Shift Cipher

$A=0,\ B=1,\ C=2,\ \dots,\ Z=25$

encryption + decryption are functions of the message and the key.

$$f_k(m) = (m+k) \bmod 26$$

%

$t=19,\ k=17$ $\quad (19+17) \bmod 26$

$$= 36 \bmod 26$$

$$= \boxed{10}$$ (must map to a value in btw 0 and 25)

K

$$d_k(c) = (c-k) \bmod 26$$

$$10 - 17 \bmod 26$$

$$-7 \bmod 26$$

$$19 \bmod 26$$

T

$$(c-k+26) \% 26$$

Affine Cipher

keys : a, b

$e_{a,b}(m) = (am + b) \bmod 26$

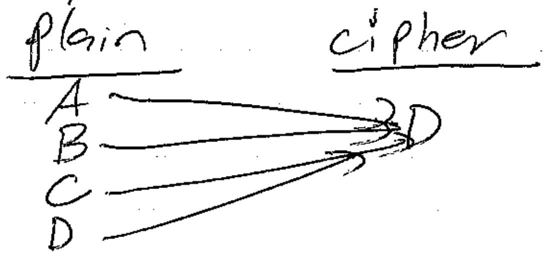
$a = 7, b = 4, m = 'J' = 9$

$e_{7,4}(9) = (7 \times 9 + 4) \bmod 26$

$= 67 \bmod 26$

$= \boxed{15}$ 'p'

If a is 0, $e(m) = 0 + b = \boxed{b}$



if 2 diff letters encrypt to the same ciphertext letter, there is NO way to decrypt reliably!

encryption function MUST BE one-to-one (injection)

What are possible values for a?

2, 3, 5, 7, 11, 13, 17, 19, 23

two of these don't work...

2 and 13 because they are factors of 26.

$\gcd(a, 26) = 1.$

Shift cipher is a special case of the affine with a set to 1.

a and b are relatively prime, if and only if $\gcd(a,b) = 1.$

$a = 2 \quad f(m) = (2m + b) \% 26$

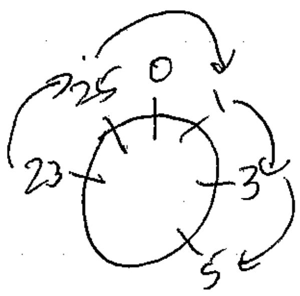
$a = 8 \quad f(m) = (8m + b) \% 26$

$m = 3, \; m = 16$

$f(3) = \boxed{(2 \times 3 + b) \% 26}$

$f(16) = (2 \times 16 + b) \% 26$

$= (32 + b) \% 26$



So, the possible values of a are:

$1, ~~2~~, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$

affine cipher has $12 \times 26 = 312$ possible keys.

Cipher

$$\boxed{e_{a,b}(m)} = (am+b) \bmod 26$$

$$C = (am+b) \bmod 26$$

$$\boxed{C - b = am \bmod 26}$$

$C-b$ might <u>NOT</u> equal am they just both give same remainder when ~~...~~ modded by 26.

You can't divide a mod equation on both sides but you can multiply both sides.

$C=15$

$15(15-4) = (7m)15 \bmod 26 \quad (m = 9(5))$

Affine Cipher

$$e_{7,4}(m) = (7m+4) \bmod 26$$

$J=9$, $e_{7,4}(9) = (7\cdot 9+4) \bmod 26$
$= 67 \bmod 26$
$= 15 \bmod 26$ $\boxed{\text{'P'}}$

Where did this come from?

$C = 7m+4 \bmod 26$

$15(C-4) = 15(7m) \bmod 26$

$15c - 60 = 105m \bmod 26$

$m \equiv 15c - 60 \bmod 26$

$m \equiv \boxed{15c + 18 \bmod 26}$

Decryption function is $\boxed{f(c) = (15c+18) \bmod 26}$

Problem I want to solve is as follows: for any value a, what value a' exists such that $a \times a' \equiv 1 \bmod 26$.

We call a' $\boxed{a^{-1} \bmod 26}$.

$\boxed{7^{-1} \equiv 15 \bmod 26}$

In general, we want an algorithm, given a and n, (positive ints), which determines $a^{-1} \bmod n$, if it exists.

$3^{-1} \bmod 15$ DOES NOT EXIST!

$6^{-1} \bmod 15$ DOES NOT EXIST!

$a^{-1} \bmod n$ exists if and only if $\gcd(a, n) = 1$. (Greatest Common Divisor)

$\boxed{n=26,\ a=7}$

Euclidean Algorithm

A. $26 = 3 \times \underline{7} + \underline{5}$ $\qquad \boxed{26 - 3\times 7} = 5$

B. $7 = 1 \times \underline{5} + \underline{2} \rightarrow \qquad \boxed{7 - 1\times 5} = 2$

C. $5 = 2 \times \underline{2} + \boxed{1}$

$2 = 2 \times 1$

Extended Euclidean

Write last step (C), backwards:

$\underline{5} - 2 \times \underline{2} = 1$, Use equation B to substitute for the smaller of the underlined values

$5 - 2 \times (7 - 1\times 5) = 1$

$5 - 2\times 7 + 2 \times 5 = 1$ $\quad$ Simplify

$3 \times \underline{5} - 2 \times \underline{7} = 1$ Use equation A to substitute smaller of the 2 values

$3 \times (26 - 3\times 7) - 2 \times 7 = 1$

$3 \times 26 - 9 \times 7 - 2 \times 7 = 1$

$3 \times \underline{26} - 11 \times \underline{7} = 1 \mod 26$

$-11 \times 7 \equiv 1 \mod 26$ 8/26 3

$15 \times 7 \equiv 1 \mod 26$

$$\boxed{7^{-1} \equiv 15 \mod 26}$$

Value	1	3	5	7	11	17	25
Inverse mod 26	1	9	21	15	19	23	25

Find $53^{-1} \bmod 198$

$198 = 3 \times \underline{53} + \underline{39}$

$53 = 1 \times \underline{39} + \underline{14}$

$39 = 2 \times \underline{14} + 11$

$14 = 1 \times \underline{11} + \underline{3}$

$11 = 3 \times \underline{3} + \underline{2}$

$3 = 1 \times 2 + \boxed{1}$

$2 = 2 \times 1$

$3 - 1 \times 2 = 1$

$3 - 1 \times (11 - 3 \times 3) = 1$

$3 - 1 \times 11 + 3 \times 3 = 1$

$4 \times \underline{3} - 1 \times \underline{11} = 1$

$$\left.\begin{array}{l} 4(14 - 1 \times 11) - 1 \times 11 = 1 \\ 4 \times \underline{14} - 5 \times \underline{11} = 1 \end{array}\right\} \text{2 steps...}$$

$4 \times 14 - 5(39 - 2 \times 14) = 1$

$4 \times 14 - 5 \times 39 + 10 \times 14 = 1$

$14 \times \underline{14} - 5 \times \underline{39} = 1$

$14(53 - 1 \times 39) - 5 \times 39 = 1$

$14 \times \underline{53} - 19 \times \underline{39} = 1$

$14 \times 53 - 19(198 - 3 \times 53) = 1$

$14 \times 53 - 19 \times 198 + 57 \times 53 = 1$

$71 \times 53 - 19 \times 198 = 1 \bmod 198$

$71 \times 53 \equiv 1 \bmod 198$

$53^{-1} \equiv 71 \bmod 198$