Kryptos 2023 Challenge 2 Solution

The backstory reveals that the cipher used was likely a version of the Playfair cipher where the rules have been modified. The Playfair cipher encrypts pairs of letters using a 5x5 grid where the letters of the alphabet are in order alphabetically, except for a code word at the beginning of the square (I/J are combined in one cell). There are three rules for encryption depending on whether the pair of letters lie in the same **row**, same **column**, or **neither**.

Identifying the cipher rules

The hint in the backstory is that the rules can be found embedded in the classified ads. The letter from Brenda to Billy suggests that the rule to map RG to IW can be found in the ad related to the bicycle. Looking at the part of the text outlined by Eddy, we see a block of 5x5 text in which RG and TA both appear, with R and G in **neither** the same row nor column. This suggests that the rule for two letters not in the same row or column of the 5x5 Playfair grid is to *shift down*.

S E A T A
B **R** A K E
B **I** K E T
T H I N **G**
B I K E **W**

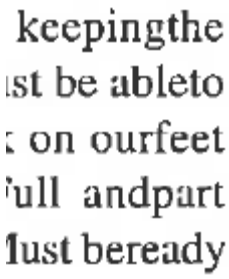
The letter from Brenda to Billy also suggests there are clues in the 2-bedroom apartment ad (VN → OL) and the Warehouse worker ad (GP→ TA).

The 2-bedroom apartment ad has a notation next to a block of text that presumably contains the clue. Indeed, we can find the VN and OL in the block. This gives the rule for two letters in the **same row** (*shift up*).

A P A R T
C **O** U **L** D
I **V** I **N** G
L A R G E
F R O O M

To find the last clue we need to look in the ad for the Warehouse worker. The text to use has not been indicated, but in the other two ads the text used had typos where the spacing between words was omitted. We can identify such a block in the Warehouse ad where we see the letters GP and TA appear.

Kryptos 2023 Challenge 2 Solution



N	**G**	**T**	H	E
B	L	E	T	O
R	F	E	E	T
D	**P**	**A**	R	T
R	E	A	D	Y

The rule for two letters in the **same column** is to *shift right*.

Building the Playfair square

Next, we try to reconstruct the Playfair square. We are given the hint that “Tucson, Arizona” likely appears in the plaintext. If the letters were paired this way

TU CS **ON** AR IZ **ON** A..

then it would follow there is a duplicate pair of letters in the ciphertext with two pairs of letters between. We can see this occurs near the beginning of the ciphertext:

TB BY BH MN XW **VU** GX OP **VU** GC PU TV OI YR BT TV HG BF VZ VD YC

YS BU UZ LO WS

This gives the following plaintext cipher text pairs:

PT	**TU**	**CS**	**ON**	**AR**	**IZ**	**ON**
CT	MN	XW	VU	GX	OP	VU
	1	2	3	4	5	

1. We can use this information to begin to build our Playfair square. Starting with the first plaintext/ciphertext pair (TU → MN) we have three choices for formations in the Playfair square

T				
M		**U**		
		N		

PT letters in neither same row nor column (shift down)

M			**N**	
T			**U**	

PT letters in same row (shift up)

	T	**M**		
	U	**N**		

PT letters in same column (shift right)

Kryptos 2023 Challenge 2 Solution

Since the letters in a Playfair square are alphabetical, if the letters are not in the codeword, the “same row” option makes the most sense since the alphabetic ordering of the letters is preserved. Thus, we proceed based on the assumption that TU are in the same row (and next to each other)

		M	N	
		T	U	

Since there are only 3 spaces between the MN and TU but there are 4 letters (OPQR) we know that one of O,P,Q,R is in our codeword. It is unlikely that Q is in the codeword since U is not (based on this assumption).

- We can conclude that one of O, P, R is in our code word.

2. Our second plaintext/ciphertext pair is CS → XW. Again, we have 3 options:

S				
W		C		
		X		

PT letters in neither same row nor column (shift down)

		W	X	
		S	C	

PT letters in same row (shift up)

	C	X		
	S	W		

PT letters in same column (shift right)

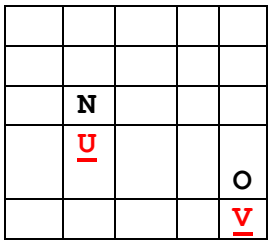
Again, alphabetically, the letters in the “same row” option makes the most. However, if W,X are not in the codeword they likely occur at the bottom of the box so it would look something like this:

	S	C		
	W	X		

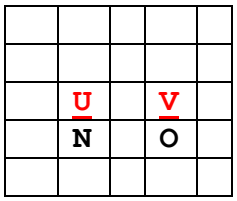
If we add this to our previous square we might fit it in this way (assuming for now that V, X,Y,Z are not in the codeword).

	S	C		
			M	N
			T	U
V	W	X	Y	Z

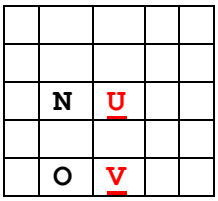
3. Our third PT/CT pair is ON → VU.



PT letters in neither same row nor column (shift down)



PT letters in same row (shift up)



PT letters in same column (shift right)

Only the “neither same row nor column” option fits with our current guess of the square so we will assume that is the situation and update our square.

	S	C		
			M	N
O			T	U
V	W	X	Y	Z

- Note we only have 2 spaces between the O and the T but alphabetically we have PQRS We see that S is in the codeword and we’ve assumed Q is not so that tells us P or R is in the codeword (again consistent with our previous assumption).

4. Our 4th PT/CT pair is AR → GX. If R were above the X in the playfair box, this would make sense alphabetically and also with a “shift down” encryption meaning that A and R are neither in the same row nor column. This would mean A’s location is above G (we will place the R and just keep that in mind)

	S	C		
			M	N
O		R	T	U
V	W	X	Y	Z

5. Our 5th PT/CT pair is IZ →OP

If I and Z were in the same column, then Z would map to V which is incorrect. Also, if our box is correct, I is not in the same ROW as Z thus we must have I and Z in different rows and columns. This means that Z shifts “down” (or in this case wraps around to the top row to put “P” in the top left corner). It also means O is below I giving:

	S	C		P
I			M	N
O		R	T	U
V	W	X	Y	Z

6. Now, there are 2 spaces between I and M and 2 letters alphabetically (since we group I/J) so we can fill in those two spaces:

	S	C		P
I	L	M	M	N
O		R	T	U
V	W	X	Y	Z

7. Since we know A is above G we could try slotting that in where G fits alphabetically:

	S	C	A	P
			G	H
I	L	M	M	N
O		R	T	U
V	W	X	Y	Z

8. By assumption, Q is not in the code word, and we have used S and P so it is the only thing left to put between O and R

	S	C	A	P
			G	H
I	L	M	M	N
O	Q	R	T	U
V	W	X	Y	Z

9. At this point we are missing the following letters: B, D, E, F. Of those, only E makes sense to be at the beginning of the codeword creating ESCAP(E) giving the following completed square:

E	S	C	A	P
B	D	F	G	H
I	L	M	M	N
O	Q	R	T	U
V	W	X	Y	Z

10. Using this square, we can decrypt the remaining cipher text:

    ME ET IN TU CS ON AR IZ ON AX AT MO UN TL EM MO NM IL EP OS TX TW EN TY FI VE:

    MEET IN TUCSON ARIZONA X AT MOUNT LEMMON MILEPOST X TWENTY FIVE.

    The x's in the plaintext were necessary to separate duplicate letters (Playfair cannot encrypt pairs of letters that are the same (e.g. aa or tt)). Thus, the final message is

    MEET IN TUCSON ARIZONA AT MOUNT LEMMON MILEPOST TWENTY FIVE.

    (Both plaintext with either the x's left in or removed were accepted.)

    Note: Other ways to construct the square are certainly possible including guessing the codeword earlier on or using a partially filled square to start decrypting the message where possible and filling in more of the square based on new information.