Shift Cipher

A = 0, B = 1, C = 2, ..., Z = 25

Encryption and decryption are functions of the message and the key.

\[ f_k(m) = (m + k) \mod 26 \%

\[ t = 19, \ k = 17 \quad (19 + 17) \mod 26 \]

\[ = 36 \mod 26 \]

\[ = 10 \quad \text{(value in blue 0 and 25)} \]

\[ d_k(c) = (c - k) \mod 26 \]

\[ 10 - 17 \mod 26 \]

\[ -7 \mod 26 \]

\[ 19 \mod 26 \]

\[ (c - k + 26) \mod 26 \]
Affine Cipher

Keys: $a, b$

$e_{a,b}(m) = (am + b) \mod 26$

$a = 7, \ b = 4, \ m = 'J' = 9$

$e_{7,4}(9) = (7\times 9 + 4) \mod 26$

$= 67 \mod 26$

$= 15$ \rightarrow P$

If $a$ is 0, $e(m) = 0 + b = b$

<table>
<thead>
<tr>
<th>Plain</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>20</td>
</tr>
</tbody>
</table>

If 2 letters encrypt to the same ciphertext letter, there is NO way to decrypt reliably!

Encryption function MUST BE one-to-one (injection)
What are possible values for $a$?

$2, 3, 5, 7, 11, 13, 17, 19, 23$

two of these don't work...

2 and 13 because they are factors of 26.

$\text{gcd}(a, 26) = 1$.

Shift cipher is a special case of the affine with $c = 1$.
$a$ and $b$ are relatively prime, if and only if $\text{gcd}(a, b) = 1$.

$a = 2$  $f(m) = (2m + b) \mod 26$

$a = 8$  $f(m) = (8m + b) \mod 26$

$m = 3, m = 16$

$f(3) = (2 \times 3 + b) \mod 26$

$f(16) = (2 \times 16 + b) \mod 26$

$= (32 + b) \mod 26$
So, the possible values of $c$ are:

$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$

An affine cipher has $12 \times 26$ cipher keys = 312 possible keys.

\[
E_{a,b}(m) = (am + b) \mod 26
\]

\[
C = (am + b) \mod 26
\]

\[
C - b = am \mod 26
\]

$C - b$ might not equal $am$ when $C$ and $am$ are modeled by 26. They just both give the same remainder when modeled by 26.

You can't divide a mod equation on both sides but you can multiply both sides.

\[
C = (5 \times (5 - 4) - 17) \mod 26 \implies 9 \mid 5
\]
**Affine Cipher**

\[ e_{7,4}(m) = (7m + 4) \mod 26 \]

If \( J = 9 \), \( e_{7,4}(9) = (7 \cdot 9 + 4) \mod 26 \)

\[ = 67 \mod 26 \]

\[ = 15 \mod 26 \]

Where did this come from?

\[ C = 7m + 4 \mod 26 \]

\[ (C - 4) = (15 \cdot 7m) \mod 26 \]

\[ 15C - 60 = 105m \mod 26 \]

\[ m = 15C - 60 \mod 26 \]

\[ m = (15C + 18) \mod 26 \]

Decryption function is \( f(c) = (15c + 18) \mod 26 \)

Problem I want to solve is as follows:

for any value \( a \), what value \( a' \) exists such that \( a \cdot a' \equiv 1 \mod 26 \).

We call \( a' \) \( a^{-1} \mod 26 \).

\[ 7^{-1} \equiv 15 \mod 26 \]
In general, we want an algorithm, given \( a \) and \( n \) (positive ints), which determines \( a^{-1} \mod n \), if it exists.

\[ 3^{-1} \mod 15 \text{ DOES NOT EXIST!} \]
\[ 6^{-1} \mod 15 \text{ DOES NOT EXIST!} \]

\( a^{-1} \mod n \) exists if and only if \( \gcd (a, n) = 1 \). (Greatest Common Divisor)

\( n=26, \ a=7 \)

### Euclidean Algorithm

#### A.
\[ 26 = 3 \times 7 + 5 \]

#### B.
\[ 7 = 1 \times 5 + 2 \rightarrow 7 - 1 \times 5 = 2 \]

#### C.
\[ 5 = 2 \times 2 + 1 \]
\[ 2 = 2 \times 1 \]

### Extended Euclidean

While last step (C), backwards:

\[ 5 - 2 \times 2 = 1 \]

Use equation B to substitute for the smaller of the underlined values

\[ 5 - 2 \times (7 - 1 \times 5) = 1 \]

\[ 5 - 2 \times 7 + 2 \times 5 = 1 \]

Simplify

\[ 3 \times 5 - 2 \times 2 = 1 \]

\[ 3 \times (26 - 3 \times 7) - 2 \times 7 = 1 \]

\[ 3 \times 26 - 9 \times 7 - 2 \times 7 = 1 \]
\[\frac{3 \times 26}{-11 \times 7} \equiv 1 \mod 26\]
\[-11 \times 7 \equiv 1 \mod 26\] 8/26 ③
\[15 \times 7 \equiv 1 \mod 26\]
\[7^{-1} \equiv 15 \mod 26\]

<table>
<thead>
<tr>
<th>Value</th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>17</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inverse mod 26</td>
<td>1</td>
<td>9</td>
<td>21</td>
<td>15</td>
<td>19</td>
<td>23</td>
<td>25</td>
</tr>
</tbody>
</table>
Find $S3^{-1} \mod 198$

$198 = 3 \times S3 + 39$

$S3 = 1 \times 39 + 14$

$39 = 2 \times 14 + 11$

$14 = 1 \times 11 + 3$

$11 = 3 \times 3 + 2$

$3 = 1 \times 2 + 1$

$2 = 2 \times 1$

$3 - 1 \times 2 = 1$

$3 - 1 \times (11 - 3 \times 3) = 1$

$3 - 1 \times 11 + 3 \times 3 = 1$

$4 \times 3 - 1 \times 11 = 1$

$4(14 - 1 \times 11) - 1 \times 11 = 1$

$3 \text{ steps...}$

$4 \times 14 - 5 \times 11 = 1$

$4 \times 14 - 5 \times (39 - 2 \times 14) = 1$

$4 \times 14 - 5 \times 39 + 10 \times 14 = 1$

$14 \times 14 - 5 \times 39 = 1$

$14(53 - 1 \times 39) - 5 \times 39 = 1$

$14 \times 53 - 19 \times 39 = 1$

$14 \times 53 - 19(198 - 3 \times 53) = 1$

$14 \times 53 - 19 \times 198 + 57 \times 53 = 1$

$71 \times 53 - 19 \times 198 = 1 \mod 198$

$71 \times 53 \equiv 1 \mod 198$

$53^{-1} \equiv 71 \mod 198$