CIS 3362 8/23/2023

last time Shift cipher

key: 0 to 25 letters #s A = 0 – Z = 25

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

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

↑ linear function

new idea

let our keys be a, b (0 – 25 each)

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

key a = 5, b = 8

encrypt "CAKE"

2, 0, 10, 4

C → S
A → I
K → G
E → C

$f(2) = (5\times2+8) = 18$

$f(0) = (5\times0+8) = 8$

$f(10) = (5\times10+8) \equiv 6 \pmod{26}$

$f(4) = (5\times4+8) \equiv 2 \pmod{26}$

↓ make chart

ciphertext = SIGC

(1) How do I decrypt?

(2) Do all the keys "work"?

Try encrypting with $f_1(x) = (4x+7) \bmod 26$

$f_2(x) = (13x+1) \bmod 26$

$f_2(0) = (13\times0+1) = 1$

$f_2(2) = (13\times2+1) \equiv 1 \bmod 26$ } PROBLEM!

all evens encrypt to 1
odds encrypt to 14] Can't reverse This!

For what values of a and b does

$f(x) = (ax+b) \bmod 26$ have an inverse?

The value of b doesn't matter (all b's are valid provided that a works)

26 possible values of b

What about a?

let's look @ $f(x) = (4x+7) \bmod 26$

$f(0) = (4\times0+7) = 7$

$f(13) = (4\times13+7) \equiv 7 \bmod 26$

$f(x_1) = ax_1 + b$

$-\ f(x_2) = ax_2 + b$

$a(x_1 - x_2) \equiv 0 \bmod 26$

$0 < |x_1 - x_2| < 26$

↳ if a and 26 share a common factor then $x_1 - x_2 = \frac{26}{cf}$.

$\gcd(a, 26) = 1$ $\quad$ $\gcd(a, \text{ALPHASIZE}) = 1$

$a = 1, 3, 5, 7, 9, 11$
$25\ 23, 21, 19, 17, 15$

12 values

7 and 26 are relatively prime means $\gcd(7, 26) = 1$.

Affine Cipher has a total of $12 \times 26 = 312$ keys

$$f(x) = (5x + 8) \mod 26$$

$$x = (5y + 8) \mod 26$$

$$5y \equiv (x - 8) \mod 26$$

$$21 \times 5y \equiv 21(x - 8) \mod 26$$

$$105y \equiv (21x - 168) \mod 26$$

$-168 + 7 \times 26 = 14$

$$y \equiv (21x + 14) \mod 26$$

$$f^{-1}(x) = (21x + 14) \mod 26$$

encrypt CAKE $\Longrightarrow$ SIGC
18, 8, 6, 2

$$f^{-1}(18) = (21 \times 18 + 14) \equiv (-5)(-8) + 14$$
$$= 40 + 14$$
$$= 54$$
$$\equiv 2 \mod 26 \ (C)$$

$$f^{-1}(8) = (21 \times 8 + 14) = (-5 \times 8) + 14$$
$$= -40 + 14$$
$$= -26$$
$$\equiv 0 \pmod{26} \quad (A)$$

$$f^{-1}(6) = (21 \times 6 + 14) = (-5 \times 6) + 14$$
$$= -16$$
$$\equiv 10 \pmod{26} \quad (K)$$

$$f^{-1}(2) = (21 \times 2 + 14) \equiv (-5 \times 2 + 14)$$
$$\equiv 4 \bmod 26 \quad (E)$$

for 26, I have a table you can use for the "guesses" → MODULAR INVERSES

$$5 \times 21 \equiv 1 \bmod 26$$

thus $21 \equiv 5^{-1} \bmod 26$

and $5 \equiv 21^{-1} \bmod 26$

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

② Is there a method to obtain $a^{-1} \bmod n$?

① When does $a^{-1} \bmod n$ exist?

→ $ax \equiv 1 \bmod n$ is impossible if $\gcd(a, n) > 1$.

$6x \equiv \square \bmod 15$

↳ has to be mult 3.

→ Extended Euclidean Algorithm

$\gcd(26, 5) = 1$

$26 = 5 \times 5 + 1$ ← gcd

$5 = 5 \times 1$

$\gcd(26, 7)$

$26 = 3 \times 7 + 5 \longrightarrow 26 - 3 \times 7 = 5$

$7 = 1 \times 5 + 2 \longrightarrow 7 - 1 \times 5 = 2$

$5 = 2 \times 2 + 1$

$5 - 2 \times 2 = 1$ ← will never change

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

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

$3 \times 5 - 2 \times 7 = 1$

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

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

$3 \times 26 - 11 \times 7 = 1$

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

$-11 \times 7 \equiv 1 \mod 26$

$7^{-1} \equiv (-11) \equiv 15 \pmod{26}$