Affine, Shift
Substitution, Vigenère - Monoalphabetic

breakable in 19th century

Codemakers ⇒ Polyalphabetic

Playfair Cipher
- need to implement by hand
- encrypt more than 1 letter at a time

Keyword: "PROBLEMS" // BOKKEPR

<table>
<thead>
<tr>
<th>Y</th>
<th>W</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>T</td>
<td>Q</td>
</tr>
<tr>
<td>N</td>
<td>K</td>
<td>R</td>
</tr>
<tr>
<td>S</td>
<td>M</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>L</td>
<td>B</td>
</tr>
<tr>
<td>O</td>
<td>R</td>
<td>P</td>
</tr>
</tbody>
</table>

PROBLE
EMSAC
DFGHIJ
KNQTV
WXYZ

1. Split into digraphs
2. Look for doubles (aa, bb, etc.)
   → Insert a padding char. (Q) - as needed left to right.

SHE WENT TO THE STORE

SH EW EN IT OT HE ST OR E

1. If 2 letters are on the same row,
   each encrypts to its neighbor to the right, using wrap-around.

2. If 2 letters are on the same col,
   each encrypts to its neighbor below,
   using wrap-around.

3. Box Rule
How to break Playfair?

1. Much easier if you have a little matching plain/cipher text.

Plain: ASAMPLE
Ciphertext: PKJKMKME
Can't be Playfair

Plain: ASAMPLE
Ciphertext: EWOWQNB

Some row col box? Some row col box