CIS 3362 8/21/24

1. TA intro
2. Cipher #4
3. Shift + Break Shift
4. Affine
5. Coding w/letters

SHIFT

key = [0, 25]

$f_k(x) = (x+k) \bmod 26$ ARE DIFF ✗ $(x+k) \bmod 26$

$a \equiv b \pmod n \iff n \mid (a-b)$

"n divides evenly into a-b"

expression $a \bmod n$ is evaluated as the remainder when a is divided by n, provided that a, n & are positive.

NEGATIVES WORK WEIRD

↳ Char mappings don't work w/negatives

Decrypt undo the operation

$$y = (x + k) \mod 26$$

$$(y - k) = x \mod 26$$

$$f_k^{-1}(c) = (c - k) \mod 26$$

↑ in code we do +26

To break it we'll just use brute force: try all 26 keys + see what makes sense.

CAT

2, 0, 19 key = 7

+7 +7 +7

9, 7, 26

9, 7, 0

JHA

9 7 0

+19 +19 +19

28, 26, 19

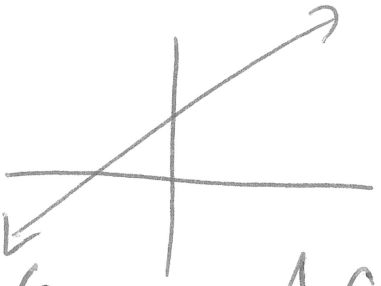
2, 0, 19

CAT ✓

encryption key = 7

not 19

$f(x) = x + k$



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

Affine Cipher

$a = 5, \quad b = 18$

$f(x) = 5x + 18$

PLAINTEXT

KNIGHTS

10, 13, 8, 6, 7, 19, 18

$f(10) = 5(10)+18 = 68 \rightarrow 16$ Q

$f(13) = 5(13)+18 = 83 \rightarrow 5$ F

$f(8) = 5(8)+18 = 58 \rightarrow 6$ G

$f(6) = 5(6)+18 = 48 \rightarrow 22$ W

$f(7) = 5(7)+18 = 53 \rightarrow 1$ B

$f(19) = 5(19)+18 = 113 \rightarrow 9$ J

$f(18) = 5(18)+18 = 108 \rightarrow 4$ E

In Shift it was easy to decrypt.
How do we undo this operation?

$y = (5x + 18) \mod 26$

$y - 18 = 5x \mod 26$

You can't divide a mod equiv.

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

$21y - 18 \times 21 = 105x \mod 26$

$21y - 378 = 105x \mod 26$

$21y - 378 = x \mod 26$

$21y + 12 = X \mod 26$

$105 \equiv 1 \mod 26$

$-378 \equiv 12 \mod 26$

To decrypt use $a = 21$, $b = 12$

$Q = 16 \quad 21 \times 16 + 12 = 336 + 12$

$= 348$

$\equiv 10 \mod 26$ K

Will "magic" always work for all pairs of encryption keys (a, b)

$a \neq 0$

$\gcd(a, 26) = 1$

$f(x) = (13x + 5) \mod 26$

$f(0) = 5$

$f(1) = 18$

$f(21) = 13 \cdot 2 + 5 = 31 \equiv 5 \mod 26$

each letter must encrypt into a unique ciphertext letter.

if $x \neq y$, then $f(x) \neq f(y)$.

encryption is applying some function f

decryption is the inverse function (undoing the transformation of f)

$$f(x) = (13x + 5) \bmod 26$$

$$f(x) = (4x + 5) \bmod 26$$

↓

even though 4 doesn't divide into 26, 2 divides into both, so

$f(0) = f(13)$

13 and 26 share a common factor of 13

$$13 \times \left(\frac{26}{13}\right) = 26$$

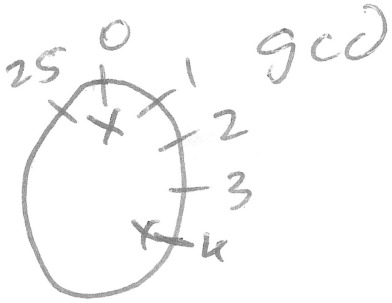
2

$f(0) = 4 \times 0 + 5$

$f(13) = 4 \times 13 + 5$

$2 \times 2 \times 13$

2×26



All valid affine keys are

a s.t. $\gcd(a, 26) = 1$ [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]

b can be anything

TOTAL # KEYS = $12 \times 26 = 312$