Proposed Solution
to Kryptos fourth part (K4)

Hamid Samak

hamidreza.samak@gmail.com

March 2018

Introduction

My name is Hamid Samak[1], a web developer from Iran. I've about 15 years experience working with programming languages and mostly web programming languages and technologies. I'm working on Kryptos since December 2015 when I read an article about unsolved mysteries in the world. I've spent hours and days finding a logical solution for K4 with attempts like brute-force and multiple transpositions that sometimes took days to finish, and got no success.

After all these, I've found significant relations between given clues and hints in Kryptos cipher text and plain text both. I'm not going to say that it is the final solution to K4, but I believe that it might be the right path for further attempts.

I'm trying to explain all I've got step-by-step, so please read this from the beginning and remember the results of each section, because there are relations between them.

Morse Codes

As we know there are several morse code messages (known as K0) in the CIA HQ area. If we read the morse codes in forward or backward mode we get different results. For example, `VIRTUALLY` can be read in morse code as bellow in backward mode.

>	V	I	R	T	U	A	L	L	Y	
	…-	..	.-.	-	..-	.-	.-..	.-..	-.--	
	B	I	R	T	D	N	F	F	Q	<

There is another interesting word in this section `INTERPRETATI` with missing `ON` at the end.

>	I	N	T	E	R	P	R	E	T	A	T	I	
	..	-.	-	.	.-.	.--.	.-.	.	-	.-	-	..	
	I	A	T	E	R	P	R	E	T	N	T	I	<

Maybe it's very soon to consider it as a crypto-system but this can be a direct addressing or hint for further decryptions.

It's clear that some English letters in morse codes follow ambigram pattern. So here is the list of letters with backward morse translations based on International Morse Codes.

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

We can see that there are no translations for C, J, and Z with reading in backward mode. Please remember these three letters for the next sections, especially J and Z.

[1] http://hamidsamak.ir

Frequency Analysis

In this section, I'm going to show a letter frequency analyse in the plain text of solved parts. I'm just pointing to missing or suspicious letters, not all 26 English letters.

	J	Q	X	Y	Z
K0	0	0	0	3	0
K1	0	1 Misspelling	0	0	0
K2	0	0	7 Added	10	0
K3	0	1 Added	1 Added	8	0

Added means there is no word or words containing that letter in the text but added somewhere in the text for some purposes (hint or mistake, I consider them as hints).

The J and Z letters which had no translation in reading morse codes backwardly have not used in solved parts. So I can guess that the K4 plain text wouldn't have any J and Z based on perceptual sequences. Although there are not enough proofs to claim this sentence for whole K4 decryption but just considering it as a standard for computer attacks and searching words in results.

Misspellings

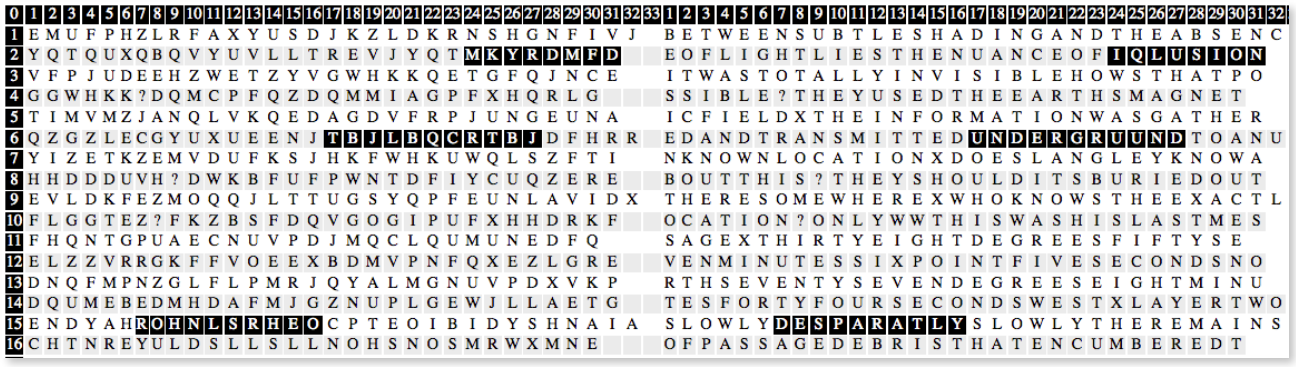
After decrypting the first three parts of Kryptos we found three misspelling words in plain texts.

	Misspelling word	Correct word	Misspelling letter	Correct letter
K1	IQLUSION	ILLUSION	Q	L
K2	UNDERGRUUND	UNDERGROUND	U	O
K3	DESPARATLY	DESPERATELY	A	E

This is notable to point out that the `IQLUSION` and `UNDERGUUND` are in lines at front of cutouts of the petrified tree in Kryptos tableau.

There is also a missing `E` in `DESPARATLY` that I've not found any relation to my proposed solution.

Please remember the correct letters `LOE` for next sections, It will be part of a key for decoding one of the given clues.



Primary Key

Mr. Sanborn revealed two clues and their positions in the cipher text in 2010 and 2014. The clues are BERLIN and CLOCK, the 64th letter of K4 to 74th letter. We can easily use Vigenère cipher to find the key for given clues. By the given clues the NYPVTTMZFPK will be deciphered to BERLINCLOCK with ELYOIECBAQK key.

I've tested an English dictionary with 128,000 words to find nearest words to ELYOIECBAQK. The only word very closed to this key is GIMCRACKERY. It might seem an accident and maybe there are a million combinations of words for this key but I'm going to find a logical hypothesis to link GIMCRACKERY to ELYOIECBAQK.

Facts and findings

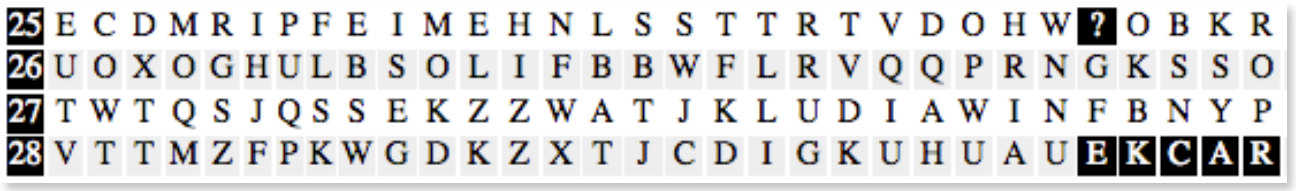
1. The keyword ELYOIECBAQK has the same pattern with ERYGIMCRACK in odd letters.

2. If you start the GIMCRACKERY from the beginning of K4 (OBKR...) it goes in right place for NYPVTTMZFPK, starts with ERY.

```
OBKRUOXOGHU...NYPVTTMZFPK...
GIMCRACKERY...ERYGIMCRACK...
```

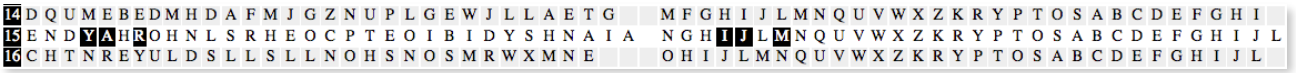
3. The K4 ending is pointing to GIMCRACKERY based on keyword sequence in reverse mode.

```
OBKRUOXOGHU...NYPVTTMZFPK...EKCAR
GIMCRACKERY...ERYGIMCRACK...RACKE
```



4. GIM has the same (or close) pronunciation for JIM, the first name of Kryptos creator (Jim Sanborn).
   I know that it might seem a false hypothesis for cryptanalysis, but just consider that if you were the creator of an artwork, would you leave or hide your name somewhere in that?

5. The raised letters in K3 YAR are in same positions for IJM in the right panel (Vigenère tableau), referring to sculpture creator's first name (Jim) or the keyword.



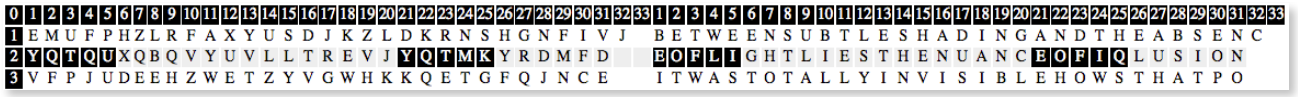
6. If you use Vigenère cipher to decipher the K4 from the 64th letter (NYP...) there would not be any J or Z in odd letters. (pointing to letter frequency analysis that explained before).

```
CIPHER      =     NYPVTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
KEY         =     E?Y?I?C?A?K?R?G?M?R?C?E?Y?I?C?A?K?
DECIPHER    =     B?R?I?C?O?K?F?G?S?I?R?Y?N?S?F?N?A?
```

Solving BERLIN

Let's get back to 2010 when Mr. Sanborn revealed the `BERLIN` clue for `NYPVTT`. The key to deciphering the clue would be `ELYOIE` and the even letters are `LOE` (and odd ones `E?Y?I?` from `GIMCRACKERY`). The `LOE` letters are the corrections for misspelled letters as mentioned in Misspellings section.

So I'm going to find out is there any sign for a keyword to decipher `NYPVTT` to `BERLIN`. Based on what explained in Morse Code section (reading the morse codes backward), I've checked the whole plain texts (K1 to K3) to find a relation between `ELYOIE` and any set of characters. There are two sequences in the second line (K1) that can be translated to this keyword.




```
1. EOFLI   >     backward morse   >     EOLFI
2. EOFIQ   >     backward morse   >     EOLIY
```

Note: You can use the table in Morse Code section to translate each letter.

The second one (`EOFIQ` translated to `EOLIY`) which have a part of the misspelled word (`IQLUSION`) in K1 is very close to the key ELYOIE in characters. So I'm going to re-order the letters from 12345 to 13524:

```
1. EOLFI   >     12345 to 13524   >     ELIOF
2. EOLIY   >     12345 to 13524   >     ELYOI
```

In the second one, it completely matches with the keyword. This re-ordering method does not seem to be accidental, so please remember this for next sections.

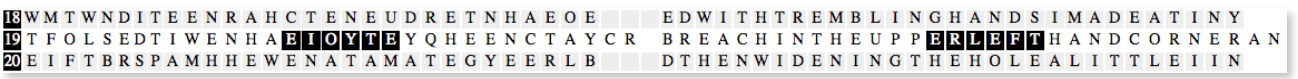
I'm going to call this method as Method 1. (The method to create the key from K1 plain text).

```
Method 1 = Backward Morse + 13524
```

There is no difference between the priority of Backward Morse and re-ordering in this section, but in next sections, we will do re-ordering at first. So the equivalent will be:

```
Method 1 = 13524 + Backward Morse
```

Despite what explained above there is also an interesting sequence in nineteenth line `EIOYTE` that is reversed version of `ELYOIE` just with the difference in `T` letter. I did not find anything important in this case but just wanted to mention this for those who still think the `GIMCRACKERY` and `ELYOIE` are accidental.

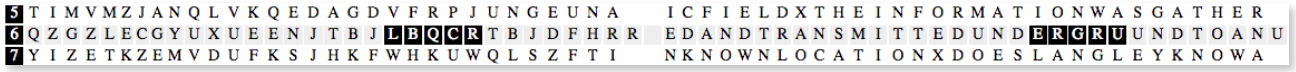


In the next section, I will present more information about further decryption based on what we had in this and previous sections.

Solving CLOCK

As what we have done for reaching to the key for decrypting BERLIN, in this case, we're going to find the key for decrypting MZFPK to CLOCK. The key according to Vigenère cipher is CBAQK for decryption and as what we had in the Primary Key section it's in GIMCRACKERY pattern.

I've found another interesting link between CBAQK and a sequence in K2 exactly before the second misspelling. (The key for BERLIN also was before the first misspelling [EOFIQ]). But this time the key is in cipher text of K2 (LBQCR).



In this case, I found another method to reach CBAQK from LBQCR. At first I tried 13524 re-ordering.

```
LBQCR       >     12345 to 13524   >     LQRBC
```

Next, reversing the string:

```
LQRBC       >     reverse          >     CBRQL
```

And we have found the B and Q for CBAQK. I'm going to call this method as Method 2:

```
Method 2 = 13524 + Reverse String
```

It is worth mentioning that base on results we can expect the GIMCRACKERY is the primary key used in odd and even order pattern but because of the length of it (odd number) the key would be repeated like this:

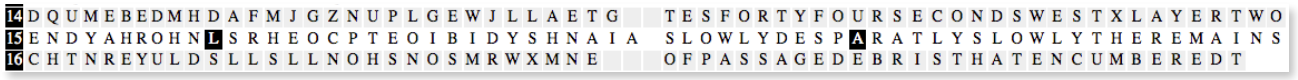
```
?I?C?A?K?R?G?M?R?C?E?Y
```

and we should find question marks (L–O–E–B–Q) to decipher K4. In the next section I'll go for third misspelling and four letters before that and use that one as key for WGDK.

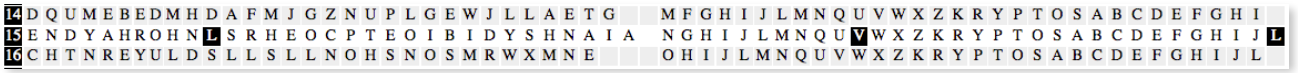
Further Solutions

According to previous sections and finding keys for BERLIN and CLOCK, we've found that the misspelling letters and four letters before them (totally five letters) would be part of the secondary key as part of the mixed keys for decrypting K4.

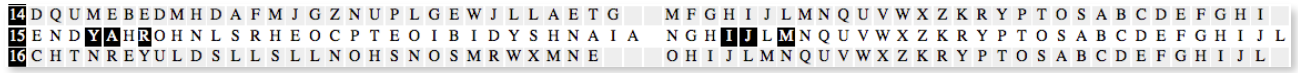
The third misspelling letter which is placed in K3 at DESPARATLY can shape our next key for decrypting after BERLINCLOCK.



Although it's important to note that there is an extra L in Vigenère table (right tableau). Maybe the extra L which break the order of the table (additional column) is going to point on the only L in line 15 in cipher text, the same misspelled letter in DESPARATLY.



Other interesting hints are in raised letters YAR just before the third misspelling which somehow are referring to IJM or JIM in Vigenère table.



I've spent hours to find some kind of relation or link in YAHROHNL letters and have found out that it might be encoded using ROT13, a simple substitution cipher.

YAHROHNL > ROT13 > LNUEBUAY

The encoding and decoding of underlined letters YA and NL return same results. Let's have look to ROT13 table:

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

It's also very similar to backward morse code reading. Remember the INTERPRETATI and effect of backward reading morse codes.

INTERPRETATI > Backward Morse > IATERPRETNTI

So I found the third method (Method 3) including a combination of previous methods and ROT13.

Method 3 = 13524 + Reverse String + ROT13

And the result based on misspelled letter position and four letters before that would be like this:

```
ROHNL     >    12345 to 13524   >    RHLON
RHLON     >    Reverse String   >    NOLHR
NOLHR     >    ROT13            >    ABYUE
```

By the final key, we can mix the B and U with primary key (GIMCRACKERY) and the result for after BERLINCLOCK would be like this:

```
CIPHER     =     NYPVTTMZFPKWGDK
KEY        =     ELYOIECBAQKBRUG
DECIPHER   =     BERLINCLOCKIFIG
```

Well, it's very soon to say that is the right solution and I'm waiting for some kind of confirmation from people who are working on K4 but in first view, it reminds me a sentence like IF I GO at the end.

Conclusions

According to above sections, we found how we can solve given clues BERLIN and CLOCK using hints (mainly misspelled words). I cannot say that the previous section about after BERLINCLOCK is the correct solution because I'm not the person to prove that but I'll be waiting for getting feedback from people who have something to say about it.

The methods to reaching keys for BERLINCLOCK and after that would be:

```
Method 1 = 13524 + Backward Morse
Method 2 = 13524 + Reverse String
Method 3 = 13524 + Reverse String + ROT13
```

We can also have the second and third methods like this:

```
Method 2 = 42531
Method 3 = 42531 + ROT13
```

It's very interesting that all methods contain backward or reversing the string. The EKCAR at the end of K4 which might refer to GIMCRACKERY is reversed too.

Overall, I've spent many times trying to solve K4 using multiple computer attacks but got nothing until last 8 months hard working finding these results. I hope to get technical feedback from people who love puzzles and especially Kryptos that is a fantastic one. I also have a notebook that I use it to write any ideas about my working on Kryptos and many programming functions and scripts about that, I hope to find free time to release the important ones of them.