CIS 3362 8/20/2025

Shift Cipher

encrypt $f_k(x) = (x + k) \bmod 26$

k: 0 to 25

k: 1 2

decrypt $f_k^{-1}(x) = (x - k + 26) \bmod 26$

x: Cipher

26: alphasize

map $y = ax + b$

a, b: keys

26: alpha size

$f_{a,b}(x) = (ax + b) \bmod 26$

x: 0 to 25

$a = 3$, $b = 5$

$f(x) = (3x + 5) \bmod 26$

Plain	Cipher	Cipher #
A	F	5
B	I	8
C	L	11
D	O	14
E	R	17
F	U	20
G	X	23
H	A	0

Plain	Cipher	Cipher #
I	3D	3
J	6	6
⋮		

Under what conditions will the chart we produce be a one-to-one function?

$a = 14,\ b = 13$ → NOT VALID KEYS!!!

A $f(0) = 14 \times 0 + 13 = 13$

N $f(13) = 14 \times 13 + 13$

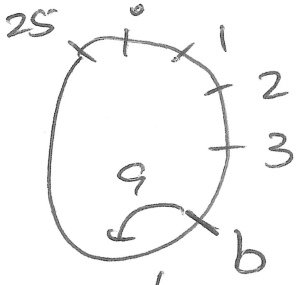
$= \cancel{13(15)}$

$= 7 \times (2 \times 13) + 13$

$= 7 \times 26 + 13$

$\equiv 13 \mod 26$

A key affine cipher is valid if and only if $\gcd(a, \text{alphabet size}) = 1$.



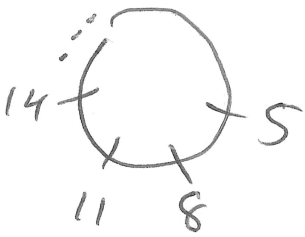
hop by a

$f(0) = b$

$ax + b$

$\equiv$

x to x+1 adding a.



$3J = 26R$

$14J = 26R$

common factor means repeats!

gcd is = # times you land on each landed on spot.

Valid keys are $b \in [0, 25]$

$a \in \{1, 3, 5, 7, 9, 11, 25, 23, 21, 19, 17, 15\}$] 12 valid values relatively prime with 26.

possible keys = 12×26
$= 312$

How do I decrypt???

$$f(x) \equiv (3x+5) \mod 26$$

$$x \equiv (3y+5) \mod 26$$

$$(x-5) \equiv 3y \mod 26$$

$n \equiv (n+26) \bmod 26$
$n \equiv (n-26) \bmod 26$

$$9(3y) \equiv 9(x-5) \mod 26$$

$$27y \equiv (9x-45) \mod 26$$

$$1y \equiv 9x + 7$$

$$f^{-1}(x) = (9x+7) \mod 26$$

Observation

Shift is a specific type of Affine Cipher with $a = 1$.

Affine Cipher for encryption keys (3,5) the matching decryption keys are (9,7).

Plain	Cipher
(9) J →	G (6)

$f^{-1}(6) = (9 \times 6 + 7) \mod 26$
$= (54+7) \mod 26$
$= 61 \equiv 9 \mod 26$

Affine Encryption Function

$a = 15, \quad b = 4$

Find the corresponding Decryption Function.

$$x = (15y + 4) \mod 26$$

$$7(15y) \equiv 7(x - 4) \mod 26$$

$$y \equiv (7x - 28) \mod 26$$

$$y \equiv (7x + 24) \mod 26$$

$n \equiv (n+26) \mod 26$

$n \equiv (n-26) \mod 26$

$a = 7, b = 24$

encryption

3, 5	⟷	9, 7
15, 4	⟷	7, 24

Let's say we don't want to try all 312 keys!

Cipher M → Plain (B)

Cipher (Q) → Plain (H)

Affine Cipher

WZUYN

ZOOX(M)BQ

(H)EFX

$f^{-1}(12) = (a \cdot 12 + b) = 1 \mod 26$

$f^{-1}(16) = (a \cdot 16 + b) = 7 \mod 26$

$-\quad 12a + b \equiv 1 \mod 26$

$\quad\; 16a + b \equiv 7 \mod 26$

$4a \equiv 6 \mod 26$

$a = 8 \mod 13$

$8 \mod 26$

$21 \mod 26$

$4a = 6 + 26n, \quad n \in \mathbb{Z}$

$2a = 3 + 13n$

$2a \equiv 3 \mod 13$

$a = 21$

$21 \times 12 + b \equiv 1 \mod 26$

$-5 \times 12 + b \equiv 1 \mod 26$

$-8 + b \equiv 1 \mod 26$

$b \equiv 9 \mod 26$

Decrypt $a = 21, \quad b = 9$