Kryptos 2021 Challenge 3 Solution

The back story to Challenge 3 does not indicate the method of encryption so our first step is to make a guess. A frequency analysis of the ciphertext shows that the letter usage most closely matches an English alphabet so likely some sort of transposition cipher has been used.

The screenshot of the zoom meeting shows a whiteboard in the background of one of the participants that has a grid with arrows suggesting perhaps a columnar or row (or both) transposition cipher. Both ciphertexts contain 108 letters so if a columnar transposition was used the underlying grid could have various dimensions including 12x9, 18x6, 27x4,… If you study the chat box in the zoom call screenshot you will notice the words “July”, “January”, “February”,… “Nov”. If we assume a 12x9 grid, those might be clues to the way the columns or rows were permuted since there are 12 months in a year and we are guessing 12 columns or rows.

In a columnar transposition, the plaintext is typically written across the rows, then the columns are permuted, and finally the ciphertext is read down the columns. To decrypt we begin by writing the ciphertext down the columns. We guess 12 columns and 9 rows.

First ciphertext:

	1	2	3	4	5	6	7	8	9	10	11	12
1	T	O	W	O	M	A	Y	R	S	N	R	A
2	B	A	U	O	R	S	E	C	O	D	E	K
3	N	E	D	A	N	T	I	4	L	I	H	M
4	V	A	N	E	A	D	E	C	N	I	M	C
5	U	R	R	D	E	D	O	I	I	S	E	N
6	O	D	A	D	V	C	C	E	R	O	C	W
7	N	E	E	L	B	O	O	Y	L	I	U	W
8	I	V	E	T	H	K	L	E	D	E	E	R
9	S	M	O	T	F	U	R	E	A	T	R	E

Second ciphertext:

	1	2	3	4	5	6	7	8	9	10	11	12
1	U	B	T	E	N	D	O	L	G	A	O	E
2	O	T	T	M	P	H	N	A	E	T	A	T
3	O	U	N	N	I	E	H	S	T	A	T	E
4	I	R	U	R	F	R	H	T	O	F	T	Y
5	H	A	L	F	P	A	C	N	O	E	N	G
6	K	M	A	T	S	F	C	E	A	T	E	E
7	E	R	C	R	U	T	H	I	T	S	I	N
8	I	N	A	R	W	S	S	S	E	D	D	I
9	N	S	F	R	E	U	O	B	A	C	L	E

If we assume that the months in the chat correspond to the way the columns were permuted upon encryption (7, 1, 2, …, 11) then the first column in our ciphertext came from the 2nd column of the plaintext, the second column in our ciphertext came from the 3rd column of plaintext, the seventh column of the ciphertext came from the 1st column of the plaintext and the 11th column of our ciphertext came from the 12th column of the ciphertext. We start to rebuild the plaintext grid from this:

First message:

	1	2	3	4	5	6	7	8	9	10	11	12
1	Y	T	O									R
2	E	B	A									E
3	I	N	E									H
4	E	V	A									M
5	O	U	R									E
6	C	O	D									C
7	O	N	E									U
8	L	I	V									E
9	R	S	M									R

Second message:

	1	2	3	4	5	6	7	8	9	10	11	12
1	O	U	B									O
2	N	O	T									A
3	H	O	U									T
4	H	I	R									T
5	C	H	A									N
6	C	K	M									E
7	H	E	R									I
8	S	I	N									D
9	O	N	S									L

To confirm we are on the right track we notice a few words starting to emerge. In the first message row 5 we see “our” and in row 7 we see “one”. In the second message we see “not” in the second row.

At this point we can continue to transfer the remaining columns from our ciphertext grid to our plaintext grid in a way that builds words in one message. We can check to see if the other message is also forming words using the same choice of columns. For example, we might guess the word “vaccine” appears in a message given the context of the story and we see a “va” in the first message columns 2 and 3 in row 4. Looking back at the first ciphertext along row 4 at the columns we have not yet used we find a “c” in columns 8 and 12, an “i” in column 10, an “n” in column 9 and an “e” in column 4. If we guess this is the word vaccine then the columns 4-8 in our plaintext would come from our ciphertext columns 8, 12 (or vice versa) 10, 9, 4

First message:

	1	2	3	4	5	6	7	8	9	10	11	12
1	Y	T	O	R	A	N	S	O				R
2	E	B	A	C	K	D	O	O				E
3	I	N	E	4	M	I	L	A				H
4	E	V	A	C	C	I	N	E				M
5	O	U	R	I	N	S	I	D				E
6	C	O	D	E	W	O	R	D				C
7	O	N	E	Y	W	I	L	L				U
8	L	I	V	E	R	E	D	T				E
9	R	S	M	E	E	T	A	T				R

Second message:

	1	2	3	4	5	6	7	8	9	10	11	12
1	O	U	B	L	E	A	G	E				O
2	N	O	T	A	T	T	E	M				A
3	H	O	U	S	E	A	T	N				T
4	H	I	R	T	Y	F	O	R				T
5	C	H	A	N	G	E	O	F				N
6	C	K	M	E	E	T	A	T				E
7	H	E	R	I	N	S	T	R				I
8	S	I	N	S	I	D	E	R				D
9	O	N	S	B	E	C	A	R				L

At this point we can choose either message and try to finish the process of forming words across the rows. The columns from our ciphertext that we have yet to place in our plaintext are columns 3, 5, and 6. By inspection (trying to make words) we fill columns 9-11 of our plaintext grid by placing columns 5, 3, and 6 respectively from the ciphertext:

First message:

	1	2	3	4	5	6	7	8	9	10	11	12
1	Y	T	O	R	A	N	S	O	M	W	A	R
2	E	B	A	C	K	D	O	O	R	U	S	E
3	I	N	E	4	M	I	L	A	N	D	T	H
4	E	V	A	C	C	I	N	E	A	N	D	M
5	O	U	R	I	N	S	I	D	E	R	D	E
6	C	O	D	E	W	O	R	D	V	A	C	C
7	O	N	E	Y	W	I	L	L	B	E	O	U
8	L	I	V	E	R	E	D	T	H	E	K	E
9	R	S	M	E	E	T	A	T	F	O	U	R

Second message:

	1	2	3	4	5	6	7	8	9	10	11	12
1	O	U	B	L	E	A	G	E	N	T	D	O
2	N	O	T	A	T	T	E	M	P	T	H	A
3	H	O	U	S	E	A	T	N	I	N	E	T
4	H	I	R	T	Y	F	O	R	F	U	R	T
5	C	H	A	N	G	E	O	F	P	L	A	N
6	C	K	M	E	E	T	A	T	S	A	F	E
7	H	E	R	I	N	S	T	R	U	C	T	I
8	S	I	N	S	I	D	E	R	W	A	S	D
9	O	N	S	B	E	C	A	R	E	F	U	L

Now we have words across our rows, but the rows don’t’ seem to be in order. It appears a row permutation was also performed on the grid. By trial and error we unwind the rows in both grids until the words appear in a logical order.

First message:

	1	2	3	4	5	6	7	8	9	10	11	12
5	O	U	R	I	N	S	I	D	E	R	D	E
8	L	I	V	E	R	E	D	T	H	E	K	E
1	Y	T	O	R	A	N	S	O	M	W	A	R
2	E	B	A	C	K	D	O	O	R	U	S	E
6	C	O	D	E	W	O	R	D	V	A	C	C
3	I	N	E	4	M	I	L	A	N	D	T	H
4	E	V	A	C	C	I	N	E	A	N	D	M
7	O	N	E	Y	W	I	L	L	B	E	O	U
9	R	S	M	E	E	T	A	T	F	O	U	R

Second message:

	1	2	3	4	5	6	7	8	9	10	11	12
5	C	H	A	N	G	E	O	F	P	L	A	N
8	S	I	N	S	I	D	E	R	W	A	S	D
1	O	U	B	L	E	A	G	E	N	T	D	O
2	N	O	T	A	T	T	E	M	P	T	H	A
6	C	K	M	E	E	T	A	T	S	A	F	E
3	H	O	U	S	E	A	T	N	I	N	E	T
4	H	I	R	T	Y	F	O	R	F	U	R	T
7	H	E	R	I	N	S	T	R	U	C	T	I
9	O	N	S	B	E	C	A	R	E	F	U	L

Reading across the rows we find the following (punctuation added).

First message: Our insider delivered the key to ransomware back door. Use code word vaccine4mil and the vaccine and money will be ours. Meet at four.

Second message: Change of plans. Insider was double agent. Do not attempt hack. Meet at safe house at nine thirty for further instructions. Be careful.