CIS 3362 8/23/24

(1) Announcement: Class Monday (8/26/24) will be replaced with a Zoom recording posted beforehand. Watch before Wednesday.

(2) HW #1 is due today.

Affine Cipher

$f_{a,b}(x) = 5x + 18$

$y = 5x + 18$ → MAGIC

$21(y - 18) = 21(5x) \mod 26$

$ax \equiv b \mod n$

~~Now~~ Not allowed to divide by a.

Find a value, c such that

$ac \equiv 1 \mod n$

Given

if a and n share common factor this is IMPOSSIBLE

$a = da'$, $n = dn'$, $d > 1$

$da' \cdot c \equiv 1 \mod dn'$

$\Rightarrow (dn') \mid (da'c - 1)$

$\Rightarrow d \mid (dac - 1)$

$c = (a^{-1} \bmod n)$

"a inverse mod n"

Extended Euclidean Algorithm

Goals:

Given 2 pos ints a, b

(1) find greatest common divisor of a, b

(2) if $\gcd(a,b) = 1$, we can also obtain $a^{-1} \bmod b$.

Goal: Find $5^{-1} \bmod 26$

Run GCD w/ 26, 5

$26 = 5 \times 5 + 1$

$26 - 5 \times 5 = 1$

$\rightarrow 26 - 5 \times 5 \equiv 1 \bmod 26$

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

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

47^{-1} mod ~~187~~ 195

$^{2}47$ $\times 4$ = (188)

q r

$195 - 4\times 47 = 7$

$47x \equiv 1 \mod 195$

$* \; 195 = 4 \times \underline{47} + (7)$

$* \; 47 = 6 \times 7 + \underline{5}$ → $47 - 6\times 7 = 5$

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

$5 = 2 \times \underline{2} + \underline{1}$ ← gcd // Euclidean

$2 = 2 \times 1$ $\square$

→ $\underline{5} - 2\times\underline{2} = 1$ ← Step

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

$\underline{5} - 2\times 7 + 2\times\underline{5} = 1$

$3\times\underline{5} - 2\times\underline{7} = 1$

$3(47 - 6\times 7) - 2\times 7 = 1$

$3\times 47 - 18\times 7 - 2\times 7 = 1$

$3\times\underline{47} - 20\times\underline{7} = 1$

$3\times 47 - 20(195 - 4\times 47) = 1$

$\underline{3\times 47} - 20\times 195 + \underline{80\times 47} = 1$

$83\times\underline{47} - 20\times\underline{195} = 1$

$83\times 47 - 20\times 195 \equiv 1 \mod 195$

$83\times 47 \equiv 1 \mod 195$

$\boxed{47^{-1} \equiv 83 \mod 195}$

$108^{-1} \mod 239$

$239 = 2 \times 108 + 23$

$108 = 4 \times 23 + 16$

$*23 = 1 \times 16 + 7$

$16 = 2 \times 7 + 2 \longrightarrow 16 - 2 \times 7 = 2$

$7 = 3 \times 2 + \boxed{1}$ gcd

$7 - 3 \times 2 = 1$

$7 - 3(16 - 2 \times 7) = 1$

$7 - 3 \times 16 + 6 \times 7 = 1$

$7 \times 7 - 3 \times 16 = 1$

$7(23 - 1 \times 16) - 3 \times 16 = 1$

$7 \times 23 - 7 \times 16 - 3 \times 16 = 1$

$7 \times 23 - 10 \times 16 = 1$

$7 \times 23 - 10(108 - 4 \times 23) = 1$

$7 \times 23 - 10 \times 108 + 40 \times 23 = 1$

$47 \times 23 - 10 \times 108 = 1$

$47(239 - 2 \times 108) - 10 \times 108 = 1$

$47 \times 239 - 94 \times 108 - 10 \times 108 = 1$

$47 \times 239 - 104 \times 108 = 1 \mod 239$

$-104 \times 108 \equiv 1 \mod 239$

$108^{-1} \equiv -104 \equiv 135 \pmod{239}$

$239 - 104 = 135$

$f(x) = 16x + 13 \mod 35$ encryption

$y = 16x + 13 \mod 35$

$(y - 13) \equiv 16x \mod 35$

Find $16^{-1} \mod 35$

$35 = 2 \times 16 + 3$

$16 = 5 \times 3 + 1$

$\underline{16} - 5 \times \underline{3} = 1$

$16 - 5(35 - 2 \times 16) = 1$

$\underline{16} - 5 \times 35 + \underline{10 \times 16} = 1$

$11 \times 16 - 5 \times 35 = 1 \mod 35$

$11 \times 16 \equiv 1 \mod 35$

$16^{-1} \equiv 11 \mod 35$

$11(y - 13) \equiv 11(16x) \mod 35$

$x \equiv (11y - \underline{\underline{143}}) \mod 35$

$x = 11y + 32 \mod 35$

Decryption $a = 11$, $b = 32$

$35 \times 5 = 175$

$175 - 143 = 32$

Given matching plain cipher chars for affine find key

Cipher F → E Plain

Cipher G → T Plain

find decryption function

- $f(5) = 5a + b = 4 \mod 26$
  $f(6) = 6a + b = 19 \mod 26$

$a = 15 \mod 26$

found a.
backsub find b.

15
Cipher P → E
20 U → T

- $f(15) = 15a + b = 4 \mod 26$
  $f(20) = 20a + b = 19 \mod 26$

$5^{-1} \mod 26$

$21 \times 5a \equiv 15 \times 21 \mod 26$

$a \equiv 3 \mod 26$