Kryptos 2021

Challenge 2 solution:

We are told that the ciphertext was generated with a Vigenere Cipher using a Running Key. Based on the given information, the running key is the start of some book, possibly a piece of literature. Thus, the key is as long as the ciphertext and some normal attacks on Vigenere, like the Kasiski test, are not useful. What will be helpful is that the key is, most likely, in English. Thus the key (and the plaintext) will have all the underlying frequency properties of English and we should be able to recognize parts of either when we uncover them.

Two possible approaches are given here.

Method 1: Crib Dragging

If we can guess at some possible words or phrases that appear in the encrypted message, called "cribs", we can place the cribs in every possible position. For each position, one can use the CT/pt pairing of a Vigenere cipher to identify the letters in the key. If the resulting portion of the "key" does not look like English, we can assume that the crib is not in the correct place and move it over one position. If one chooses a phrase that does not produce any reasonable key portion in any position, then that phrase is probably not in the plaintext. Try again. We will try the following cribs:

- "freezer"
- "thefreezer"
- "unlock"

For example, if the plaintext begins with "freezer", the key that would produce the given ciphertext would be "wjwbkaq", which does not look like part of an English phrase. If "freezer" is placed beginning with the fourth letter of the cipher text, the key would become "asadark" or "as a dark", which is promising. To place "freezer" here, we would need three letters in front of it. If we press our luck and try "thefreezer" in the first positon we get the key "itwasadark" or "it was a dark". You are looking for a book that begins "It was a dark…". An internet search might quickly turn up "It was a dark and stormy night…" as a famous first line of the book *Paul Clifford* by Edward Bulwer-Lytton (1830).

If one tried the crib "unlock", one would find that in position 17 one would get the key letters "rmynig", part of "stormy night".

With two or three of the above cribs, one can track down the opening sentence of *Paul Clifford*:

"it was a dark and stormy night the rain fell in torrents except at occasional intervals when it was checked by a violent gust of wind"

Using this key, one can decrypt the entire message:

"The freezer should unlock when the password is texted to five zero nine four one six six two five eight the password is Tallahassee"

Did anyone text "Tallahassee" to this number to unlock the freezer and save the day?

Method 2: Frequency Analysis

This method is described in Craig Bauer's book Secret History: The Story of Cryptology. Bauer attributes this attack to William Friedman. The idea is relatively simple: since the plaintext and the key are both in English, some plaintext/key letter pairs are more likely to produce any given ciphertext letter when encrypted with a Vigenere cipher. Our first ciphertext letter is B. There are 26 plaintext/key letter pairs that could have produced a B: ba, cz, dy, etc. But, the most likely pairs would be: it, no, hu, ab, dy (or ti, on, uh, ba, yd). So, maybe the key starts with "t" and the plaintext starts with "i", or vice-versa. The chances that every ciphertext letter comes from the most common plaintext/key pair is, ironically, not very common. But, we might assume that it comes from one of the five or six most common pairings.

One could cleverly arrange this information as follows (first 14 CT letters listed):

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

Under each CT letter are the five most common pt/key letter pairs. These pairs are listed again with their positions swapped (since we don't know which is the pt and which is the key). Now, in the upper half, pick a letter from each column so you start to form an English sentence as you read from left to right. Look at the corresponding positions in the lower half. If they are also looking like English, you are on the right track! If not… try again. One could also look for cribs like "freezer" or "unlock" or simply assume some common words like "the" might start the sentence. When you are all done, the plaintext will be in one half and the key in the other. The context should tell you which is which.

For example, it looks like we can form “the” at the start. Highlight those letters in the upper half and the letters in the corresponding positions in the lower half:

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

If “the” is part of the pt or key, then “itw” is part of the other. “itw” could be the start of an English sentence, so this looks good. After “the” one starts to find the letters for “freezer”:

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

The “z” and “r” were not among our five most likely choices, but you can always just put them in. That would produce, in the lower half, “it was a dark”. One could now try to finish the phrase in the lower half to get more of the upper half. Or, if one recognizes the phrase “it was a dark and stormy night…”, one could just complete the key and get the plaintext as usual.