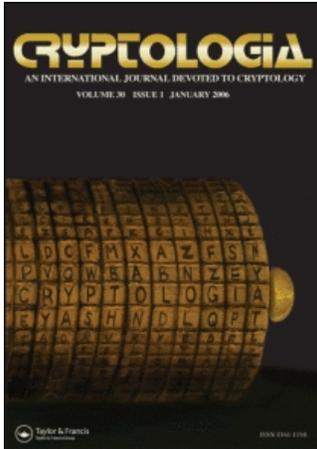


This article was downloaded by:[Winkel, Brian]
On: 14 March 2008
Access Details: [subscription number 769884566]
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Cryptologia

Publication details, including instructions for authors and subscription information:
<http://www.informaworld.com/smpp/title~content=t725304178>

POE CHALLENGE CIPHER SOLUTIONS

Online Publication Date: 01 October 1977

To cite this Article: (1977) 'POE CHALLENGE CIPHER SOLUTIONS', Cryptologia, 1:4, 318 - 325

To link to this article: DOI: 10.1080/0161-117791833066

URL: <http://dx.doi.org/10.1080/0161-117791833066>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article maybe used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

POE CHALLENGE CIPHER SOLUTIONS

In the January 1977, Vol. I, No. 1, issue, pp. 93-96, readers were challenged to solve the following message:

Ge Jeasgdxv,
 Zij gl mw, laam, xzy zmlwhfzek ejlvdxw
 kwkw tx lbr atgh lbmx aanu bai Vsmukks pwn
 vlwk agh gnumk wdlzweg jnbxvv oaeg enwb
 zwngy mo mlw wnbx mw al pnfdcfpkh wzkek
 hssf xkiyahul. Mk num yexdm wbxv sbc hv
 wyx Phwkgnamcuk?

The article may be seen for details surrounding the cipher. While several readers sent us solutions and were duly credited in the April 1977 issue, we take time to list solvers who sent solutions:

John Ambruz, Burlington, Ontario, Canada
 Arthur J. Dore, Jr., Buffalo Grove, Illinois
 Ross Eckler, Morristown, New Jersey
 Henry J. Gibson, Jr., Stamford, Connecticut
 H. Gary Knight, Baton Rouge, Louisiana
 D.C.B. Marsh, Golden, Colorado
 Randall K. Nichols, Torrance, California
 R.E.A. Poole, Austin, Texas

We present now the solution and comments of four of the solvers, Messrs. Knight, Gibson, Dore, and Ambruz.

Poe Cipher Solution (Errors Corrected):

MR. ALEXANDER, HOW IS IT THAT THE MESSENGER ARRIVES HERE AT THE SAME TIME WITH THE SATURDAY COURIER AND OTHER SATURDAY PAPERS WHEN ACCORDING TO THE DATE IT IS PUBLISHED THREE DAYS PREVIOUS. IS THE FAULT WITH YOU OR THE POSTMASTERS?

H. Gary Knight's Solution:

1. Calculation of the index of coincidence (1) indicated that the cipher was almost certainly polyalphabetic. Working on that assumption, application of the Kasiski method (2) suggested a period of 12, with 6 a close second. The mathematical formula (3) gave a period of about 3, an error probably induced by the repeated letters in the keyword (one advantage of the Kasiski method over the formula is that the former is not fooled by repeats in the keyword).
2. Working on a 12 period, I was having difficulty extracting individual alphabets because of the dearth of letters in each. Thinking that I might also be in error with the 12 period, I put some effort in on a 6 period (which, incidentally, gave very good indices of coincidence for the individual alphabets — .047, .069, .077, .075, .052, and .062). Utilizing traditional Vigenere solution techniques for the individual alphabets (4) I developed a probable keyword of ITES. The T and E columns gave especially good plaintext, the two-letter words "at" and

"or" not easily being attributable to accident. Convinced now that the period was in fact 6, I underlined all three-letter words and tried to match them where parallel in a 6 period block, using a list of the most frequent three-letter words. This produced instant but bewildering results! For example, the matching threesome of ZIJ, LBR, and WYX (all enciphered with the same key letters if the 6 period were correct) gave plaintext of "how", "the", and "eek". I now knew I had the cipher broken in principle, but the "eek" was perplexing.

3. I then wrote out the entire "plaintext" using my best alphabets, which gave a keyword of NITESU. Several words appeared clearly, such as "arrives", but garbles appeared with equal frequency. Knowing the word divisions, and the context of the message, I guessed that my garble "messplmwr" was in fact "messenger". I then checked (and this turned out to be the critical move) to see what keyword letters would convert the obviously erroneous "plmw" into the correct "enge". Those letters were DSTA.

4. Finally, I decided to write into the six-column format the key letters (as opposed to plaintext) that would produce the obviously correct plaintext I had deduced to that point ("the messenger arrives here at the same time"). Bingo! The T and E columns stayed T and E throughout, but the other four alternated — T with N in the first, I with A in the second, D with S in the fifth, and U with S in the sixth. Suddenly I was reading the "plaintext" keyword — the words UNITED STATES!

5. Realizing that my initial calculation of 12 for the period was correct, I wrote the ciphertext out in that period, added the correct keyword, translated, and corrected the errors. Total time expenditure was 5-1/2 hours.

Errors:

1. I found 16 errors — one major and 15 minor ones. The major error was in the initial 10 letters of the message. Mr. Kulp started off with the keyword UNITEDSTATES and proceeded to encipher "Mr. Alexander". Here is his likely handiwork:

Key	U N I T E D S T A T E
Pt	M r A l e x a n d e r
Ct	G E I E I A S G D X V

Unfortunately, in transcribing the ciphertext (or, perhaps, when setting Mr. Kulp's handwritten cipher to print), two errors were made: (1) the first "I" was miswritten as "J"; and (2) worse, the second "I" was dropped altogether. Thus, we had to work with "GEJE" instead of the correct "GEIEI".

2. As for the 15 minor errors, eight are easily explicable in terms of mis-copying the original handwritten manuscript. The letters "g" and "q" are confused five times, "h" and "k" once, "x" and "k" once, and "u" and "n" once. An example of how this probably occurred is shown by the plaintext at the beginning of the message which reads, prior to error correction, "how ys it that the Messenger ..." The key letter for the plaintext "y" is "I". However, one notes that the obviously correct plaintext "i" is given by ciphertext "q". In longhand, "q" and "g" are

easily mistaken for one another, as must have been the case when the message was copied from Kulp's longhand by the Messenger's printer.

3. Another error is the incorrect division of the word "courier" in the ciphertext where it appears as two words — "pwn vlwk".

4. Four other errors are attributable to simple misreading of an adjacent letter. This occurred with "g" and "h" twice and with "c" and "d" and with "s" and "t" once each. For example, the plaintext word "date" actually came out as "cate". With a keyletter of "U", plaintext "d" should have been enciphered as "X", but Kulp apparently slipped up and copied the adjacent "W" by mistake. This theory is partially verified by the fact that all three of these errors occurred relatively late in the message when the strain of encipherment might have resulted in such slips.

5. The remaining three errors are not as easily explained. With a keyletter of "A", the "r" of "Saturday" was enciphered as "Z" instead of "R". Could "Z"s look like "R"s in Kulp's handwriting? With a keyletter of "I", the "p" of "papers" was enciphered as "B" instead of "X". Finally, with a keyletter of "E", the "e" of "postmasters" was enciphered as "C" instead of "I". Why?

Footnotes

(1) The index of coincidence is calculated by the following formula:

$$I.C. = \frac{\sum_{i=A}^Z f_i (f_i - 1)}{N(N - 1)}$$

A value of .066 indicates a monoalphabetic distribution; the extreme opposite is given by .038, indicating a degree of polyalphabeticity or randomness.

(2) The Kasiski method is a system for determining the period of a polyalphabetic cipher by identifying repeated digraphs, trigraphs, etc. in the ciphertext. Assuming that most repetitions are the product of identical plaintext being enciphered by identical keyword letters, one can estimate the length of the keyword. For the history, and a more detailed explanation, see (2, pp. 207-213); for details of the technique of computations, see (1, pp. 127-129).

(3) The formula is:

$$M = \frac{.028(N)}{I.C.(N-1) - .038(N) + .066}$$

where M is the expected period or number of alphabets used, N is the number of letters in the message, and I.C. is the "index of coincidence" for the message (see footnote 1 above).

(4) The traditional method is to use sliding alphabetic strips on which the high-frequency letters are marked. One looks for the keyletter which produces the highest correlation between ciphertext high-frequency letters and plaintext high-frequency letters. For a discussion of the system, see (2, pp. 211-213).

REFERENCES

1. Helen Fouche Gaines, *Cryptanalysis*. (New York: Dover, 1956)
2. David Kahn, *The Codebreakers*. (New York: Macmillan, 1967)

Henry J. Gibson, Jr.'s Solution:

Your article, "Poe Challenge Cipher Finally Broken," in issue Number 1 of CRYPTOLOGIA was most interesting and provocative. Mark Lyster is certainly to be praised for personally testing a decision made over a century ago and unquestioned since. There can be no doubt that R. W. Kulp was falsely accused of pulling Poe's leg.

Acting from the premise that the cipher was legitimate, I followed Mr. Lyster's lead and submitted it to some statistical tests using APL/SV. Both the Kasiski and factored differences methods suggested it to be periodic with a key length of six or twelve. The two ct. MWs and the ct. MK arranged themselves nicely when the message was put into period, and cried out to be words beginning with pt. "i". Also, the ct. digraph NU, if equated to pt. "th", formed "with", "other", and "the".

Before assuming Mr. Kulp to be devious enough to use mixed alphabets, I tried fitting the message to a Vigenere tableau in period six and, lo and behold, plaintext began to emerge. But my pleasure was quickly tempered with frustration as large patches remained hopelessly garbled. Also, the keyword appeared random, though this was certainly acceptable.

Trying period twelve cleared up most of the trouble and resulted in the keyword "UNITED STATES" rotated one position to the left. As you are of course aware, the rotation was not an aberration on Mr. Kulp's part, but the result of a letter having been dropped from the second word of the message.

You asked for comment on the errors. Without seeing the original, handwritten message, this is difficult; but I think it fair to blame Mr. Kulp for the first error in the second "Saturday" and the first three errors in the last sentence. In each of these, the ct. is taken from one column or row away from where it should be. Ct. G is mistaken for Q every time the latter should appear; and this is certainly a simple misreading of the handwriting, as is, most probably, the splitting of the words "Courier" and "according", ct. J for I in "Alexander", ct. K for H in "Saturday", ct. P for A in "published", and ct. C for I in "postmasters". The remaining three errors — dropping the ct. I in "Alexander", ct. B for X in "papers", and ct. N for F in "according" — can only be guessed at. Incidentally, the misreading of Q caused me to consider the possibility that the alphabets used did not include Q, since it is the only letter with zero frequency.

Arthur J. Dore, Jr.'s Solution:

1. Each letter in the cipher was counted. The index of coincidence is 0.0474. The IC indicates a polyalphabetic substitution using three alphabets.
2. A trigram frequency was the next step. Every three-letter combination was listed. From this list, each two and three-letter combination that occurred more than once was noted. The number of letters between the repetitions was listed. The most frequently occurring distance was a multiple of six. This indicated that the cipher used a key of length six.
3. Six alphabets were initially selected. Each letter for the appropriate alphabet was counted. The IC's were within the ball park for the cipher. However, neither the alphabets nor any of the trigrams resulted in a break into the cipher.

4. The two alphabets with the highest IC's were used to develop digram substitutions. The digrams looked promising. Further attempts to expand the digrams to trigrams indicated that the actual number of alphabets in the cipher could be twelve as well as six.
5. The cipher was copied onto a separate piece of paper with every twelve letters aligned. This aided in the recovery of each alphabet. As the number of recovered alphabets increased, the cipher took on more meaning. The alignment of the letters also helped to determine the key "UNITED STATES".
6. Guessing and luck aided in coming up with the solution. Chances were that each alphabet was in alphabetical order from "a" to "z" without using a separate key for mixing the alphabet. The language of the plaintext was assumed to be English. Kulp probably wanted to add but one degree of complexity by using a keyword for the Vigenere substitution.

John Ambruz's Solution*:

After I made up my mind about what kind of a cipher it was, I used a probable word attack to solve the cipher. This decision was probably the most important step towards solution, and a lucky one for me to have made, as well. Obviously, Kulp might have thought of a great number of tricks to plague Poe with. But the cryptogram looked too much like an ordinary letter, so I assumed that every word in code stood for a word of plaintext; that every letter in code stood for some (not necessarily the same all the time) letter of plaintext; and that punctuation and spaces between words were not subject to any enciphering process. I also assumed the use of the simplest code (other than monoalphabetic) that I could think of, namely a Vigenere.

I thought that Kulp might have used some sort of a number code, such as 1, 2, 3, a basic quantum to be repeated several times. The only thing that worried me was that he might have done it with all 26 alphabets. (I had assumed the letter to have been written in English.) But even then the code would have repeated a few times. Anyway from this point on my approach was hadrdly systematic and as you will see I was lucky more than once.

The first word I tried, believe it or not, was —

XZY = the

which gave me the numerical key 4, 18, 20. The next step was to get, by hook or crook, the same or a similar combination of numbers from other words in the letter. I tried LAAM = then, and PHWKGNAMCUK = cryptograms, but these did not work. The key to the whole thing came next: I thought that since the last sentence was a question, the combination MK NUM must be "is the". "If the" was out, because the sentence was too short to contain a subordinate clause; and I had to try nothing else, for —

MK NUM = is the

gave me 4, 18, 20, 13, 8.

*Editor's note: A full account of Mr. Ambruz's well-analyzed solution was solicited after a letter was received from him with the following statements: "I am very surprised as I have never solved a cryptogram before, of any kind; in fact, I've never even tried to. I speculate that this perhaps is the reason for my success where Poe failed. Maybe too much knowledge confuses the mind."

Seeing the repetition of the numerical key, 4, 18, 20, I became convinced that I was on the right track.

Moreover, it was now apparent, assuming of course that I was right, that the word after XZY, namely ZMLWHFZEK, would have to have its first two letters deciphered by the application of the numerical key 13, 8 —

ZMLWHFZEK = me..... (13,8).

I now perhaps should have realized that "messenger" was appropriate, but Kulp (or somebody else) had forgotten to capitalize the "M". At any rate, in a dictionary I looked up all words which started with "me" and decided on "messenger" because it had the right length and because, so I thought, that word would likely appear in a cipher. Therefore, I wrote down —

LWHFZEK = ssenger (19, 4, 3, 18, 19, 0, 19).

Of course, I had no way of knowing that this was actually correct, and I went on a page-and-a-half excursion into nonsense; but I did get —

LBR = the (18, 20, 13)

and nothing further helped until I hit on —

LAAM = that (18, 19, 0, 19).

Fortunately, I remembered seeing the numerical key 19, 0, 19 before, a combination that stood in my mind; and almost immediately I guessed —

MO = to (19, 0)

and also —

MO MLW = to t.. (19, 0, 19).

I assumed that MLW was "the"; and the additional numerical key 4, 18 was recovered. The next word was WNBX, and as I had previously established 4, 18, 20, 13, 8 —

WNBX = cat. (20, 13, 8)

from which I constructed "gate" (the "c" is an error), thus gaining another 19.

Therefore, to this point I had two numerical key segments —

19, 4, 3, 18, 19, 0, 19

and

4, 18, 20, 13, 8, 19

but I did not know how they were joined together.

Perhaps I should be thankful that I had not backtracked from MO MLW WNBX, which might have been the sensible thing to do since I had more to work with (19, 4, 3, 18); since as you know there were two errors and a split word lurking in that area (ENWB ZWNGY = avco rdidg = according) which might have discouraged me from further efforts. Instead, I started from LBR and went backwards —

TX = .t (4)

which I assumed to be "at" and obtained 19. It was evident that this was not the 19 preceding the 4, 3; instead, I assumed it was the 19 that

followed the 0. Therefore, I had —

KWKE = here (3, 18, 19, 0).

At this point, I attempted to join the two segments of numerical key, above, together. Assuming that the 19 following the 8 to be the same 19 as that preceding the 4 gave me —

4, 18, 20, 13, 8, 19, 4, 3, 18, 19, 0, 19

and EJLVDXW became "arrives".

I continued to the end of the letter, applying numerical key and correcting mistakes as I went along ("cate" became "date", for example); and afterwards, I continued backwards towards the letter's beginning. I might say that the title gave me a bit of a problem. Backtracking, I came to —

G	E	J	E	A	S	G	D	X	V
13	8	19	4	3	18	19	0	19	4
t	w	q	a	x	a	n	d	e	r

which I thought to be "To Alexander". In order to get "Alexander", however, from "Qaxander", one additional letter had to be inserted. Putting in the additional letter gave me —

G	E		J	E	A	S	G	D	X	V	
20	13		8	19	4	3	18	19	0	19	4
m	r		a	l	e	x	a	n	d	e	r

and I saw that the letter correctly began "Mr. Alexander".

The numerical key of twelve numbers started at 20 and ended at the second 4. I was puzzled as to why Kulp selected these particular numbers, but apart from the fact that there are 12 months in the year at the moment I made no other observations. I sent you the solution. But two days later I happened to notice that if A=0, B=1, C=2,...,Z=25, starting at where I thought was the beginning of the numerical key, one would have —

20	13	8	19	4	3	18	19	0	19	4	18
U	N	I	T	E	D	S	T	A	T	E	S

A fact about Mr. Kulp which I find interesting is that he was in all likelihood a patriot: I myself would tend to use for the numerical key the numbers of my birthdate, or something else equally selfish, as perhaps most people would.

There may be methods which give you directly the keyword UNITED STATES; but since I had only obtained numbers - which by great ingenuity I had transformed into meaning - you will perhaps understand how overjoyed I was and why I rushed you a somewhat cryptic message. For a moment I believed myself to be in possession of an unknown fact!

Please do not be disappointed at perhaps my lack of systematic attack or failure to present a brilliant new method of solution. You must understand that I had nothing to lose when I sat down to play with the "words" of Kulp's letter at my leisure. My solution took me a little less than four hours. After this success I became more interested in ciphers; and I looked through an old book which contained cryptograms to be solved by the reader. (They were all, incidentally, monoalphabetic substitutions.) One of the great challenges, and one which the authors apparently took

especially great pride in giving, had a solution (which I had to look up in the back of the book) that ran something like this —

"Wing Ting Bing Sing Ring Ping King ... etc."

Now would you care to spend precious time attempting to solve something which at the end revealed nothing but this kind of nonsense? On the other hand, Kulp's cipher is very interesting because it speaks to us across 140 years, and gives us a little bit of the man who wrote it as well.