**Shift**

\[
f(x, k) = (x + k) \mod 26 \\
\]

\[
f^{-1}(x, k) = (x - k + 26) \mod 26 \\
\]

---

**Affine Cipher**

\[
f(x) = (3x + 7) \mod 26 \\
\]

"HOME"

7, 14, 12, 4

\[
f(7) = (3 \cdot 7 + 7) \mod 26 = 2 \\
f(14) = (3 \cdot 14 + 7) \mod 26 = 23 \\
f(12) = (3 \cdot 12 + 7) \mod 26 = 17 \\
f(4) = (3 \cdot 4 + 7) \mod 26 = 19 \\
\]

Keys = a, b

\[
f(x) = (ax + b) \mod 26 \\
\]

\[
y = (3x + 7) \\
\]

\[
x = (3y + 7) \quad \text{① flip } x, y \\
\]

\[
x - 7 \mod 3 = y \\
\]

\[
\frac{x - 7}{3} = y \\
\]

**How do we divide in "mod world"?**

---

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

\[
f(x) = (2x + 3) \mod 26 \\
\]

\[
f(0) = (2(0) + 3) \mod 26 = 3 \\
f(13) = (2(13) + 3) \mod 26 = 3 \\
\]

\[
A \rightarrow D \\
N \rightarrow W \\
\]
Encryption function is valid iff 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.
\[
\begin{align*}
  f(1) &= (4(1) + 7) \mod 26 = 7 \\
  f(2) &= (4(2) + 7) \mod 26 = 3 \\
  f(3) &= (4(3) + 7) \mod 26 = 7
\end{align*}
\]

Fancy name 26 and a must be coprime.

Greatest Common Divisor of 26 and a must equal 1.

Valid a's: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

12 valid values

Total possible # keys = 12 \times 26 = 312

Consider Affine Cipher on an alphabet of 35 letters. How many possible keys are there?
\[
\text{total} = 24 \times 35
\]

# b = 35

# a = can't have: 5, 10, 15, 20, 25, 30, 35
7, 14, 21, 28

35 - 11 = 24
\[ y = (3x + 7) \mod 26 \]
\[ x = (3y + 7) \mod 26 \]
\[ x - 7 \equiv 3y \mod 26 \]
\[ 9(x - 7) \equiv 9(3y) \mod 26 \]
\[ 9x - 63 \equiv 27y \mod 26 \]
\[ 27y \equiv (9x - 63) \mod 26 \]
\[ 1y \equiv (9x - 63) \mod 26 + 78 (\text{is okay}) 3 \cdot 26 \]
\[ y \equiv (9x + 15) \mod 26 \]

Decryption function

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

\( 1 \) divisible

\( a - b \) is divisible by \( n \)

Modular Inverse

\( a^{-1} \mod n \) is the modular inverse of \( a \mod n \), specifically,

\[ a \times (a^{-1} \mod n) \equiv 1 \mod n. \]

Modular inverses are only defined if \( 9 \gcd(a,n) = 1 \).  \( 17, 19, 23 \)
Plain

4 → T
7 → C

Cipher

T 19
C 2

\[ f^{-1}(x) = (ax + b) \mod 26 \]

\[ f^{-1}(19) = (19a + b) \equiv 4 \mod 26 \]

\[ f^{-1}(2) = (2a + b) \equiv 7 \mod 26 \]

\[ 17a \equiv -3 \mod 26 \]

\[ 19(9) + b \equiv 4 \mod 26 \]

\[ 23(17a) \equiv 23(-3) \mod 26 \]

171 + b ≡ 4 \mod 26

\[ b \equiv 15 \mod 26 \]

\[ 19(9) + b \equiv 4 \mod 26 \]

\[ a \equiv -69 \mod 26 \]

\[ a \equiv 9 \mod 26 \]

130

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