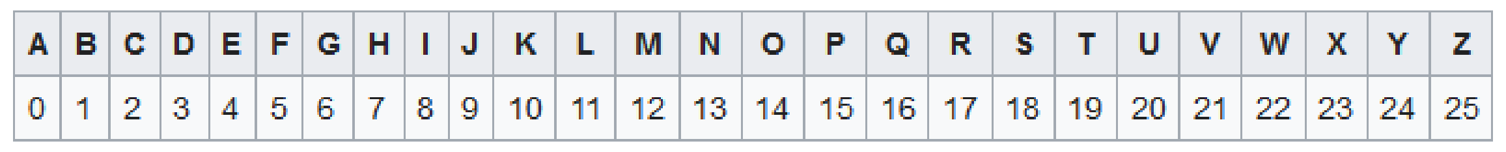
Affine Cipher

- N -> the Size of the character
- {0, n-1}

An Example:

- plaintext : Hacker



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

H -> 7 -> x
A -> 0 -> x
C -> 2 -> x
k -> 10 -> x
e -> 4 -> x
r -> 17 -> x

- Formula : (Ax+B) mod m

- 'm' is the size of the alphabet
  'A' and "B" are the keys.

=> Encryption

m -> 26
a -> 5
B -> 8

H : (5.7+8) mod 26 -> 17 -> R
A : (5.0+8) mod 26 -> 8 -> I
c : (5.2 + 8) mod 26 -> 18 -> S
k : (5.10+8) mod 26 -> 6 -> G
e : (5.4+8) mod 26 -> 2 -> C
r : (5.17+8) mod 26 -> 15 -> P

Plaintext	Cipher
HAcker ->	RISGCP

Decryption

R : 17 -> y
I : 8 -> y
S : 18 -> y
G : 6 -> y y
C : 2 ->
P : 15 -> y

$$\begin{aligned} D(E(x)) &= a^{-1}(E(x) - b) \bmod m \\ &= a^{-1}(((ax + b) \bmod m) - b) \bmod m \\ &= a^{-1}(ax + b - b) \bmod m \\ &= a^{-1}ax \bmod m \\ &= x \bmod m \end{aligned}$$

- 21(y-8) mod 26

R => 21(17-8) mod 26 -> 7 • H
I => 21 (8-8) mod 26 -> 0 • A
S => 21 (18-8) mod 26 -> 2 • C
G => 21 (6-8) mod26 -> 10 • K
c => 21 (2 -8) mod26 -> 4 • e
p => 21 (15-8) mod26 -> 17 • r