Kryptos 2023 – Challenge 3 Solution

From the transcript, one may deduce that the ciphertext was encrypted using a Vigenère square, but using the first sentence(s) from a book as the key as opposed to the more standard repeated keyword. This is known as a “running key”.

Method 1: Craig Bauer presents a way to attack a running key cipher in his book “Secret History: The Story of Cryptology”. This method uses a little bit of probability. The idea is that when confronted with some ciphetext that was encrypted with a running key, both the plaintext and the key follow letter frequency distributions from the English language. Thus, when one sees an “H” in the ciphertext (like in this Challenge), there are certain plaintext-key pairings that are more likely to produce an “H” than others. In fact, the five most common pairings are: OT, DE, AH, NU, PS. Similarly, one could construct the five (or so) most common plaintext-key pairings that would produce the other letters in the ciphertext. The first few are illustrated below:

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

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

Notice that under each CT letter, are written the five pairs most likely to generate it. These pairs are listed a second time, with the letters from each pair reversed. One can now start in the upper half and try to build an English phrase or sentence. If the letters in the corresponding positions in the lower half also start to look like an English phrase or sentence, then you probably have it! The top will end up being either the key or the plaintext and the lower one will be the other. For example, we might guess that the plaintext starts with “the meeting”. This yields:

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

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

Seeing "one thing wa" appear in the lower half is promising. At this point, one can try to start finishing either the lower portion or the upper portion, often bouncing back and forth between. After a few more characters, one probably has enough of the key (lower half) to identify the book with an internet search. This yields "One thing was certain, that the white kitten had had nothing to do with it" from Lewis Carroll's "Through the Looking Glass". The resulting plaintext becomes:

```
The meeting will be held at ten oclock pm downtown warehouse
```

Method 2: Many teams this year tried a crib dragging approach, either with pencil and paper or by writing some code. One may guess a word(s) or phrase that you think will appear in the plaintext (crib) and use the Vigenère square to identify the corresponding letters of the key. By placing the crib in every possible position, one may look for keys that appear to come from English. This will tell you where to place the crib. As like the above method, seeing part of the key may help you guess a little more of it, which will, in turn, give you a little more of the plaintext.