CIS 3362

8/24/22

Shift Cipher

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

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

Math mod

$a \equiv b \pmod{n} \longleftrightarrow n \mid (a-b)$

"n divides evenly into difference of a and b"

$29 \equiv 3 \pmod{26}$
$29 \equiv 55 \pmod{26}$
$29 \equiv x \pmod{26}$ if true for an infinite # of x's.

math mod not a function (equivalence relation)
"adding or subtracting multiples of n will achieve other equivalent mods, mod n"

In programming, mod is a function

$29 \% 26 \Rightarrow 3$

For positive ints, in all languages the answer of a mod is in between 0 and n-1 mod n. (remainder from division)

In C, Java, negative mods work ~~true~~ like this:

$$-7 \% 5 \rightarrow -(7 \% 5)$$
$$= -2$$

$-2 \equiv x \pmod 5$ → want x, $0 \leq x < 5$

$$\boxed{x = 3}$$

In code, if a mod answer goes negative add copies of n, the mod value, until you get a positive value.

$x \% n$ but x might be "very negative"

$$((x \% n) + n) \% n$$

In python, $-7 \% 5 = 3$, so we don't have to adjust for negatives!

Shift

We'll break it by trying all 26 shifts.

* If the keyspace (# of possible keys) is small, then we can just use brute force to break cipher system.

Affine Cipher

Shift $f_k(x) = x + k$ (line slope 1)

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

To encrypt $f_{3,4}(x) = (3x+4) \bmod 26$

Plain	Cipher	
A	$3(0)+4=4$	E
B	$3(1)+4=7$	H
C	$3(2)+4=10$	K
		etc.

(1) how do I decrypt?

(2) can I try all possible values, 0 to 25, for a and b?

Consider $f(x) = (4x+7) \bmod 26$

Would this be okay?

$$f(0) = (4\cdot 0+7) = \cancel{\equiv}\ 7$$
$$f(13) = (4\times 13+7) = 52+7 \equiv 7 \bmod 26$$

Problem 4×13 is a multiple of 26

We can never have ~~4x~~ ax be a multiple of 26 if $0 < x < 26$.

a and 26 have to be relatively prime

$\gcd(a, 26) = 1$

greatest common divisor

$\boxed{\begin{array}{l} a = 1, 3, 5, 7, 9, 11 \\ 25, 23, 21, 19, 17, 15 \end{array}}$

b can be any of 26 values

Key Space Affine $12 \times 26 = 312$

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

how to decrypt?

$x \equiv 3y + 4 \mod 26$ (1) swap x, y

$3y \equiv (x - 4) \mod 26$ [in reg math divide by 3, mod not allowed to divide]

$9(3y) \equiv 9(x - 4) \mod 26$

$27y \equiv 9x - 36 \mod 26$

where did this come from???

$1y \equiv 9x + 16 \mod 26$

because
$27 \equiv 1 \mod 26$
$-36 \equiv 16 \mod 26$

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

goal find a number m such that $m \cdot 3 \equiv 1 \mod 26$

We define m as $3^{-1} \mod 26$.

By def $m \times m^{-1} \equiv 1 \mod n$.

$$m \times (m^{-1} \bmod n) \equiv 1 \bmod n$$

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

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