CIS3362  9/10/2021

1. Quizzes Still Being Graded - Returned Monday
2. Playfair Cipher
   - Old stuff monoalphabetic
   - Why not "group" letters at a time to encrypt? (Polyalphabetic)
3. Process 2 letters at a time.
4. Easy to do by hand!
   Secret key word: MILLENNIAL

\[
\begin{bmatrix}
M & E & L & E & N \\
A & B & C & D & F \\
G & H & K & O & P \\
Q & A & S & T & U \\
V & W & X & Y & Z
\end{bmatrix}
\]

For each pair of letters, find them in the key and replace with the corresponding letters in the table.

MESSAGE:  I WENT TO THE STORE

Box: Use opposite corners, with letter on the same row or column.
Some: Replace each letter with the one below it, using wrap around.
Some row: Replace each letter with the letter on the right, wrap around.
Identifying factors

1. No double letters in digraph spots
2. Even length

Harder than past ciphers

Clearly frequency info by letter is destroyed, frequency of digraphs is preserved but you need way more of this to set good patterns.

Playfair - pretty hard w/ciphertext only

Here's small amount of matching plain/cipher text:

<table>
<thead>
<tr>
<th>A</th>
<th>S</th>
<th>L</th>
<th>B</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>W</td>
<td>D</td>
<td>W</td>
<td></td>
</tr>
</tbody>
</table>

```
A D E
W M S
D A E
m w s
```