Substitution Cipher

Shift, Affine:
One-to-one functions with domain and range
\[ \mathbb{Z}, \mathbb{Z} \]
Shift \( f_k(x) = (x + k) \mod 26 \)
Affine \( f_{a,b}(x) = (ax + b) \mod 26 \)

Another way to define a function is to explicitly list each output for each input!
(Not only do this if there aren't too many inputs)

<table>
<thead>
<tr>
<th>Plain</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Q</td>
</tr>
<tr>
<td>B</td>
<td>R</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>Z</td>
</tr>
<tr>
<td>E</td>
<td>B</td>
</tr>
</tbody>
</table>

Each letter must appear exactly once!!!

Shift key size = 26
Affine key size = 312
Key size = 26!

NOT FEASIBLE TO DO A BRUTE FORCE SEARCH!!!
<table>
<thead>
<tr>
<th>Pro</th>
<th>Substitution</th>
<th>Large keypace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shift/Affine</td>
<td>easy to implement</td>
<td></td>
</tr>
<tr>
<td>Con</td>
<td>Small keypace</td>
<td>harder to implement (probably need a chart)</td>
</tr>
</tbody>
</table>

Hiding the fact that you've sent a message is **steganography**.

**Substitution cipher was used**

as well, just in case!!!

Queen Elizabeth's Cipher Person: Francis Walsingham

Some words are really common (**the**, etc.)

**CODE SYMBOLS** for 20 common words:

- **The** - \( \Delta \) 26 letters + 20 symbols (harder) 3/4 null chars

**Other Things to Make Harder**

- **NULL CHAR** (doesn't count)
- **BACKSPACE CHAR**
How did Walsingham Break the Code?

1. Frequency Analysis
   - Calculate all letter frequencies
   - 1st 5 or so probably map to the 1st 8 or so from regular English frequencies

2. Common Di, Tri grams
   - Try to match repeated di-tri grams in the ciphertext to common ones in English.
   - Plug in ideas and see if "impossible" conditions are created, or if a partial word forms.

3. Repeated Words
   - Match "mold" of word to dictionary. $X F X X Z = \text{daddy}$