SHIFT CIPHER

Plaintext = reg msg
Ciphertext = encoded msg

Key is used to generate ciphertext from Plaintext.

$f(P, k) = C$

f is the cipher being used

$f^{-1}(C, k) = P$

In this system, we assume k is secret!

'A' to 'Z' encoded as 0 to 25

$f(P, k) = (P + k) \mod 26$ [SHIFT]

(Intuitively to reduce something mod n, we add or subtract copies n until we get a int in the range $[0, n-1]$.)

$f^{-1}(C, k) = (C - k) \mod 26$

EXAMPLE: KNIGHTS Plain

10, 13, 8, 6, 7, 19, 18
+12 12 12 12 12 12 12 Key = 12

WZUSTFE 22, 25, 20, 18, 19, 31, 30

In math,

$-7 \equiv 19 \pmod{26}$

(add 26 to -7)

but computer, if we get a negative, it stays negative, so you have to manually add 26.

AFFINE CIPHER

~~$f(P, k)$~~

The keys in affine is an ordered pair (a, b).

$f(P, (a,b)) = (aP + b) \bmod 26$

EXAMPLE $a = 3$, $b = 2$

PLAIN: CAMERA

2, 0, 12, 4, 17, 0

$f(2) = 3(2) + 2 = 8$

$f(0) = 3(0) + 2 = 2$

$f(12) = 3(12) + 2 = 38 \equiv 12 \pmod{26}$

$f(4) = 3(4) + 2 = 14$

$f(17) = 3(17) + 2 = 53 \equiv 1 \pmod{26}$

ICMOBC

What are the valid values of a and b?

Does $a=4, b=3$ work 8/25/21 ③

$f(p) = (4p+3) \bmod 26$

$f(0) = 4 \cdot 0 + 3 = 3$

$f(13) = 4 \cdot 13 + 3 = 55 \equiv 3 \bmod 26$

A encrypts to D

N encrypts to D

OOPS!

We don't want ap to be a multiple of 26. This can only happen if $\gcd(a, 26) = 1$.

Valid keys for affine:

b $(0 \le b \le 25)$

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

# of valid keys $= 12 \times 26 = 312$

What about an alphabet size of 30

$b (0 \le b \le 29)$

$a (\gcd(a, 30) = 1,$
$1, 7, 11, 13, 17, 19, 23, 29$

keys $= 8 \times 30 = 240$

If I know the encryption key for affine, how do I get the decryption key?

$$f(p) = (3p+2) \mod 26$$

$$x \equiv (3y+2) \mod 26$$

$$(x-2) \equiv 3y \mod 26$$

In real #s, I divide by 3. But under I can't do that... INSTEAD MAGIC!

$$9(x-2) \equiv 9(3y) \mod 26$$

$$9x-18 \equiv 27y \mod 26$$

$$9x-18 \equiv y \mod 26$$

$$y \equiv 9x-18 \mod 26$$

$$y \equiv 9x+8 \mod 26$$

Decryption keys are $a=9, b=8$