Kryptos 2: Challenge 3-Solution

The diary holds a few clues as to the method used by Gordon to encipher her "newsletter". Her 1/15 entry mentions that she plans on "dusting off [her] old math book", indicating that the cipher may be mathematical. The most obvious clue is the odd phrase "Jack and Jill went up the ...". This brings to mind "HILL". Perhaps she is using a Hill cipher. Since the diary entries containing the ciphertext are in groups of three, one may guess that she is using a 3×3 matrix to implement the standard Hill cipher. So the "key" will be either the nine entries of the matrix used to encipher or the nine entries of the inverse matrix that is needed to decipher. On 1/19 Gordon also mentions that her "clients" don't have to memorize much more than a long distance phone number (which would be 10 digits). The same diary entry also supports the assumption that she is only enciphering the 26 letters of the alphabet. We will assume that she has already made a simple substitution according to a - 0, b - 1, ..., z - 25 and has grouped her plaintext into blocks of three which will be represented as vectors, P. We will also assume that she has created a 3×3 matrix A used for enciphering:

$$\begin{aligned}\text{ciphertext block} = C &= AP \\ &= \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} P\end{aligned}$$

where all arithmetic will be carried out mod 26.

Ms. Gordon's biggest mistake is probably the whimsical header for the 1/30 entry. All of her diary entries begin with the phrase "Dear Diary". On 1/30 she also starts with a nine letter phrase with the first and fifth letters capitalized. If we assume this is the ciphertext for "Dear Diary", we have the following crib:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 11 \\ 21 \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 17 \\ 3 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 20 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 0 \\ 17 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 11 \\ 19 \end{pmatrix}.$$

Each matrix equation yields three congruences. We group them as follows:

$$\begin{aligned} 3a + 4b + 0c &\equiv 9 \\ 0a + 17b + 24c &\equiv 14 \\ 17a + 3b + 8c &\equiv 21 \end{aligned}$$

$$\begin{aligned} 3d + 4e + 0f &\equiv 11 \\ 0d + 17e + 24f &\equiv 11 \\ 17d + 3e + 8f &\equiv 20 \end{aligned}$$

$$\begin{aligned} 3g + 4h + 0i &\equiv 9 \\ 0g + 17h + 24i &\equiv 19 \\ 17g + 3h + 8i &\equiv 6 \end{aligned}$$

We can begin to solve by forming an augmented matrix for each system of 3 congruences. Since the coefficient matrix is the same for each system, we can put this all together:

$$\left(\begin{array}{ccc|ccc} 3 & 4 & 0 & 9 & 11 & 21 \\ 0 & 17 & 24 & 14 & 11 & 19 \\ 17 & 3 & 8 & 21 & 20 & 6 \end{array}\right)$$

We now row-reduce as much as we can, keeping in mind that we are working mod 26. So, begin by multiplying the first row by $3^{-1} \equiv 9 (\text{mod } 26)$ and the second row by $17^{-1} \equiv 23 (\text{mod } 26)$. The third row can then be replaced by $-17(\text{row I}) + \text{row III}$:

$$\left(\begin{array}{ccc|ccc} 1 & 10 & 0 & 3 & 21 & 7 \\ 0 & 1 & 6 & 10 & 19 & 21 \\ 0 & 15 & 8 & 22 & 1 & 17 \end{array}\right)$$

Now replace the third row with $-15(\text{II}) + \text{III}$:

$$\left(\begin{array}{ccc|ccc} 1 & 10 & 0 & 3 & 21 & 7 \\ 0 & 1 & 6 & 10 & 19 & 21 \\ 0 & 0 & 22 & 2 & 2 & 14 \end{array}\right)$$

Unfortunately, 22 does not have a unique inverse mod 26. However, the last row give us two possibilities each for c, f, and i:

$$\begin{aligned} c &= 6 \text{ or } 19 \\ f &= 6 \text{ or } 19 \\ i &= 3 \text{ or } 16 \end{aligned}$$

The second row of the reduced matrix tells us, among other things, $b + 6c \equiv 10$. Using either $c = 6$ or $c = 19$ yields $b = 0$. Similarly, either choice for f or i yield one possibility for e and h respectively. We have:

$$b = 0; \qquad e = 9; \qquad h = 3.$$

The first row of the reduced matrix yields:

$$a = 3; \qquad d = 9; \qquad g = 3$$

There are, thus, 8 possibilities for matrix A. Using the different possibilities for c, f, and i, the determinants of the eight matrices can be computed mod 26. Four of them have determinants of 14, which is not relatively prime to 26. Assuming that Gordon started with a matrix which is invertible mod 26, these four can be excluded.

Each of the remaining four matrices are invertible mod 26. Their inverses can be computed and applied to the ciphertext messages. Only one will produce meaningful plaintext:

$$A = \begin{pmatrix} 3 & 0 & 6 \\ 9 & 9 & 6 \\ 3 & 3 & 3 \end{pmatrix} \qquad \text{and} \qquad A^{-1} = \begin{pmatrix} 9 & 18 & 24 \\ 17 & 17 & 10 \\ 0 & 17 & 1 \end{pmatrix}.$$

Keeping the capitalization used by Gordon one arrives at:

Issue #1 reads: EIPL and VRS going way upx. PPO and RSH will dropx

Issue #2 reads: Fairly high gains in NOK expected this week. Dump ALXA

The capitalized letters refer to Stocks. Clearly Gordon is giving advice on stocks that she thinks will increase or decrease significantly in value.

Note: Some teams surmised that the three letters between the two groups of capitalized letters on slip 1 represented the plaintext word "and". This extra crib made it a little easier to find the enciphering matrix.