Week 5 Thursday

Ideas

Introduce yourself to your neighbor(s) if needed. Then discuss:

We're about half way through the quarter! What do you think are some of the most interesting and/or important ideas we've encountered in the class so far? Brainstorm a few things with your neighbors!

G-Tests, Breaking Rectangular Transposition

1. Suppose you have just intercepted a ciphertext with 10000 characters that was encrypted using rectangular transposition. How many periods might you have to guess?

(A) 2

(B) 4

(C) 8

(D) None of the above

2. Suppose that, when trying to codebreak some ciphertext that was encrypted using rectangular transposition, you make a guess for the period and find the following "*G* box."

$$\begin{bmatrix} \infty & 2449.8 & 1184.1 & 2572.5 & 1263.3 & 2465.9 \\ 1226.4 & \infty & 2500.9 & 1393.9 & 2688.2 & 2531.3 \\ 2391.8 & 2542.1 & \infty & 2376.1 & 2506.3 & 2342.5 \\ 2646.2 & 1249.5 & 2424.9 & \infty & 2524.8 & 1162.5 \\ 2571.5 & 2492.5 & 2597.8 & 2485.5 & \infty & 2300.3 \\ 2360.4 & 2417.6 & 2431.6 & 2372.1 & 2175.2 & \infty \end{bmatrix}$$

Does it seem like you've guessed the right period?

(A) Yes

(B) No

3. Suppose that, when trying to codebreak some ciphertext that was encrypted using rectangular transposition, you find a "G box" that looks as follows, where ! indicates an entry that is much smaller than every other entry on the same row:

$$\begin{bmatrix} . & . & ! & . & . \\ . & . & . & ! & . \\ . & ! & . & . & . \\ . & . & . & . & . \\ ! & . & . & . & . \end{bmatrix}$$

Use the decrypting permutation suggested by this "G box" to decrypt the ciphertext `ATRHE`.

4. Some time ago, you intercepted some ciphertext that was encrypted using rectangular transposition. In your notebook, you wrote down that the “G box” for the correct period looked something like this:

$$\begin{bmatrix} \infty & 1918.5 & 2013.8 & 2068.5 & 433.2 \\ 2068.7 & \infty & 1711.6 & 485.2 & 1961.2 \\ 1884.4 & 1914.7 & \infty & 2035.6 & 2186.3 \\ 505.9 & 2243.6 & 1997.7 & \infty & 2163.7 \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \end{bmatrix}$$

You inadvertently smudged the ink on the last line and can’t read it anymore, but you’ve just intercepted a new ciphertext that you know was encrypted using the same key as the last one. The new ciphertext reads `ACMHSDOOFOYMEQE`. What is the plaintext?