JEEVAN.S.U
241059038



# Affine Cipher

## Substitution Cipher

### Encryption process

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

$E(x)$ → Encrypted letter

$x$ → position of plaintext letter in alphabet

$a$ → Key1 and $b$ → Key2

$m$ → size of Alphabet.

HELLO → message ; Key → $a = 5$ , $b = 8$

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

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

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

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

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

RCLLA → Encrypted message

## Decryption Process : (Affine ciphers)

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

$a^{-1}$ → Multiplicative inverse of a mod 26

RCLLA → Message  Key → a=5, b=8

Multiplicative inverse of 5 mod 26 is 21

R → 17 → 21(17-8) mod 26 → 21(9) mod 26 → 7

C → 2 → 21(2-8) mod 26 → 21(-6) mod 26 → 4

L → 11 → 21(11-8) mod 26 → 21(3) mod 26 → 11

L → 11 → 21(11-8) mod 26 → 21(3) mod 26 → 11

A → 0 → 21(0-8) mod 26 → 21(-8) mod 26 → 14

7 → H

4 → E

11 → L

11 → L

14 → O

HELLO → Decrypted Message