## Shift

$$f(x,k) = (x+k) \% 26$$
$$f^{-1}(x,k) = (x-k+26) \% 26$$

---

## Affine Cipher

$A=0, B=1, \ldots Z=25$

$$f(x) = (3x+7) \% 26$$

"HOME"
7, 14, 12, 4

$f(7) = (3 \cdot 7+7) \% 26 = 2$ C
$f(14) = (3 \cdot 14+7) \% 26 = 23$ X
$f(12) = (3 \cdot 12+7) \% 26 = 17$ R
$f(4) = (3 \cdot 4+7) \% 26 = 19$ T

Keys = a, b $\quad f(x) = (ax+b) \% 26$

| Plain | Cipher |
|---|---|
| A | H |
| B | K |
| C | N |
| ↓ | ↓ |

$y = (3x+7)$

$x = (3y+7)$ ① flip x, y

$\frac{x-7}{3} = y$ ② solve y

* How do we divide in "mod world"?

Of all possible values of a and b, which ones are valid?

$$f(x) = (2x+3) \% 26$$
$$f(0) = (2(0)+3) \% 26 = 3$$
$$f(13) = (2(13)+3) \% 26 = 3$$

A → D
N ↗

Encryption function is valid <u>iff</u>

~~two~~ there is no case where 2 different inputs map to the same output.

(function must be invertible.)

b can be any of the 26 possible values.

But a is restricted!

↳ a can't be a factor of 26.

$$f(x) = (4x+7) \% 26$$
$$f(0) = (4(0)+7) \% 26 = 7$$
$$f(13) = (4(13)+7) \% 26 = 7$$

Fancy name 26 and a must be coprime

~~Great~~ Greatest Common Divisor of 26 and a but equal 1.

$\boxed{\text{Valid a's: } 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}$

↓ 12 valid values

~~Max # k~~ Total possible # keys $= 12 \times 26 = 312$

Consider Affine Cipher on an alphabet of 35 letters. How many possible keys are there?

total $= 24 \times 35$

$\# b = 35$

$\# a =$ can't have: 5, 10, 15, 20, 25, 30, ~~35~~ 0

7, 14, 21, 28

$35 - 11 = 24$

$$y \equiv (3x+7) \bmod 26$$

$$x \equiv (3y+7) \bmod 26$$

$$x-7 \equiv 3y \bmod 26$$

if $a \equiv b \bmod n$, then $ca \equiv cb \bmod n$.

$$9(x-7) \equiv 9(3y) \bmod 26$$

$$9x-63 \equiv 27y \bmod 26$$

$$27y \equiv (9x-63) \bmod 26$$

$$1y \equiv (9x-63) \bmod 26$$

+78 (is okay) 3·26

In mod eqn, I can substitute a for b if $a \equiv b \bmod n$.

↳ for additive + multiplicative factors

$$\boxed{y \equiv (9x+15) \bmod 26}$$

↳ Decryption function

if math, $a \equiv b \pmod{n} \iff n \mid (a-b)$

| divisible

a−b is divisible by n.

## Modular Inverse

$a^{-1} \bmod n$ is the modular inverse of $a \bmod n$, specifically,

$$a \times (\underline{a^{-1} \bmod n}) \equiv 1 \bmod n.$$

modular inverses are only defined if $\gcd(a,n)=1$.

17, 19, 23

| mod 26 |
|---|
| $1 \leftrightarrow 1$ |
| $3 \leftrightarrow 9$ |
| $5 \leftrightarrow 21$ |
| $7 \leftrightarrow 15$ |
| $17 \leftrightarrow 23$ |
| $11 \leftrightarrow 19$ |
| $25 \leftrightarrow 25$ |

8/28/19 4

| Plain | | Cipher |
|---|---|---|
| 4 E | $\rightarrow$ | T 19 |
| 7 H | $\rightarrow$ | C 2 |

$f^{-1}(x) = (ax + b) \bmod 26$

$$
\begin{array}{rl}
f^{-1}(19) = (19a + b) & \equiv 4 \bmod 26 \\
- \; f^{-1}(2) = (2a + b) & \equiv 7 \bmod 26 \\
\hline
17a & \equiv -3 \bmod 26
\end{array}
$$

$19 - 2 = 17$

$19(9) + b \equiv 4 \bmod 26$

$171 + b \equiv 4 \bmod 26$

$b \equiv -167 \bmod 26 \quad (+182)$

$\boxed{b \equiv 15 \bmod 26}$

$23(17a) \equiv 23(-3) \bmod 26$

$a \equiv -69 \bmod 26$

$+78$

$\boxed{a \equiv 9 \bmod 26}$

130

156

26

Cryptanalysis - using information, patterns, to reduce total # of keys we search.