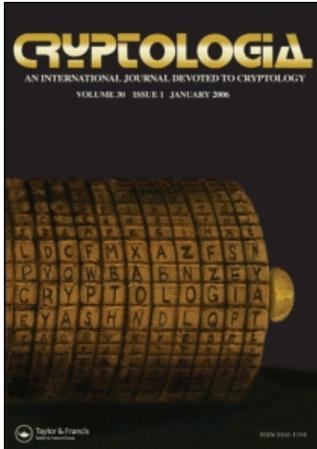


This article was downloaded by:[Winkel, Brian]  
On: 14 March 2008  
Access Details: [subscription number 769884566]  
Publisher: Taylor & Francis  
Informa Ltd Registered in England and Wales Registered Number: 1072954  
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



## Cryptologia

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

### POE CHALLENGE CIPHER FINALLY BROKEN

Brian J. Winkel

Online Publication Date: 01 January 1977

To cite this Article: Winkel, Brian J. (1977) 'POE CHALLENGE CIPHER FINALLY BROKEN', Cryptologia, 1:1, 93 - 96

To link to this article: DOI: 10.1080/0161-117791832823

URL: <http://dx.doi.org/10.1080/0161-117791832823>

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 FINALLY BROKEN

Brian J. Winkel

During the spring semester of 1975 I taught a cryptology course at Albion College. The course was open to all students and since the response was overwhelming I took 20 students on a first come, first serve basis. It was a general course, using a low level cryptanalysis text [8] supported by the book in cryptology [5]. We touched on many topics from history, literature and espionage, to cryptograms, various cipher schemes and their cryptanalysis, and computer encryption. For example we had discussions and presentations on the "Shakespearean" ciphers, a computer simulation of a Japanese rotor machine, secret ink usage, and the lack of security in linear feedback shift register sequences for key stream generation. This was a broad survey course.

As you might imagine, in any first attempt there were students whose enthusiasm dwindled. But there were students whose interest and participation grew. Among the latter was Mark Lyster, a senior chemistry major. Mark particularly enjoyed the elementary cryptanalysis we covered and he always had ideas on new attacks. He also gave the demonstration on secret inks.

It was late on the Sunday evening before the last week of classes when I received a phone call from Mark. He had been going over some of the materials on Edgar Allen Poe which I had placed on reserve at the library. He believed he was on to something.

In his column of December 18, 1839 in Alexander's Weekly Messenger [Philadelphia] Poe had challenged his readers to submit cryptograms (monoalphabetic substitutions) to him. He would "...read it forthwith---however unusual or arbitrary may be the characters employed" [1, p. 58]. In his February 26, 1840 column Poe discussed a message submitted by a G. W. Kulp [1, p. 92]. Poe showed that "...Mr. Kulp's

puzzle is not genuine" [1, p. 94]. In fact, Poe demonstrated, in his own words, "...as absolutely conclusive as any mathematical one can be," [1, p. 94] that the message was "...an imposition---that is to say, we fully proved it a jargon of random characters, having no meaning whatsoever." This last quote is from an essay by Poe, "A Few Words on Secret Writing," written a year after his demonstration in the Messenger [7, p. 34]. See [3, p. 270] for more details on the essay itself. It was the Kulp message that Mark wanted to discuss.

Incidentally the Kulp message along with much of Poe's other materials from the Messenger were lost to scholars until their recovery and republication in 1942 [1]. Previous to that time William F. Friedman had published two scholarly works on Poe as cryptographer [3, 4]. In 1943 William K. Wimsatt, Jr., a distinguished professor of English literature at Yale, published his scholarly work, "What Poe Knew About Cryptography," [9] in which the Kulp message is glanced over in a few sentences [9, p. 761]. Wimsatt must have been in touch with Friedman concerning the newly found Poe material for he acknowledges Friedman's expert advice at the same time he acknowledges receipt of "photostatic copies of the Poe items in the American Antiquarian Society Alexander's" [9, p. 754]. Unfortunately Professor Wimsatt died in 1975. And so, taken together with William Friedman's earlier death it can only be presumed that both men saw the Kulp message and either accepted Poe's proof without questioning the real cipher used by Kulp or chose not to devote any time to it. It is unlikely that had they asked themselves about the technique used by Kulp, they would have left it unnoticed, for there was great interest in the use of symbolism in American letters, enough to merit the pursuit of any trail in this area. Moreover, there were serious doubts about Poe's real ability, as well as his integrity, in the field of cryptology [6, p. 103; 2, pp. 28-29].

I knew all of this as Mark spoke and I myself had glanced through Poe's

rather nice proof of the impossibility of the Kulp message, never asking the important question, "What was Kulp's message?" Mark had done what teachers preach and, too often, do not practice. He began to ask the question, "What cipher system did G. W. Kulp of Lewiston, Pennsylvania, use in his(her) secret message of 1841?" Mark had used some computer programs, prepared by two students in our class, to do some statistical tests on the message. All of the notions used were taken from [8]. After several computer runs and some judicious guessing he believed he was getting some plain text. He was excited; I was excited. We worked off and on through our class breaks on Monday and by that night we had it. We did not break the Japanese Purple Machine! The message had little, if any, literary value! And, it was not all that hard, in hindsight!

But one of my students had dared to ask and then seek the answer with tools available from our course. With help from me, the teacher, he broke the message. That made my day, my week; in fact, it made the course for me.

We want you to give the message a try. We reproduce it below. Some final comments are worth noting. Poe said in his July 1841 article that "...had it been a 'genuine article', it would not have been written in as free and running a hand as it is---a hesitation would have been apparent about the characters" [1, p. 92]. We determined several errors. You should make your own conclusions as to the nature of these errors. We have several possible answers which we shall not suggest to you, but we suggest you send us your solution to the cryptogram with some idea as to how you did it along with your conjectures on the errors. We shall list solvers and interesting points on solutions and the errors in a future issue of CRYPTOLOGIA.

Ge Jeasgdxv,

Zij gl mw, laam, xzy zmlwhfzek ejlvdxw  
 kwke tx lbr atgh lbmX aanu bai Vsmukkss pwn  
 vlwk agh gnumk wdlnzweg jnbxvv oaeg enwb  
 zwmgY mo mlw wnbx mw al pnfdcfphk wzkeX  
 hssf xkiyahul. Mk num yexdm wbxY sbc hv  
 wyx Phwkgnamcuk?

## REFERENCES

1. Clarence S. Brigham, "Edgar Allen Poe's Contributions to Alexander's Weekly Messenger", Proceedings of the American Antiquarian Society, April, 1942, pp. 45-125.
2. Killis Campbell, The Mind of Poe and Other Studies, Harvard University Press, Cambridge, Massachusetts, 1933.
- \*3. William F. Friedman, "Edgar Allen Poe, Cryptographer", American Literature, 8 (November, 1936) pp. 226-280. (Reprinted in Signal Corps Bulletin, No. 97 (July-September, 1937) pp. 41-53.)
- \*4. William F. Friedman, "Edgar Allen Poe, Cryptographer (Addendum)", Signal Corps Bulletin, No. 98 (October-December, 1937) pp. 54-75.
5. David Kahn, The Codebreakers: The Story of Secret Writing, Macmillan, New York, 1967.
6. Joseph W. Krutch, Edgar Allen Poe: A Study in Genius, Alfred A. Knopf, New York, 1926.
7. Edgar Allen Poe, "A Few Words on Secret Writing", Graham's Magazine, 19 (July, 1841) pp. 33-38.
8. Abraham Sinkov, Elementary Cryptanalysis, A Mathematical Approach, Random House, New York, 1968. [Now available in The New Mathematical Library of the Mathematical Association of America, Washington, D.C.]
9. William K. Wimsatt, Jr., "What Poe Knew About Cryptography", Publications of the Modern Language Association, 58 (1943) pp. 754-779.

\*Editor's Note: Both Friedman articles were reprinted in Articles on Cryptography and Cryptanalysis Reprinted from the Signal Corps "Bulletin", Government Printing Office, Washington, 1942 and are currently available in Cryptography and Cryptanalysis Articles, Vol. II, Ed. William F. Friedman, Aegean Park Press, Laguna Hills, California, 1976.