Affine Ciphers

<u>Substitution Cipher</u>

<u>Encryption processes</u>

$$E(x) = (ax + b) \bmod m$$

$E(x) \rightarrow$ encrypted letter.

$x \rightarrow$ position of plain text letter in alphabet

a and $b \rightarrow$ keys.

$m \rightarrow$ size of alphabet

HELLO → Message , key → $a = 5$, $b = 8$

$H \rightarrow 7 \rightarrow (5(7) + 8) \bmod 26 \rightarrow 43 \bmod 26 \rightarrow 17 \rightarrow R$

$E \rightarrow 4 \rightarrow (5(4) + 8) \bmod 26 \rightarrow 28 \bmod 26 \rightarrow 2 \rightarrow C$

$L \rightarrow 11 \rightarrow (5(11) + 8) \bmod 26 \rightarrow 63 \bmod 26 \rightarrow 11 \rightarrow L$

$L \rightarrow 11 \rightarrow (5(11) + 8) \bmod 26 \rightarrow 63 \bmod 26 \rightarrow 11 \rightarrow L$

$O \rightarrow 14 \rightarrow (5(14) + 8) \bmod 26 \rightarrow 78 \bmod 26 \rightarrow 0 \rightarrow A$

RCLLA → encrypted message.

Decryption processes :-

$$D(x) = a^{-1}(x-b) \mod 26$$

$a^{-1} \Rightarrow$ Multiplicative invers of $a \mod 26.$

RCLLA $\rightarrow$ Message   key $\rightarrow$ $a = 5, b = 8$

Multiplicative Invers of 5 mod 26 is $\boxed{21}$

$R \longrightarrow 17 \longrightarrow 21(17-8) \mod 26 \longrightarrow 21(9) \mod 26 \longrightarrow 7$

$C \longrightarrow 2 \longrightarrow 21(2-8) \mod 26 \longrightarrow 21(-6) \mod 26 \longrightarrow 4$

$L \longrightarrow 11 \longrightarrow 21(11-8) \mod 26 \longrightarrow 21(3) \mod 26 \longrightarrow 11$

$L \longrightarrow 11 \longrightarrow 21(11-8) \mod 26 \longrightarrow 21(3) \mod 26 \longrightarrow 11$

$A \longrightarrow 0 \longrightarrow 21(0-8) \mod 26 \longrightarrow 21(-8) \mod 26 \longrightarrow 14.$

$7 \longrightarrow H$
$4 \longrightarrow E$
$11 \longrightarrow L$
$11 \longrightarrow L$
$14 \longrightarrow O$

HELLO $\rightarrow$ Decrephed message.

Ciphers

A → 0	N → 13
B → 1	O → 14
C → 2	P → 15
D → 3	Q → 16
E → 4	R → 17
F → 5	S → 18
G → 6	T → 19
H → 7	U → 20
I → 8	V → 21
J → 9	W → 22
K → 10	X → 23
L → 11	Y → 24
M → 12	Z → 25