b	c	d	e	f	g	h	i	j
10	11	12	13	14	15	16	17	18	19
k	l	m	n	o	p	q	r	s	t
20	21	22	23	24	25.				
u	v	w	x	y	z				

p - 15

a - 0

y - 24

m - 12

o - 14

r - 17

e - 4

m - 12

o - 14

n - 13

e - 4

y - 24.

The key is 3×3 matrix ∴ so the first three letters of the plaintext are represented by the vector.

$\therefore C_1 = KP \mod 26.$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 & 0 & 24 \end{bmatrix} \quad [\rightarrow \text{wrong}]$$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \quad [- \frac{3\times3}{3\times1}].$$

$= (255+0+120 \quad 315+0+504 \quad 30+0+456) \bmod 26$

$= \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} L \\ N \\ S \end{bmatrix}$

Step 2:

Next three letters $\begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix}$

$C_2 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} \bmod 26.$

$= \begin{bmatrix} 527 \\ 861 \\ 875 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 3 \\ 11 \end{bmatrix} = \begin{bmatrix} H \\ D \\ L \end{bmatrix}.$

Step 3:

Next three letters (E M O) $\Rightarrow$ (4 12 14).

$C_3 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 342 \\ 594 \\ 298 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 22 \\ 12 \end{bmatrix} = \begin{bmatrix} E \\ W \\ M \end{bmatrix}.$

Step 4:

Next three letters n e y ⇒ (13 4 24).

$$C_4 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix} \text{ (4 26)} \bmod 26$$

$$= \begin{bmatrix} 409 \\ 849 \\ 490 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 17 \\ 22 \end{bmatrix} = \begin{bmatrix} T \\ R \\ W \end{bmatrix}.$$

The cipher text is LNS HDLEWMTRW.

Decryption:

Decryption requires using the inverse of matrix K:

$$KK^{-1} = K^{-1}K = I.$$

In this case $K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$

$$P_1 = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} \equiv \begin{bmatrix} 431 \\ 494 \\ 570 \end{bmatrix} \bmod 26$$

$$P_1 = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} P \\ a \\ y \end{bmatrix}.$$

$$P_2 = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \\ 11 \end{bmatrix} = \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} = \begin{bmatrix} m \\ o \\ r \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 4 \\ 22 \\ 12 \end{bmatrix} = \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix} = \begin{bmatrix} e \\ m \\ o \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \\ 22 \end{bmatrix} = \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix} = \begin{bmatrix} n \\ e \\ y \end{bmatrix}$$

plain text = Pay more money.

Polyalphabetii Ciphers:

- Improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- Use each alphabet in turn
- Repeat from start after end of key is reached.

(i) vigenere cipher
(ii) Auto key system.
(iii) vernam cipher.

Vigenere Cipher:

- Simplest polyalphabetic substitution cipher.
- Effectively multiple caesar ciphers.
- Key is multiple letters long $K = K_1, K_2 \ldots K_d$.
- i^{th} letter specifies i^{th} alphabet of the key to use
- Repeat from start after 'd' letters in message
- Decryption simply works in reverse.

Example:

plaintext : weare discovered save yourself.

Key : deceptive.

```
w e a r e d i s c o v e r e d s a v e y o u r s e l f
d e c e p t i v e d e c e p t i v e d e c e p t i v e
```

ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ.

Advantage:

(i) Have multiple ciphertext letters for each plaintext letter.

(ii) Repeated letter frequencies are obscured.

DisAdvantage:

By obtaining the repeated words in cipher text to guess the key value length.

Autokey System:

- Ideally want a key as long as the message
- Vigenere proposed the autokey cipher.
- with keyword is prefixed to message as key.
- knowing keyword can recover the first few letters
- Use these in turn on the rest of the message.

Example:

Key : deceptive

plaintext : we are discovered save yourself.

```
we are discovered save yourself
deceptivewearediscoveredsav
```

Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA.

Vernam cipher:

(i) The message is represented as a binary string (a sequence of 0's and 1's using acoding mechanism such as Ascii coding).

(ii) Key is also a truly random sequence of 0's and 1's of the same length of message.

(iii) The encryption is done by using XOR operation.

a	b	$c = a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Example:

Let the message be 'IF' then its ASCII code be (1001001 1000110) and the key be (1010110 0110001).

Encryption : 1001001 1000110
1010110 0110001

0011111 1110110

Decryption : 0011111 1110110
1010110 0110001

1001001 1000110

Onetime pad:

- Random key as long as the message is used, the cipher will be secure.

Example:

plaintext Hello
key XMCKL

{ plaintext, key should have same length

H (7) E (4) L (11) L (11) O (14)
X (23) M (12) C (2) K (10) L (11)

30 16 13 21 25

mod 26

4 16 13 21 25

Ciphertext ⇒ E Q N V Z

Advantages:

→ Unbreakable Algorithm
→ Random key generation so guessing not possible

Limitations:

→ Practical problem of making large quantities of random keys.
→ Difficult to generate key having same length of message.

Transposition Technique:

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

Railed Fence Technique:

1. The plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

Example: Message: Meet me after the yoga party.

m e m a t r h y g p r y
. e t e f e t e o a a t

Encrypted Message: MEMATRHYGPRYETEFETEOAAT.

Row Transposition ciphers:

2. The plaintext is written in a rectangle, row by row and the read message column by column order of the column become the key to algorithm.

Keyed Transposition cipher:

The key used for encryption and decryption is a permutation key, which shows how the character are permutated.

Message : Enemy attacks to night.

Key : 3 1 4 5 2

Enemy attac kston ightz.

3 1 4 5 2 ↑ Decryption.

Encryption ↓

1 2 3 4 5

EEMYN TAACT TKONS HIT2Z. → ciphertext.

To decrypt the ciphertext is divided into 5 character group using the key in the reverse order the plaintext is retrieved

Steganography:

A plaintext may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformation of the text.

Character Marking:

Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Invisible Link:

A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures:

Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon:

Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.