Shift Cipher

\[ f_k(x) = (x + k) \mod 26 \]

\[ f_k^{-1}(x) = (x - k) \mod 26 \]

Math mod

\[ a \equiv b \pmod{n} \quad \leftrightarrow \quad n \mid (a-b) \]

"\( n \) divides evenly into difference of \( a \) and \( b \)"

\[ 29 \equiv 3 \pmod{26} \]

\[ 29 \equiv 55 \pmod{26} \]

\[ 29 \equiv x \pmod{26} \quad \text{is true for an infinite # of} \ x \text{es.} \]

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 like this:

\[-7 \% 5 \rightarrow - (7 \% 5) = \neg \]

\[-2 \equiv x \pmod{5}\] want \(x\) with \(0 \leq x < 5\)

\[
\underline{x = 3}
\]

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

\[\text{if } x < 0 \Rightarrow x \rightarrow (x + n) \pmod{n}\]

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

\[\underline{Shift}\]

We'll break it by trying all 26 shifts.

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

Shift \( f(x) = x + k \) (line slope 1)

\[ f_{a,b}(x) = (ax + b) \mod 26 \]

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

<table>
<thead>
<tr>
<th>Plain</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3(0)+4=4 E</td>
</tr>
<tr>
<td>B</td>
<td>3(1)+4=7 H</td>
</tr>
<tr>
<td>C</td>
<td>3(2)+4=10 K</td>
</tr>
</tbody>
</table>

etc.

(1) how do I decrypt?

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

Consider \( f(x) = (4x + 7) \mod 26 \)

Would this be okay?

\[
\begin{align*}
  f(0) &= (4 \cdot 0 + 7) = 7 \\
  f(13) &= (4 \cdot 13 + 7) = 52 + 7 = 7 \mod 26
\end{align*}
\]

Problem \( 4 \cdot 13 \) is a multiple of 26

We cannot have \( ax \) be a multiple of 26 if \( 0 \leq x \leq 26 \).
\( a \) and \( 26 \) have to be relatively prime
\[ \gcd (a, 26) = 1 \]
\( \text{gcd: greatest common divisor} \)
\( a = 1, 3, 5, 7, 9, 11, 25, 23, 21, 19, 17, 15 \)
\( b \) can be any of 26 values

Key Space Affine \( 12 \times 26 = 312 \)

\[ f(x) = (3x+4) \mod 26 \]
how to decrypt?

\[ x \equiv 3y + 4 \mod 26 \]
\[ 3y \equiv (x-4) \mod 26 \]
\[ q(3y) \equiv q(x-4) \mod 26 \]
\[ 27y \equiv 9x - 36 \mod 26 \]

\[ 1y \equiv 9x + 16 \mod 26 \]

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

where did this come from??

\[ \text{goal: find a number } y \text{ such that } m \cdot 3 \equiv 1 \mod 26 \]

We define \( m \) as \( 3^{-1} \mod 26 \).
By def \( m \cdot m^{-1} \equiv 1 \mod n \).
\[ m \times (m^{-1} \mod n) \equiv 1 \mod n \]

\[ 3^{-1} \equiv 9 \mod 26 \]

\[ 5^{-1} \equiv 21 \mod 26 \]