Challenge 2

Solution

`uzs yfr uvjf kay | btoh abkqhb khgb tv hbk lk t tv bg akwv obgr muc utb gkzt qn`

The hint "the cipher method used can be found by reading the first part of the ciphertext" suggests that you can somehow "read" the cipher text.

If you try to pronounce the first part of the ciphertext, it reads "Use cipher of JFK". Those of you who know history or a quick google search of "cipher of JKF" leads one to guess that the message was encrypted using the Playfair Cipher (see http://en.wikipedia.org/wiki/Playfair_cipher for more details on the cipher, but the encryption rules are summarized below).

To crack the code we have to build the 5x5 matrix key that was used for encryption. A codeword or "key" is written in the matrix with duplicate letters dropped. The rest of the alphabet is then written in alphabetical order skipping any letters that were already used in the codeword. In order to get only 25 letters for the 5x5 matrix the "j" is often dropped (if a j occurs in the plaintext message it would then be replaced by an i when encoding and it becomes obvious upon decryption when an i should be replaced by a j). In this case the j was in fact dropped.

To encrypt a message it is broken into blocks of two letters and then one of the following rules is applied to each pair of letters:

1. If both letters are in the same row of the table, then replace each letter with the letter to its immediate right. If a letter is at the end of the row "wrap around" and replace it with the first letter of the (same) row.
2. If both letters are in the same column, then replace each letter with the letter that appears immediately below it. If one of the letters is the last one in the column "wrap around" and replace it with the top letter in the (same) column.
3. If the letters are not in the same row or column, then replace them with the letters on the same row respectively but at the other pair of corners of the rectangle created by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same **row** as the first letter of the plaintext pair.

   Notes:

   - If there are an odd number of letters in the plaintext then an "x" or some such uncommon letter is usually added to the end to complete the last pair.
   - The cipher method does not allow for the encryption of double letters so if they occur when you group the plaintext into twos, they must be split apart. It is common to just insert an "x" between them.

Now, on to breaking the code. The ciphertext begins after the vertical line |: `btoh abkqhb khgb tv hbk lk t tv bg akwv obgr muc utb gkzt qn.`

The back story suggests the suspected location of the attack, “Brighton Bridge”, might be in the message so let’s try to use that as a crib. If we go on that assumption we can see that if the plaintext letters were lined up just right then when the plaintext was broken up into groups of two we would get

BR IG HT ON **BR** ID GE

and so the ciphertext would have two identical blocks of two (corresponding to the BR) separated by three other (different) blocks of two. Writing out the ciphertext in blocks of two we see two places that satisfy the requirement: the “hb” and the “tv”:

```
Bt oh ab kq hb kh gb tv hb kl kt tv bg ak wv ob gr mu cu tb gk
zt qn
```

Let’s start by assuming that “Brighton Bridge” lines up under the “hb”s and see where we get:

```
Bt oh ab kq hb kh gb tv hb kl kt tv bg ak wv ob gr mu cu tb gk

            br ig ht on br id ge

zt qn
```

We proceed to try to build the 5x5 matrix as if this is the case working backwards using the Playfair encryption rules:

1. BR → HB. Since B occurs both in the plaintext and ciphertext, it must be the case that B and R are in the same row or column, since it is impossible to make a rectangle where BR → HB. Further, since R→B then B must be either immediately to the right or directly below the R. Here are the two possible cases:

   R B H or R
B
H

2. IG → KH There are several choices for how this might be built into the key, but if you look at them all then the best choice that stands out is GHIK because it puts the letters in alphabetical order and we know that once the codeword has been written in the rest of the letters are placed in alphabetically.

3. If we try to put 1 & 2 together, then the row choice for 1 is not compatible so we will continue under the assumption that the column choice from #1 works giving us this so far:

	R		
	B		
G	H	I	K

4. Now look at HT →GB. If we assume the above we know where G,B and H are in the matrix and there is only one place to put the T.

	R		
T	B		
G	H	I	K

5. ON →TV. There are several possible cases here:

Case 1: ON are in the same row. Since O→T, then O would have to be to the left of T and then N and V would have to be next to each other in that order giving this as the only option:

		R		
O	T	B	N	V
	G	H	I	K

If we remember that the letters not used in the code word are then placed in alphabetically we can see this is unlikely to be correct because of the placement of the N and V before G H I K. Thus we rule this out.

Case 2: If ON are in the same column then O would have to be above T and N above V giving this as the only option:

O	R		
T	B		
G	H	I	K
N			
V			

This looks promising because it maintains the alphabetical ordering with a reasonable number of spaces between the N and V.

Case 3: We form a rectangle with the letters in which case there are several options, but we know that O is in the same row as T and N is in the same row as V. Here is one option:

R

T	B	O	
G	H	I	K
N		V	

There are more possible rectangles, but if you explore these options it becomes clear that Case 2 is the most promising so let's continue with that:

O	R		
T	B		
G	H	I	K
N			
V			

6. ID → KL. If our above assumption is right, then since K is next to I and there isn't room to have DL in that row, then ID is not in the same row or column and must form a rectangle. Here are the possibilities:

O	R	L	D	choice 1
T	B	L	D	choice 2
G	H	I	K	
N		L	D	choice 3
V		L	D	choice 4

Choices 2, 3 and 4 look very unlikely because they throw off the alphabetical ordering. Further we can make out part of a word in choice one "orld". We will guess that the first part of the code word is "world" thus giving us the following:

W	O	R	L	D
	T	B		
	G	H	I	K
	N			
	V			

7. GE -> KT since we know where the T,K and G are there is only one place to put the E:

W	O	R	L	D
	T	B		E
	G	H	I	K
	N			
	V			

8. Since we used the W and there are 3 spaces after the V, the X, Y, and Z must not have been used in the code word so we can place those in. Further there is only one space between E and G so it must be F and there is only one space between the K and N so it must be M since L was used in the code word.

W	O	R	L	D
	T	B		E
F	G	H	I	K
M	N			
	V	X	Y	Z

9. Since the B is after the T and the D has already been used the C must be between the B and E and so the only place to put the A is in the spot before the T:

W	O	R	L	D
A	T	B	C	E
F	G	H	I	K
M	N			
	V	X	Y	Z

Now we can fill in the rest alphabetically omitting letters already used:

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

It appears the code word was “world at” but it really was “world war two” (since we can’t use duplicate letters we get “world ~~w~~a~~r~~ t~~wo~~” = “world at” in the matrix). World War Two is when JFK used the Playfair cipher.

If you decrypt using this board you get the plaintext

Target is brighton bridge on the fourth of may at five pm

We can now stop the attack of the Phantoms!