Transposition

1) Key a number
2) Rail fence
3) Triangular
4) Permutation
5) Column Perm
6) Double Trans

Permutation (Spillman book)

Key = [3, 6, 2, 1, 5, 4]

Plain: TODAY IS WEDNESDAY XX

Cipher: ADTIYO DESENW YASXXD

To break: guess block size

ADTIYO
DESENW
YASXXD
Column Permutation

Keyword: UMBRELLA

Assign a perm based word

Sort letters in alpha order + label

Ties → left to right

Write plain row by row

<table>
<thead>
<tr>
<th>8 6 2 7 3 4 5</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEALREAD</td>
<td></td>
</tr>
<tr>
<td>YOUERVED</td>
<td></td>
</tr>
<tr>
<td>THISIDEA</td>
<td></td>
</tr>
<tr>
<td>WHENWEASA</td>
<td></td>
</tr>
<tr>
<td>WADFGVX</td>
<td></td>
</tr>
</tbody>
</table>

Cipher: DDAAOIIEOERIEWGEDRDEV

AEESX ECHHA LVSNFE WYTUN

How to decrypt:

Write key: \( \lfloor 39/6 \rfloor = 5 \) long columns,

# chars = 39 \( \lfloor 39/6 \rfloor = 7 \Rightarrow 1 \) short column

\( \text{last column} \)

<table>
<thead>
<tr>
<th>8 6 2 7 3 4 5</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEALREAD</td>
<td></td>
</tr>
<tr>
<td>YOUERVED</td>
<td></td>
</tr>
<tr>
<td>THISIDEA</td>
<td></td>
</tr>
<tr>
<td>WHENWEASA</td>
<td></td>
</tr>
<tr>
<td>WADFGVX</td>
<td></td>
</tr>
</tbody>
</table>

Compute this col we have 4 letters. I read the 1st 4 letters but write them down column
QUIZ TOPICS

0) Playfair
1) ADFGVX  AID: calculator

2) Hill Cipher
   - encrypt
   - get decryption key given encryption
   - setting up equations for matching
     plain/cipher attack

3) Enigma
   - counting # rotor settings
   - ?

4) Navajo
   - ?

5) Transposition
   - column perm  encrypt or
   - perm  decrypt w/key
   - what index a character will
     end up in.

Code Notes

write msg in grid reg way

\[
\begin{bmatrix}
\begin{array}{ccc}
\text{p}\{0\} & \text{p}\{1\} & \text{p}\{2\} \\
\text{p}\{3\} & \text{p}\{4\} & \text{p}\{5\}
\end{array}
\end{bmatrix}
\]

find column 0

\[
\begin{bmatrix}
\begin{array}{c}
0 \rightarrow 7 \\
2 \rightarrow 6 \\
\end{array}
\end{bmatrix}
\]

we stored 7, 5, 1, 6, 2, 3, 4, 0