

Kryptos 8: Challenge 3 Solution

The coffee stained paper lets us know that the Vigenère cipher was used, but we don't know the keyword. Further the Vigenère table is in a different order than usual so we need to be careful when we decrypt.

One effective approach to cracking a Vigenère cipher is to find a crib. As we read through the backstory it seems reasonable that the words "big event" were used in the plain text since we know the author of the message is writing about what he refers to as a "big event". If we work with this assumption we can try to find which ciphertext corresponds to the plaintext "big event" to help us find the keyword that was used to encrypt.

One way to do this is to write a simple program (or even an excel look up table) that takes as input the ciphertext and plaintext letter and gives as output the corresponding key. Then we can just put "big event" in all possible locations for the plaintext to see which one gives a key that makes sense as a code word.

For example if we try "big event" as the first two words we get:

key	u	i	d	n	x	y	m	b
ct	W	P	I	Q	T	B	A	V
PT	b	i	g	e	v	e	n	t

This would lead to a keyword with the letters "uidnxymb" which doesn't make sense. So we proceed to move the word "big event" down to the next position to see if we get a sensible keyword:

key		n	b	l	q	f	x	h	t
ct	W	P	I	Q	T	B	A	V	N
PT		b	i	g	e	v	e	n	t

This gives a keyword with "nblqfxht" which also does not make sense. If we continue to try every possible location for this this plaintext until we get a keyword that makes sense we first find a candidate at "JPHNAQQB"

```
WPIQT BAVNV UKQZP NFPDW VCZMX XWWWU MCEHA VZVSN WNWOE FBEFF OWSWE
OFHWG FHQAX LDEIA BKWTX KZPII OLLHJ GLQBY AEKVQ SEBGN VUEMQ NHADS
HEXKL AAHOW NBOWP QGOID XAQUH NFKSR PAATX FUCTT FOLNW ZVOWV NUKVQ
SEBGB VTAWQ CLCKN SQXYC KNPAN KKWEM QIOAT EUFPB LTEHF TELOW KUQHU
OHYVF JPHNA QQBPT XSVCV MJLEB QUDUN AQCTC KNKUQ HUOXF NWOVQ KSRWO
TFBRI FIIQK QZNUK JWL MF HWGKF OPSYO RVVPA ANRVE JUWTP WAVVM BNWAX
OUOMH SUHWW AEFLI QJLES PVLAE KFJLI ZEHBC SN
```

key	h	i	c	k	e	n	c	h
ct	J	P	H	N	A	Q	Q	B
PT	b	i	g	e	v	e	n	t

This corresponds to the key “hickench” which we can see is probably the keyword “chicken”.

To check this keyword we can write a second program (or look up table in excel) to decipher the ciphertext using the keyword “chicken” to find the following plaintext message:

Thank you for all of your hard work to date our operatives are in place and we expect dozens of local citizens to be on hand for the marches we expect full media coverage and our social media trolls are on hand to spread the news the moment the first protesters yell finally the big event is on hand i can now reveal the final location and time so we can all mobilize and accomplish our missions ground zero will be grant park Chicago next Friday ten am g