

Kryptos 2020 Challenge 2 solution:

Portions of the mysterious sheet of letters appear to be plaintext. For example on the first row: “ERTHAT” and “INCOMP” seem like partial phrases of plain English. There seems to be a definite break between the first four cells and the last four cells. The arcs also seem to be clearly separated into blocks of four-by-four cells. If this sheet of paper is cut into eight equal four-by-four squares, they can be rearranged so all the arcs form concentric ellipses and the text becomes readable:

T	HI	S	IS	A	NE	X	AM
PL	E	OF	O	UR	N	EW	C
I	PH	E	RA	S	YO	U	KN
OW	T	HE	F	IR	S	TE	N
T	RY	C	OU	L	DB	E	AS
IN	G	LE	L	ET	T	ER	O
R	AP	A	IR	B	UT	Y	OU
SH	O	UL	D	AL	T	ER	N
A	TE	A	FT	E	RT	H	AT
AC	R	OS	S	FI	R	ST	R
O	WA	N	DC	O	LU	M	NP
RO	C	EE	D	AS	W	IT	H
C	OL	U	MN	A	RT	R	AN
SP	O	SI	T	IO	N	KE	Y
W	OR	D	SE	N	TS	O	ON
CH	E	CK	N	EW	D	RO	P

It now reads (with some added punctuation): “This is an example of our new cipher. As you know the first entry could be a single letter or a pair, but you should alternate after that across first row and column. Proceed as with columnar transposition. Keyword sent soon.”

From here we see that the cipher we should expect is much like a columnar transposition cipher except that each entry could be a single letter or a pair of letters. Starting with the upper left entry, one should write out the plaintext but alternate between single letters and pairs across the first row and down the first column. We would expect the columns to then be permuted and the final ciphertext read off column by column. We do not know the keyword, which would determine the number of columns and the order of the final permutation, so our work is cut out for us.

We now turn our attention to the intercepted SMS text message containing the ciphertext.

We will assume that the ciphertext was created as indicated in the example. We do not know if the first row/column started with a single letter or a pair. But the first row and column would alternate after that. We will not make any assumptions as to the number of columns used.

There are ways to break the cipher without using cribs, but having a crib could speed up the process. So, one might first start by guessing a few cribs. Based on the context there are a few that one might consider (virus, sample, etc.), but one might think that the importance of keeping the sample at 42 degrees could mean these instructions are repeated in the plaintext message. [Some teams fed the ciphertext through some online tools to help create words that could be made with the Ciphertext letters. This also led to some good cribs.]

Assumption 1: "forty two" appears in the plaintext. While this could be split across two rows, we might assume that a small portion of it could appear on a single row, say "forty". It would be split up like "fo r ty" or "f or t yX" where "X" stands for an unknown letter. There are no "FO" combinations in the ciphertext, so we **assume the placement is "f or t yX"**. There are three occurrences of "F" in the ciphertext and only one of "OR". The first "F" and the only "OR" are 38 characters apart. This could happen if there were two columns of 19 letters each separating them. Consider the following column patterns that could produce about 19 letters in a column:

1	2		1	
	3		2	3
4	5		4	
	6		5	6
7	8		7	
	8		8	9
10	11		10	
	12		11	12
13	14		13	
	15		14	15
16	17		16	
	18		17	18
19	20		19	

Since the columns would alternate between having 19 and 20 letters, the average would be 19.5 letters per column. There are 117 characters in total and $117/19.5 = 6$, making six complete columns!

Assumption 2: The word "degrees" is part of the plaintext. So it may be broken up as "de g r e s", "d e g r e e s" or "Xd e gr e es". Since no "GR" appears in the ciphertext, we can remove this possibility. Looking

for “DE” and “RE” in the ciphertext yields a couple of results. In one instance these digraphs are separated by 20 letters and in another 25 letters (the first is promising as it reinforces our earlier work that there may be 19-20 letters in each column). There are also occurrences of “EE” and “EG”, but none are 19-20 letters apart. For now, we will assume that “de g re s” is the correct pattern and...

Assumption 3: Let’s assume that six columns were used and there are 19 or 20 characters per column depending on whether that column starts with a single letter or a pair. Looking at the first 19-20 letters of cipher text, one of the columns must be one of the following:

E		E E
E E		E
T		T E
E T		T
E		E S
S O	OR	O
E		E H
H O		O
I		I X
X L		L
O		O U
U E		E
P		P R

Col 1

The digraph “XL” does not look promising whereas the digraph “IX” looks much better. Let’s assume that the first twenty letters form a column like the second one above. We’ll call this column 1.

Under assumption 1, we want the “F” in the next few letters to be a singleton. That means we need to place these letters in a column like:

M
G E
F
E G
I
A G
W
O N
E
O O
A
G O
I

Col 2

The next set of letters (either 19 or 20) will form column 3, but let's skip those for now and move onto the next set of letters. We need the "OR" to be in the same row as our "F" in Col 2. This means Col 4 starts with a pair of letters and alternates after that. Placing Col2 and Col 4 together we have:

M	P L
G E	R
F	O R
E G	R
I	V E
A G	E
W	A R
O N	E
E	S T
O O	D
A	R D
G O	F
I	N E

Col 2 **Col 4**

We now know that the twenty letters forming column three must also start with pair of letters. Looking at that columns of letter also indicates that it could fit in nicely before Col 2:

S A	M	P L
I	G E	R
A T	F	O R
D	E G	R
E L	I	V E
R	A G	E
N D	W	A R
E	O N	E
Y W	E	S T
W	O O	D
E V	A	R D
N	G O	F
L N	I	N E
Col 3	Col 2	Col 4

Since we are expecting to have three columns with 19 letters and three columns with 20 letters, we see that we have already identified three columns with 20 letters, so the remaining two columns have 19 letters each (and they must start with a single letter). It is easy at this stage to create these last two columns and find the correct permutation to fit with the rest of our work yielding the final plaintext:

keep sample refrigerated at forty two degrees deliver to garage behind warehouse one sixty west hollywood boulevard evening of april nine