CryploGraphy

The method of transforming information so that it cannit be easily recovered without special knowledge

Julius Ceaser made the message secret by shifting each letter three letters forward in alphabet

For example:

using this scheme the letter B is sent as E & X is sent as A etc.

A	B	C	...	X	Y	Z
0	1	2		23	24	25

Encryption function

$f(p) = (p+k) \bmod 26$

∵ p is letter number to encrypt

∵ k is the key (shift key)

eg

to encrypt B

$f(1) = (1+3) \% 26$

$= 4 \% 26$

$$\begin{array}{r} 0 \\ 26\overline{)4} \\ \underline{0} \\ 4 \end{array}$$

$f(1) = 4$

$= E$

∴ so E will be used instead of B

Example

Encrypt the word "PARK"

Sol:

First we replace letter by numbers

P A R K

15 0 17 10

Now each letter is replaced using $f(p) = (p+k) \% 26$

18 3 20 13

so encrypted form of "PARK" will be

"SDUN"

=> To recover the original message from encrypted message we use decryption function

$f(p) = (p - K) \% 26$

if the result is smaller than 0 then add 26 in the result.

example

Decrypt "LEWLYPLUJL" using key 7

LEWLYPLUJL

11 4 22 11 24 15 11 20 9 11

using

$f(p) = (p-K) \% 26$

$if\ (f(p) < 0)$

$(f(p) = fp + 26)$

Rough

$(4-7) \% 26$

$= -3 \% 26$

$= -3$

$= -3+26 = 23$

4 23 15 4 17 8 4 13 2 4

"E X P E R I E N C E"