Last Time 8/27/21 CIS 3362

Affine Cipher

$f(x, (a,b)) = (ax+b) \mod 26$

Given the encryption function, how do we find the decryption function?

$f(x) = (3x+2) \mod 26$

$x \equiv 3y + 2 \mod 26$

$\Rightarrow$ magic

$9(x-2) \equiv 9(3y) \mod 26$

$9x - 18 \equiv 27y \mod 26$

$y \equiv 9x - 18 \mod 26$

$y \equiv (9x + 8) \mod 26$

decryption function

$(a^{-1})(x-b) \equiv (a^{-1})ay \mod 26$

We want a^{-1} to be such that

$a \cdot a^{-1} \equiv 1 \mod 26$

a^{-1} is the multiplicative inverse of a mod 26

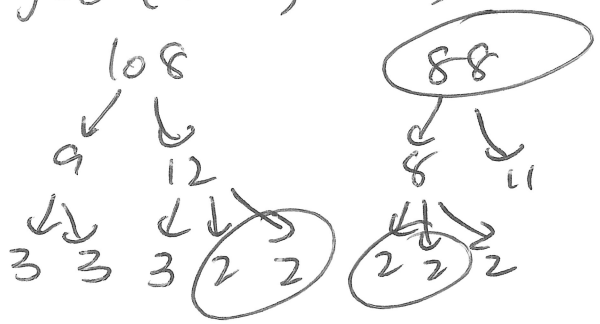
Euclid

Father of Geometry, but he also solved this modular inverse problem!

(1) Euclidean Algorithm
(2) Extended Euclidean Algorithm

→ Set of steps to find the greatest common divisor of 2 integers.

gcd(108, 88)



$108 = 1 \times 88 + 20$

$88 = 4 \times 20 + 8$

$20 = 2 \times 8 + 4$

$8 = 2 \times 4$

gcd(108, 88) = 4

$(x - b) \equiv ay \mod 26$

if gcd(a, 26) ≠ 1, no a^{-1} exists!

Let's do gcd(26, 3) = 1

$26 = 8 \times 3 + 2 \Rightarrow 26 - 8 \times 3 = 2$

$3 = 1 \times 2 + 1$

$2 = 2 \times 1$

Goal of the Extended Euclidean Alg:
Find integers x and y such that

$$ax + by = 1$$

$$26x + 3y = 1$$

$3 - 1 \times 2 = 1$ Work bottom eq backwards

$3 - 1 \times (26 - 8 \times 3) = 1$ Substitute for 2 writing the prev. eq. backwards.

$3 - 1 \times 26 + 8 \times 3 = 1$

$9 \times 3 - 1 \times 26 = 1$, one soln $x = -1, y = 9$

$9 \times 3 - 1 \times 26 \equiv 1 \pmod{26}$

$9 \times 3 - 1 \times 0 \equiv 1 \pmod{26}$

$9 \times 3 \equiv 1 \pmod{26}$

$\equiv$

$5x + 1$
05_1 102 26

Find 34^{-1} mod 175

(What number do I have to multiply 34 by to obtain 1 mod 175?)

$175 = 5 \times 34 + 5 \longrightarrow (175 - 5 \times 34) = 5$

$34 = 6 \times 5 + 4 \longrightarrow 34 - 6 \times 5 = 4$

$5 = 1 \times 4 + 1$

$5 - 1 \times 4 = 1$

$5 - 1 \times (34 - 6 \times 5) = 1$

$5 - 1 \times 34 + 6 \times 5 = 1$

$7 \times 5 - 1 \times 34 = 1$

$7 \times (175 - 5 \times 34) - 1 \times 34 = 1$

$7 \times 175 - 35 \times 34 - 1 \times 34 = 1$

$7 \times 175 - 36 \times 34 = 1$

$7 \times 175 - 36 \times 34 \equiv 1 \mod 175$

$-36 \times 34 \equiv 1 \mod 175$

$-36 \equiv \boxed{139 \pmod{175}}$

So $34^{-1} \equiv 139 \pmod{175}$

Affine function

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

What is the decryption function?

We need to find $15^{-1} \mod 26$.

$26 = 1 \times 15 + 11$

$15 = 1 \times 11 + 4$

$11 = 2 \times 4 + 3$

$4 = 1 \times 3 + 1$

$11 - 2 \times 4 = 3$

$15 - 1 \times 11 = 4$

$26 - 15 = 11$

$4 - 1 \times 3 = 1$

$4 - 1 \times (11 - 2 \times 4) = 1$

$4 - 1 \times 11 + 2 \times 4 = 1$

$3 \times 4 - 1 \times 11 = 1$

$3(15 - 11) - 1 \times 11 = 1$

$3 \times 15 - 3 \times 11 - 1 \times 11 = 1$

$3 \times 15 - 4 \times 11 = 1$

$3 \times 15 - 4(26 - 15) = 1$

$3 \times 15 - 4 \times 26 + 4 \times 15 = 1$

$7 \times 15 - 4 \times 26 = 1$

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

$15^{-1} \equiv 7 \pmod{26}$

$x = 15y + 4 \mod 26$

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

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

$\boxed{y = (7x + 24) \mod 26}$

Breaking Affine

$f('e') = 'b'$
$f('t') = 'y'$
} let's say we knew this.

$f^{-1}(x) = (ax + b) \bmod 26$

$f^{-1}(1) = a(1) + b \equiv 4 \bmod 26$
$f^{-1}(24) = a(24) + b \equiv 19 \bmod 26$

$17(23a) \equiv (15)17 \bmod 26$

$a \equiv 255 \bmod 26$
$a \equiv -5 \equiv 21 \bmod 26$

$f^{-1}(1) = 21 \cdot 1 + b \equiv 4 \bmod 26$
$21 + b \equiv 4 \bmod 26$
$b \equiv -17 \equiv 9 \bmod 26$

$$\boxed{f^{-1}(x) = (21x + 9) \bmod 26}$$

What do I do if I get something like

10 $\boxed{4a \equiv 7 \cdot 10 \bmod 13}$
$a \equiv 70 \equiv 5 \bmod 13$

$8a \equiv 14 \bmod 26$?
$8a = 14 + 26n$ for some int n
$4a = 7 + 13n$