This article was published in
Cryptologia
Volume 6 Number 4 October 1982, pp.378-382

A BASIC PROBE OF THE BEALE CIPHER AS A BAMBOOZLEMENT*

LOUIS KRUH

[* This is a transcript of a slide illustrated talk delivered by the author at the Third Beale Cipher Symposium, held 12 September 1981 in Arlington, VA]

What would the average, red-blooded American do if he found a mysterious cipher that was said to give the location of a $30,000,000 treasure of gold, silver and jewels?

The same as any normal person engulfed by avarice, greed and a primordial urge to become rich in a quick and easy fashion. He would spend as much time as he could trying to solve the cipher.

But how about trying to prove that the cipher is a hoax. How much time would you invest? Well, given the opportunity to become a millionaire by solving a cipher, what would you do? The answer is obvious. If you manage to destroy the legitimacy of the secret instructions which may lead to the treasure, you eliminate any possibility of finding $30,000,000 so why do that. Why shatter any dreams you have of retiring a rich man. Besides, Carl Hammer, through the use of a computer, has already proved that the Beale cipher is not just a random jumble of numbers and that it is a genuine cipher. [1] And when a computer is involved in any kind of analysis you know what that means - it is prima facie evidence of a clear, cold, calculating logic that is indisputably correct in accomplishing whatever task has been assigned to it. But, while Carl may have shown that a genuine message is hidden in the jumble of numbers did he prove that the message, once deciphered, would be a sensible one or that its plaintext, if ever read, would lead to a treaure. Obviously, even if the message is a genuine encipherment of a legitimate message, it could still be a hoax. But who wants to spend time proving that possibility. I don't, but I did spend a few hours along those lines, which I would like to share with you.

There were three events which triggered my research. First, I had the great pleasure of interviewing Frank Rowlett. During our talk he mentioned that William F. Friedman had him and his colleagues in the Signal Intelligence Service working on the Beale cipher as part of their training program and that they had concluded it was a hoax. An interesting sidelight is that in the story about the interview, which appeared in Cryptologia, [2] I mentioned that Rowlett had run across two similar legends, one of which involved an enciphered text. Subsequently, despite the myriad of fascinating historical subjects covered in the article, every letter received about the story only wanted to obtain details on the other hidden treasures.

In the same vein, it should be noted that the curator at the Friedman Collection at the George C. Marshall Research Foundation reports that requests for information from its files on the Beale cipher outnumber all other queries. I guess it is more evidence of that primordial urge mentioned earlier.

The second of the three events was receipt of a decipherment of the Beale cipher from a friend. I was amazed by what appeared to be an unambiguous, systematic and legitimate solution. In later conversations with Carl Hammer and Carl Nelson I was doubly amazed to learn that they have seen several other decipherments which appear logical and not at all forced.

Event three was the acquisition of a review of Ronald Clark's biography of Friedman by Soloman Kullback, which appeared in an intelligence agency publication. In it, Kullback recalls their work on the Beale cipher and wrote that, "Based on a statistical stylistic comparison of the text of the documents, using procedures since employed in other published historical cases of disputed authorship, we conclude that the writers of the two texts were the same person and thus that the whole affair was a hoax." His reference to two texts was to "one supposedly written by Thomas Jefferson Beale … and one by the supposed finder of the documents a generation or two later." The latter person was undoubtedly James Ward who received the Beale material from Beale's friend, Robert Morriss, in 1862, 40 years after Beale had left the papers with Morriss.

My interest was now sufficiently piqued that I visited the New York Public Library to find out something about "stylometry", which, according to Webster's unabridged 3rd Edition, is "the study of the chronology and development of an author's work based especially on the recurrence of particular turns of expression or trends of thought."

As one author on the subject, C. B. Williams, in his book, Style and Vocabulary: Numerical Studies, points out, it refers to "… fingerprints in writing, of which the author is quite unconscious but could be revealed by some mathematical or statistical reasoning." [3] Another book worth reading for background purposes, and which may be easier to obtain, is Andrew Morton's Literary Detection: How to prove authorship and fraud in literature and documents. [4]

The books recommend a variety of statistical techniques for stylistic comparison purposes. One very important comparison is the average number of words used in a sentence. Being a rather simple procedure I decided to experiment by comparing the writing of Ward with the writing of Beale. For Ward, I used his 1885 pamphlet, "The Beale Papers", as contained in the Beale Cypher Association's reprint of the George L. Hart, Sr. essay. [5] For Beale, I used his letters of January 4, 5, and May 8, 1822, to Robert Morriss plus the decipherment of cipher number two, which are part of Ward's pamphlet.

According to my count, the Ward pamphlet, omitting other than Ward's writing, i.e., Beale's letters and ciphers, contains 164 sentences and 4,727 words.

Beale's letters and his deciphered message contain 95 sentences and 2,731 words. This means that the average sentence word length for Ward is 28.82 and for Beale it is 28.75 - an incredible similarity. Of course, one test result does not justify a conclusion but it certainly calls for further investigation.

Other suggested analyses include a count of the words common to both writers and the number used only by one author, occurences of certain words like "and" plus comparisons of the first, second, and third words used in each sentence. There are other tests but these should give you an idea of the kinds of analyses involved. Nothing exceptionally difficult but undoubtedly tedious without the use of a computer.

Over the years many others have expressed doubts about the Beale story and its famed ciphers. For example, after Colonel George Fabyan, owner of the famed Riverbank Laboratories, examined the ciphers, he wrote, "It seems improbable to us that a cipher of this character could be deciphered by a novice without the key, regardless of whether he put 20 years or 40 years on it. … The stumbling of a novice upon a method of this character lies rather beyond the range of possibility …" [5]

Another example involves M. E. Ohaver, who, during the 1920's and 1930's edited the column, "Solving Cipher Secrets" in some detective pulp magazines. Ohaver, known as Sunyam in the American Cryptogram Association, was sent a copy of the ciphers in 1927 by John Ingles, [6] a Virginia insurance company executive, who said he was related to Thomas Jefferson Beal (sic.) [7]

Ohaver later wrote to Ingles that cipher number three was rather peculiar because it purports to give the names of "Parties and Their Residences" but consists of only 618 numbers, each presumably representing a letter. It is supposed to contain the names and addresses of the relatives and others to whom they devise their respective shares. In other words, according to Ohaver, "… we have here sixty names and addresses represented by only 618 numbers, which would take about 5 or 6 letters for each name, which seems to me a rather small number." [8] The same point was made by Herbert O. Yardley years later when he wrote that the number three cipher "… is not long enough to contain all the names of the so-called heirs." [9]

Some other anomalies. After Ward received the papers from Morriss, according to his own words, he "arranged the papers in the order of their length, and numbered them …" [5] Note that the ciphers which had been identified by Ward as numbers 1, 2, and 3 contain 520, 763, and 618 elements respectively. Obviously, they are not arranged in the order of their length. Supposedly, he

either made a mistake at the outset, or, more likely, reversed his numbering of 2 and 3 after solving (?) what is now identified as cipher number 2 but which he probably first marked as number 3 because it was the longest of the three ciphers. The reason for renumbering would be that the solution (?) gives the location of the treasure as being in cipher number 1 and says the names and addresses of the party are in cipher number 3. Therefore, the solved cipher becomes number 2 automatically.

Nowhere, however, does Ward indicate by what divine guidance he had been able to determine which of the two unsolved ciphers was number 1 and which was number 3. Nevertheless, his trustworthiness is apparently so beyond reproach that to this day virtually everyone accepts as an undisputed fact his labeling of one cipher as number 1 and the other as number 3.

But here the most curious questions of all. First, how did Beale, who allegedly wrote the message found in cipher number 2, know that it would be deciphered first? Because if it wasn't, his references to the other ciphers would not make sense. And, secondly, if he was confident it would be deciphered first, why didn't he refer to the other ciphers as number 2 and number 3, which would have been the normal and logical thing to do.

Our last example and a recent one is an article by Jim Gillogly in Cryptologia. [10] In addition to demonstrating why cipher number 1 may be a hoax, Jim bolsters his contention by asking why Beale would have ended cipher number 2 with "Paper number 1 describes the exact location of the vault, so that no difficulty will be had in finding it" when that sentence would be redundant after paper number one is deciphered. He suggests that, "the author wanted to sell the idea that the first document was worth reading."

The only point with these examples is to illustrate that there is a great deal of justification for viewing the Beale story as a bamboozlement. I think I have demonstrated that in a scientific fashion. Now it is up to some Beale Cypher Association members with computer capabilities to take the time to complete the necessary analyses and, perhaps, put the issue to rest. Then, we can devote all out time and energy to solving the Shakespearan ciphers and find out who really wrote those plays.

References

1. Hammer, Carl. 1970. Signature Simulation and Certain Cryptographic Codes. Washigton: Computer Services UNIVAC.

2. Kruh, Louis. 1980. Reminiscences of a master cryptologist. Cryptologia. 4: 45-50.

3. Williams, C. B. 1970. Style and Vocabulary: Numerical Studies. London: Charles Griffin and Co.

4. Morton, Andrew. 1978. Literary Detection: How to prove authorship and fraud in literature and documents. New York: Charles Scribner's Sons.

5. The Beale Ciphers. 1978. Medfield, MA. The Beale Cypher Asscociation.

6. Letter from John Ingles to M. E. Ohaver. January 3, 1927.

7. Letter from John Ingles to Editor, Flynn's Weekly. December 22, 1926.

8. Letter from M. E. Ohaver to John Ingles. August 8, 1933.

9. The Cryptogram. 1954. Vol. XXIII No. 6, 93-120.

10. Gillogly, James J. 1980. The Beale cipher: A dissenting opinion. Cryptologia. 4: 116-119