* cryptosystem Services.

1- Confidentiality.

2- integrity.

3- Authentication.

4- Nonrepudiation.

5- Access control.

---

* confidentiality :- ensure that the information in computer system and transmitted information are accessible only by Authorized parties (users).

* integrity :- ensure that only Authorized users are able to modify computer system and transmitted informations.

* Authentication:- ensure that the origin of message is correctly identified with an Assurance that identify is not False.

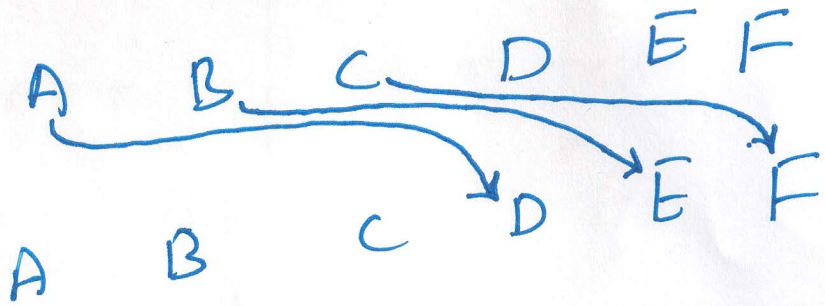
* Non Repudiation:- requires that neither the sender nor receiver of message be able to denying the transmission.

* Access Control:- requires that access to information resources may be controlled by the system.

Caesar Cipher algorithm

the Caeser Cipher involve :-

replacing each letter of the alphabets with the letter standing 3 places.



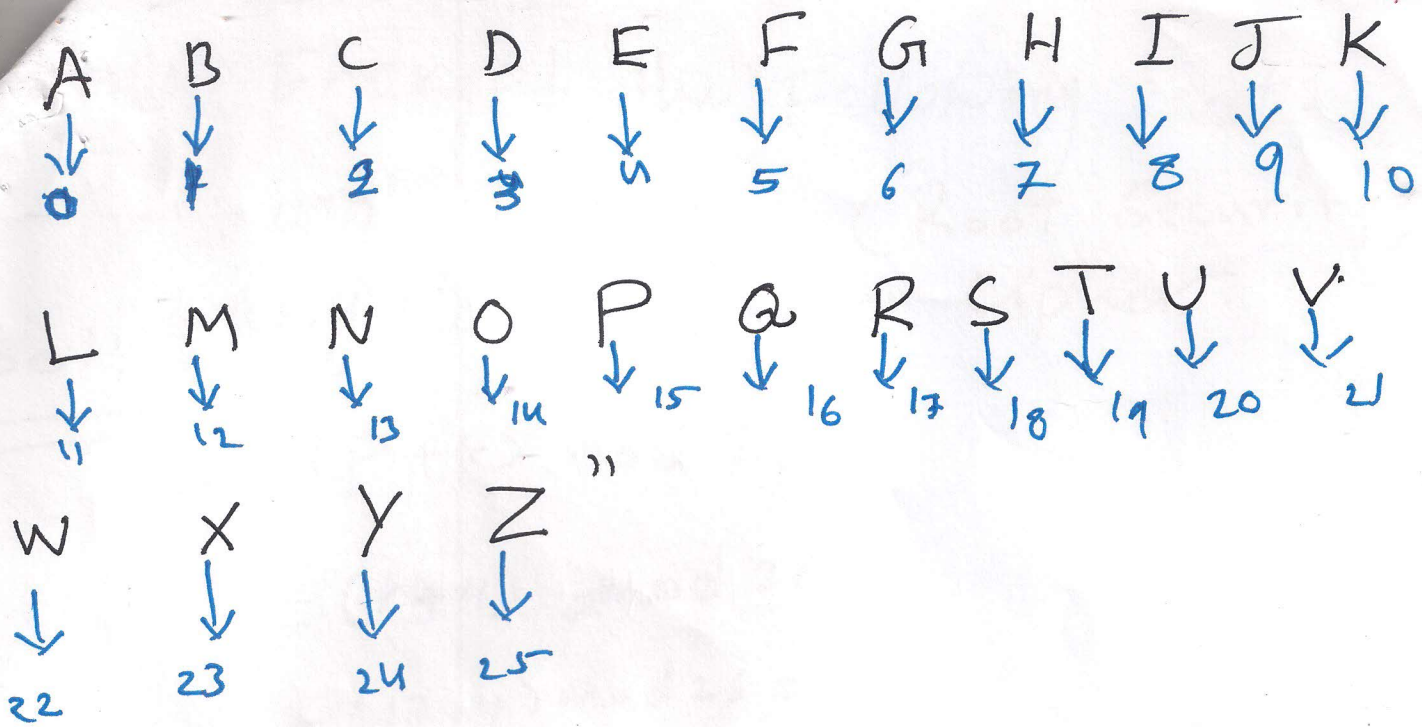
example :

my computer ← plain text.

PBFRPSXWHU ← cipher text.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

P	Q	R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A	B	C



For each plain text "p" substitute the cipher text "c" as the following equations.

$$C = E(p) = (p + k) \bmod 26$$

$$p = D(c) = (c - k) \bmod 26$$

where

c : cipher text.

p : plain text.

k : key.

Example:. Encrypt the Following text. with key = 4. ("Root Security") by using Caeser Cipher.

Sol:

$C = (P + k) \bmod 26$

$= (r + 4) \bmod 26$

$= (17 + 4) \bmod 26 = 21 = V$

$C = (0 + 4) \bmod 26 = (14 + 4) \bmod 26 = 18 = S$

$C = (0 + 4) \bmod 26 = (14 + 4) \bmod 26 = 18 = S$

$C = (T + 4) \bmod 26 = (19 + 4) \bmod 26 = 23 = X.$

وهكذا بالنسبة للكلمة الثانية.

note:-

في حالة ان قيمة الحرف المشفر اقل من قيمة المفتاح فعندها نطرح قيمة n الا قيمة الحرف المشفر ثم نطرح منها قيمة المفتاح.

$(n = 26)$

Example: Decrypt the following text. (6)

with the key = 3

"P B E R P S X W H U"

by using Caeser Cipher.

Sol:-

P	B	E	R	P	S	X	W	H	U
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
16	1	5	17	15	18	23	22	7	20
15									

* $P = (C - k) \bmod 26$

$= (15 - 3) \bmod 26 = (12) \bmod 26 = 12 = M$

* $P = (1 - 3)$ ← [illegible]

$(1 + n - k) \bmod 26$

$(1 + 26 - 3) \bmod 26$

$(24) \bmod 26 = 24 = Y$

* $P = (5 - 3) \bmod 26 = (2) \bmod 26 = 2 = C$
* $P = (17 - 3) \bmod 26 = 14 \bmod 26 = 14 = O$
* $P = (15 - 3) \bmod 26 = 12 \bmod 26 = 12 = M$
* $P = (18 - 3) \bmod 26 = 15 \bmod 26 = 15 = P$
* $P = (23 - 3) \bmod 26 = 20 \bmod 26 = 20 = U$
* $P = (22 - 3) \bmod 26 = 19 \bmod 26 = 19 = T$
* $P = (7 - 3) \bmod 26 = 4 \bmod 26 = 4 = E$
* $P = (20 - 3) \bmod 26 = 17 \bmod 26 = 17 = R$

then the plain text is "my computer".