A note on cryptologic aspects of the Waberski trial

David Joyner*

2013-07-30

Abstract

Lothar Witzke, also known as Pablo Waberski, was arrested in Arizona on February 1, 1918 crossing from Mexico into the United States. A 424-letter cryptogram was found sewn into the left upper sleeve of his jacket. This note gives Manly's description of his solution of the cipher from the court testimony he gave at the military trial.

Lothar Witzke, also known as Pablo Waberski (see Figure 1), was arrested in Arizona on February 1, 1918 crossing from Mexico into the United States. A 424-letter cryptogram was found sewn into the left upper sleeve of his jacket. In his 1931 book [Y], Yardley describes his detailed solution of the cipher. However, as Kahn points out [Ka2], Yardley did not solve the cipher, John Manly did (assisted by "Miss Dickens," who was probably a trained crypto clerk). As this is an important occasion in American history, it is worth while having Manly's description of his solution of the cipher. This was taken from the court testimony he gave at the Ft. Sam Houston military trial, which concluded with his sentencing on November 2, 1918.

Manly edited a section of the transcript of that trial that explains most lucidly the process which led codebreakers like himself and Elizebeth Smith Friedman to a successful decoding of the spy's secret messages, and must typify the testimony she gave at so many trials. The material below was found in an endnote in Kyle's unpublished biography of Elizebeth Smith Friedman (see [Ky], page 209), but can also be found among the papers of ESF collected at the Marshall Foundation, Lexington VA [EF].

*wdjoyner@gmail.com.

Figure 1: Lothar Witzke, aka Pablo Waberski, circa 1918

Q. Do you recognize these papers?

A. Yes.

Q. What are they?

A. This one is a cipher message submitted to me for solution. The other contains my decipherment and a translation of it from German into English ...

Q. Is there any possibility that another cipher expert could obtain a different decipherment?

A. It is not possible.

Q. Is the translation correct?

A. It is as accurate as I could make it, and no correct translation could differ from it materially.

Q. Can you explain to the court the method by which you obtained the decipherment?

A. I will attempt to do so if you will interrupt me for questions on any point that is not entirely clear.

Q. Proceed.

A. The first step was to ascertain the general type of cipher.

Q. What do you mean by type?

A. Ciphers may in general be divided into two types, substitution ciphers and transposition ciphers. Substitutions ciphers

are those in which the letters of the original message are replaced by other letters of the alphabet, by figures, or by arbitrary signs. For example a may be represented by s or any other letter, or by 7 or any other number, or by a triangle or any other sign. In a transposition cipher, on the other hand, the letters of the original messages are kept but are transposed from their normal positions in the words of the message to other positions according to some definite system.

Q. Is it necessary that they should be transposed according to a system? Could they not be transposed unsystematically or capriciously?

A. An unsystematic transposition would not give a cipher but a jumble of letters which could not be read by the person for whom the message was intended. He is able to read the cipher only because he knows the system of the disarrangement and from this knowledge is able to restore the disarranged letters to their original positions forming the words of the original message.

Q. How do you determine to which type a cipher message belongs?

A. By counting the letters and making a frequency table, which is then compared with a normal frequency table. If the agreement between the two tables is close, the cipher belongs to the transposition type; if not, it must be a substitution cipher.

Q. What do you mean by a frequency table?

A. A table which shows how many times each letter of the alphabet is used in a message of given length, say 100, 200, or 1000 letters. The normal frequency tables are based upon larger counts, say 10,000 letters, and show the number of times each letter may be expected to occur in a passage of similar length.

Q. Are statistics thus obtained accurate and absolute; that is, does a letter always occur with the same frequency?

A. The statistics are accurate but not absolute; that is, variations from the normal frequencies occur according to subject matter and in short messages. Thus in messages of less than 100 letters the variations are often considerable, but not enough to make the frequency table unreliable.

Q. Do the frequency tables differ for different languages?

A. Yes, but there is a general resemblance between the fre-

quency tables for the principal western European languages, such as English, French, German, Spanish, Italian, etc.

Q. With what frequency tables did you compare that obtained from this message?

A. With the tables for English, German, and Spanish.

Q. Why those languages?

A. Because the paper was found in the hands of an alleged German spy who had been operating in the United States and had lately come from a Spanish speaking country.

Q. What was the result of the comparison?

A. The frequency table showed that the message was a transposition cipher and suggested that it was German.

Q. How was this conclusion indicated?

A. As the message contained no q's, it was almost certainly not Spanish, for the word que is very common in Spanish. As it contained only two w's it was probably not English, for in a message of this length there should have been approximately six w' s. Besides, the very high frequency of e and n indicated that it was German.

Q. What was the next step?

A. To find and bring together letters which certainly must have been together in the original message. A beginning was made by making use of the fact that in the German language the letter c never occurs except before an h or a k. A list was therefore made of all the c's in the cipher and the positions which they occupied, and a similar list of all the h's and k's and their positions. It was then discovered that certain of the c's were separated from one another by the same intervals as certain of the h's, and it was concluded that these c's belonged with these h's. As it further appeared that each of the h's was separated from its corresponding c by an interval of 108 letters, it was safe to conclude that the first step in the transposition of the original message bad resulted in moving each letter 108 spaces from the letter preceding it.

Q. How could this be done?

A. By writing the letters of the original message in columns of 108. This would give four columns, but as there are only 424 letters in the message the last column would be short by eight

letters. (Here he writes the message on a blackboard for the jury.)

Q. Is it possible to read the message in the form obtained by this process?

A. No, this is only the first step in the decipherment. The cipher has now been reduced to groups of four letters (the last eight groups contain only three) . The letters are in the correct order in the groups, but the groups are not in proper order and still require to be rearranged according to the proper system.

Q. How was this done?

A. The process is long and difficult. It was easy to bring together groups which would make interchangeable German words, and parts of sentences, but it was necessary to bring them together in accordance with some system or we could not be sure that the result was the original arrangement.

Q. What did you do next?

A. We experimented with arranging the groups into columns, because a transposition by columns is a very common form of cipher. As there were 108 groups, which would give either three columns of 36 groups each or six columns of 13 groups each or nine columns of 12 groups each or twelve columns of ten groups each, we tried the arrangem':nt into twelve blocks or columns of n1ne groups each, as being the most probable arrangement, and this proved to be correct.

Q. How did you proceed?

A. Examining the columns for groups which could be fitted together with certainty I observed that the first group in the second column was KMEX. As the bearer of the message had just come from Mexico, I assumed that the group which followed it would complete the word Mexico, probably spelling it with a K, as is usual in German. The only group which gave this word was the group IKOP in the fourth line of the same column. I then examined the message to see if the first line of each column could be joined to the fourth line to make good German words or parts of them. This supposition also turned out to be correct, and I knew that I was on the track of the system. The successive columns gave the following results (the slanting lines marking off the words or parts of words):

1. SCHAFT I AL
2. K/MEXIKO/P
3. B/ZUSENDE
4. SKI/ALS/RU
5. ICHEN/DER
6. N/KOMMA/ IH
7. SEND/PESO
8. EHOERIGE
9. EHEIM/AGE
10. ANSUCHEN
11. ICHEN/KON
12. D/SEINE/C

I then examined the groups thus formed to see which pointed to an unmistakable continuation. The most promising was number 9, in which the letters EHEIM were clearly the last letters of the word GEHEIM, meaning secret, and the letters AGE clearly the beginning of the word AGENT, meaning agent. As this group began with the first line of column 9, the group preceding it was looked for in column 8. The only group in that column ending in a G was group 8. In like manner the continuation of the ninth group of eight letters was looked for in column 10, and was found in line 3. NT?PU. Experiment showed that if one of the twelve groups of ten letters that had been obtained could be extended in a similar manner it would give intelligible parts of German words and sentences. For example, number 12 thus extended gave EN/UND/SEINE/CODE/T. The T following CODE suggested the word TELEGRAM, and the letters necessary to make it were found in the two following columns–ELEG, line 6 of column 2, and RAMM in line 5 of column 3. As every one of the groups could be extended in similar fashion by taking the sixth and fifth lines of the next two columns, it was clear beyond a doubt that the system discovered was the system used by the cipher makers. The result of this step of the process was to give twelve series of nine groups each, showing the same series of intervals between

> the first letters of the groups. It is clear from an examination of the beginnings and ends of these series that they will fit into one another in only one possible order, and this order gives the message as deciphered.

Witzke/Waberski was found guilty and sentenced to death. However, in 1920 President Wilson commuted his sentence to life imprisonment. In 1923 President Calvin Coolidge, ordered him deported to Berlin.

References

[EF] Collected Papers of Elizebeth Smith Friedman at the George C. Marshall Foundation, Lexington, Virginia, USA.

[Ka1] D. Kahn, *The Codebreakers*, revised edition, Scribner, Boston, 1996.

[Ka2] ——, *The Reader of Gentlemen's Mail: Herbert O. Yardley*, Yale University Press, New Haven, 2004.

[Ky] Katie Letcher Kyle, *Divine Fire*, unpublished manuscript, 223 pages, 1991.

[Y] Herbert O. Yardley, *The American Black Chamber*, Naval Institute Press, 2013.