CIS 3362 8/26/26

1. Affine Encrypt
2. Requirement to Decrypt
3. How to obtain decryption keys
4. Euclidean Alg.
5. EEA
6. Use 2 letter crypt for break affine
   Cipher (D) = Plain (T), Cipher (Y) = plain (E) example

Shift → $f(x) = x + k$ line w/ slope 1

x ↑ plain, k ↑ key

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

How do I reverse/undo this operation?

CAN I undo this operation?

$a=3 \quad b=4 \quad f(x) = (3x+4) \bmod 26$

PLAIN = "UCF"
↓ ↓ ↓
20 2 5
↓ ↓ ↓
12, 10, 19
M K T

$f(20) \equiv 3(-6)+4$ (26−6)

$\equiv -14$

$\equiv 12 \bmod 26$ M

$\boxed{20 \equiv -6 \bmod 26}$

if $x \equiv y \pmod{26}$

then $f(x) \equiv f(y) \pmod{26}$

provided that f is a polynomial.

~~a ≡ b~~

$x \equiv y \bmod 26$

iff $26 \mid (x-y)$

$f(2) = (3 \times 2 + 4)$

$\equiv 10 \bmod 26$

K

$f(5) = (3 \cdot 5 + 4) = 19$ T

$$f(x) \equiv (3x+4) \mod 26$$

$$x \equiv 3f^{-1}(x)+4 \mod 26$$

$$9\cdot(x-4) \equiv 9\cdot 3f^{-1}(x) \mod 26$$

$$(9x-36) \equiv \underset{=}{\overset{(26+1)}{27}} f^{-1}(x) \mod 26$$

$$f^{-1}(x) \equiv 9x-36 \mod 26$$

$$f^{-1}(x) = \underline{9x+16} \mod 26$$

$\boxed{27 \equiv 1 \mod 26}$

$26 \mid (27-1)$

27

$$\begin{array}{r} 2 \\ 26\overline{)52} \\ -52 \\ \hline 0 \end{array} \quad \boxed{RO}$$

$0 < a < 26$

$0 \leq b < 26$

Where did 9 come from?

How possible keys are there?

Try $a=6$, $b=15$

$f(x) = (6x+15) \mod 26$

Is this okey?

NO REASON: $\gcd(6,26) \neq 1$

$= 2$

greatest common divisor

(NOT INVERTIBLE)

$$f(0) = (6\cdot 0+15) \equiv 15 \mod 26$$

$$f(13) = \underline{6\cdot 13}+15 \equiv 78+15 \equiv 15 \mod 26$$

$$3\cdot(2\cdot 13)+15$$

$$3\cdot \underline{26}$$

$\boxed{\text{\#KEYS: } 12 \times 26 = 312}$

a can be any int from 1 to 25 such that $\gcd(a,26)=1$: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

More generally for an affine cipher on an alphabet with n letters the total # of keys equal $n \cdot \phi(n)$, where $\phi(n)$ is defined as the number of integers a in the set $\{1, 2, 3, \ldots, n\}$ with $\gcd(a, n) = 1$.

Where did I get the 9 from?

Answer: $9 \equiv 3^{-1} \bmod 26$

So ~~the~~ we define $a^{-1} \bmod n$ to be the integer b such that

$$\boxed{a \cdot b \equiv 1 \bmod n}$$

$$a \times a^{-1} \equiv 1 \bmod n$$

Euclid's Algorithm (GCD)

Extended Euclidean Alg (modular inverse)

$$\left.\begin{array}{l} 9 \equiv 3^{-1} \bmod 26 \\ 5 \equiv 21^{-1} \bmod 26 \end{array}\right\} \text{pairs}$$

$$3 \equiv 9^{-1} \bmod 26 \quad \text{etc.}$$

① $\gcd(\underline{162}, \underline{95}) = 1$ ② $95^{-1} \bmod 162$

	q		r

$162 = 1 \times 95 + 67$

$95 = 1 \times 67 + 28$

$67 = 2 \times 28 + 11$

$28 = 2 \times 11 + 6$

$11 = 1 \times 6 + 5$

$6 = 1 \times 5 + \boxed{1}$

$5 = 5 \times 1$

Euclidean Algorithm

$\boxed{11 - 1 \times 6} = 5$

$\boxed{28 - 2 \times 11} = 6$

if $a = b$
then
$a \equiv b \pmod{n}$

won't change

$\underline{6} - 1 \times \underline{5} = 1$ (linear combo 6,5)

$6 - 1(11 - 1 \times 6) = 1$

$6 - 1 \times 11 + 1 \times 6 = 1$

$2 \times \underline{6} - 1 \times \underline{11} = 1$ (linear combo 11,6)

$2(28 - 2 \times 11) - 1 \times 11 = 1$

$2 \times 28 - 4 \times 11 - 1 \times 11 = 1$

$2 \times \underline{28} - 5 \times \underline{11} = 1$ (linear combo 28,11)

$2 \times 28 - 5(67 - 2 \times 28) = 1$

$2 \times 28 - 5 \times 67 + 10 \times 28 = 1$

$12 \times \underline{28} - 5 \times \underline{67} = 1$

$12(95 - 1 \times 67) - 5 \times 67 = 1$

$12 \times 95 - 12 \times 67 - 5 \times 67 = 1$

$12 \times 95 - 17 \times \underline{67} = 1$

$12 \times 95 - 17(162 - 95) = 1$

$12 \times 95 - 17 \times 162 + 17 \times 95 = 1$

$\boxed{29 \times 95 - 17 \times 162 = 1}$

$29 \times 95 - 17 \times 162 \equiv 1 \bmod 162$

$29 \times 95 - \underline{17 \times 0} \equiv 1 \bmod 162$

$29 \times 95 \equiv 1 \bmod 162$

$29 \equiv 95^{-1} \bmod 162$

Lets say we're looking for

$67^{-1} \mod 95$ and get

$$12 \times 95 - 17 \times 67 = 1$$

$$\underline{12 \times 95} - 17 \times 67 \equiv 1 \mod 95$$

$$-17 \times 67 \equiv 1 \mod 95$$

$$67^{-1} \equiv -17 \equiv \boxed{78} \pmod{95}$$

add 95 (modual)