CIS 3362 8/26/22

affine

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

$0 \le b < 26$

$\gcd(a, 26) = 1$

enc $f(x) = (3x + 7) \bmod 26$

to find dec

$$x \equiv (3y + 7) \bmod 26$$

$$9(3y) \equiv 9(x - 7) \bmod 26$$

$$27y \equiv (9x - 63) \bmod 26$$

$$1y \equiv (9x + 15) \bmod 26$$

$x = 8$

$3 \times 8 + 7$

$= 24 + 7$

$\equiv 31$

$\equiv 5 \bmod 26$

decryption $f^{-1}(x) = (9x + 15) \bmod 26$

$9 \times 3 \equiv 1 \bmod 26$

$9 \times 5 + 15 = 45 + 15$

$= 60$

$\equiv 8 \bmod 26$

if $ab \equiv 1 \bmod n$

then $b \equiv a^{-1} \bmod n$

"b is a inverse mod n"

Today's Goal:

Learn Euclidean Algorithm +
Extended Euclidean Algorithm

W 1) efficient computation gcd

2) = computation modular inverse
(ONLY relevant if gcd = 1)

gcd(113, 72)

quotient ↙ remainder

$113 = 1 \times 72 + 41$

$72 = 1 \times 41 + 31$

$41 = 1 \times 31 + 10$

$31 = 3 \times 10 + \boxed{1}$ ← gcd

$10 = 10 \times 1$ ← no rem

gcd(186, 78)

$186 = 6 \times 31$

$78 = 6 \times 13$

$186 = 2 \times 78 + 30$

$78 = 2 \times 30 + 18$

$30 = 1 \times 18 + 12$

$18 = 1 \times 12 + \boxed{6}$ ← gcd

$12 = 2 \times 6$

Is it possible for $78x \equiv 1 \bmod 186$

No!

```
int gcd(int a, int b) {
    return b==0 ? a : gcd(b, a%b);
}
```

Goal find $72^{-1} \bmod 113$

What value of y satisfies $72y \equiv 1 \bmod 113$?

We will find int (x, y) such that

$$113x + 72y = 1$$

$113 = 1 \times 72 + 41$

$72 = 1 \times 41 + 31$

$41 = 1 \times 31 + 10$

$\Rightarrow 31 = 3 \times 10 + 1$

$10 = 10 \times 1$

$41 - 1 \times 31 = 10$

$72 - 1 \times 41 = 31$

$113 - 1 \times 72 = 41$

$31 - 3 \times 10 = 1$

$31 - 3(41 - 1 \times 31) = 1$

$31 - 3 \times 41 + 3 \times 31 = 1$

$4 \times 31 - 3 \times 41 = 1$

$4 \times (72 - 1 \times 41) - 3 \times 41 = 1$

$4 \times 72 - 4 \times 41 - 3 \times 41 = 1$

$4 \times 72 - 7 \times 41 = 1$

$4 \times 72 - 7(113 - 1 \times 72) = 1$

$4 \times 72 - 7 \times 113 + 7 \times 72 = 1$

$11 \times 72 - 7 \times 113 = 1$

$y = 11, x = -7$

$11 \times 72 - 7 \times 113 \equiv 1 \bmod 113$

$11 \times 72 - 7 \times 0 \equiv 1 \bmod 113$

$11 \times 72 \equiv 1 \bmod 113$

$11 \equiv 72^{-1} \bmod 113$

Alternate way to Break Affine

known plain/cipher text attack

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

Plain	Cipher
E	B
T	Y

encrypt

$f(4) = 4a + b \equiv 1 \mod 26$

$f(19) = 19a + b \equiv 24 \mod 26$

decrypt

$f(1) = a(1) + b \equiv 4 \mod 26$

$f(24) = a(24) + b \equiv 19 \mod 26$

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

$a \equiv 255 \mod 26$

$\boxed{a \equiv 21 \mod 26}$

$ax1 + b \equiv 4 \mod 26$

$21 + b \equiv 4 \mod 26$

$b \equiv -17 \mod 26$

$b \equiv 9 \mod 26$

decrypt: $f(x) = (21x + 9) \mod 26$

What would I do If I got

$22a \equiv 16 \mod 26$?

there's some n such that $\leftrightarrow$

$22a + 26n = 16$

$11a + 13n = 8$

$11a = 8 - 13n$

take mod 13 $\rightarrow$ $\boxed{11a \equiv 8 \pmod{13}}$

$6(11a) \equiv 6 \cdot 8 \mod 13$

$\boxed{a \equiv 9 \mod 13}$

$a \equiv 9 \mod 26$

$a \equiv 22 \mod 26$