Affine Ciphers

Substitution Ciphers

Encryption processes

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

$E(x)$ → encrypted letter.

x → position of plaintext letter in alphabet

a and b → keys.

m → size of alphabet

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

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

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

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

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

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

RCLLA → encrypted message.

Decryption processes :-

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

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.