Readers interested in seeing details of how the decipherments were obtained are referred to the original explanation published in *The Cryptogram*, but be warned, the solver described his method as "simple but extremely tedious."[11] He did not make use of a computer!

Trust, But Verify

In the April 1993 *Cryptologia* piece in which he presented Mauborgne's 1915 unsolved cipher, Kruh wrote, "The cipher was published in *The Cryptogram*, the official publication of the American Cryptogram Association, early last year." But it wasn't in a 1992 issue. It actually appeared in the March–April 1991 issue, p. 7, under Kruh's ACA pen name MEROKE.

So he made a mistake in a citation. He probably anticipated having his *Cryptologia* paper see print in 1992, and when it was delayed to the following year, he forgot to update the "early last year" reference to the previous piece. Big deal. Surely he would take care in the more important task of transcribing the cipher, right?

Rather than simply accept Kruh's presentation of Mauborgne's cipher, as a suspicious cryptologist, I wanted to see the original document. Perhaps Kruh left out something that might give us further insight into the solution, or more seriously, perhaps he made an error in copying the cipher letters for his article. Sadly, there's precedent for the latter.

Kruh and two coauthors wrote about yet another challenge cipher, actually a set of three of them, in a paper published in 1990. These ciphers were created using a system John F. Byrne designed in 1918 and called Chaocipher.[12] Byrne tried repeatedly for almost forty years to interest the U.S. government in his system, without success. He died in 1960, but his son, John Byrne, knew how the secret system worked and wished to continue promoting his father's work with the new challenge. Although the third cipher was presented correctly, the other two contained errors.

The most serious errors occurred in the second cipher. It was presented as

```
ENWSC EAQGI VIDEM WUMSN ZMNTV UFDLB JKKMR HHSNB KTJBH
VPTWH FMQQJ PGRWF FVJMD HFUZO XEOZT MKZSA MJYRL SQSXU
ZYEKR JBFRE SGGFX FEGXL PWTWL ZAVIM TBDTQ BLVRZ VEMMT
LXITZ
```

The deciphered message should have been

> Our own memories are mysterious enough even to ourselves and we should recognize that they do not exist in space only in time and that they are in all respects immaterial.

But this couldn't be obtained. The third grouping of ciphertext letters, VIDEM, was wrong. It should have been written UIOEM. Misrepresenting U as V and O as D in the ciphertext meant that even someone applying the correct deciphering algorithm (which was kept secret) with the correct key (also secret!) would get only this:

> OUROW NMEMO OIPXA AEJZG GRYTF NYMRS DJOIM USHNV LLFIN WOJWK JAGTA MUQVR CBGGS HJAMW CCRGY JKAEY SPFAP PMHPZ VXWFQ DGHXA HKHRJ EWLST ALBPT JSZAQ HQXVI WBLIC QTHQJ MZVWU[13]

The paper with this serious error was not written by Kruh alone. He had two coauthors, one of whom was John Byrne, the son of the creator of the system! Knowing that this cipher was misrepresented by Kruh, and that he also made an error in reproducing the cipher alphabets for Mauborgne's later challenge, it doesn't take a leap of faith to imagine that Mauborgne's 1915 cipher could have been misrepresented as well.

So I contacted a librarian at the New York Public Library's Rare Book Division, asking for scans of the relevant papers, just to make sure I was presenting an accurate version of Mauborgne's 1915 cipher. Here's the response I got:

> *Dear Craig,*
>
> Thanks for your email regarding the cipher question. I have searched in our catalogs and have scanned our shelves—I cannot locate an item that matches this in our collection. The description is well intended, but as you point out there is no call number (or exact title) and that makes tracking this down a bit difficult. If you do come across any other references, please do let me know, and I will continue the search for you. There is a 1912 imprint that we have in the regular collection that is authored by Mauborgne, but this pre-dates your reference. Please let me know if I can be of any more assistance and best of luck.

Best,
Kyle R. Triplett, Librarian
Brooke Russell Astor Reading Room for
Rare Books and Manuscripts
The New York Public Library
Archives, Manuscripts, and Rare Books
Stephen A. Schwarzman Building,
Room 328
476 Fifth Avenue, New York, NY 10016
manuscripts@nypl.org

So, until these pages turn up, or a copy of them is found elsewhere, we have yet another doubt to contend with!

Chapter 8: A Challenge Cipher

1 In 2011, Steven Bellovin uncovered the fact that the one-time pad had, in fact, only been rediscovered by Mauborgne and Vernam. It was previously known to Frank Miller and was published by him in an 1882 commercial code book. For details, see Steven M. Bellovin, "Frank Miller: Inventor of the One-Time Pad," *Cryptologia* 35, no. 3 (July 2011): 203–22.

2 A line from the film *Fight Club*.

3 A line from the film *Saw*.

4 A line from the film *Freddy Got Fingered*.

5 It was re-presented by William F. Friedman, who had already solved it but delayed revealing his solution until the next issue to give readers a chance to attack it for themselves.

6 Taken here from Louis Kruh, "A 77-Year Old Challenge Cipher," *Cryptologia* 17, no. 2 (April 1993): 172–74.

7 Kruh, "A 77-Year Old Challenge Cipher," 172.

8 Louis Kruh, "Riverbank Laboratory Correspondence, 1919 (SRH-50)," *Cryptologia* 19, no. 3 (July 1995): 236–46.

9 A line from the film π.

10 Thanks to Moshe Rubin for helping me identify this individual.

11 TRIO (ACA pen name for Fenwick Wesencraft), "Solutions of the M-94 Test Messages," *The Cryptogram* 48, no. 8 (November–December 1982): 6–7.

12 Byrne promoted the system most famously in John F. Byrne, *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* (New York: Farrar, Straus and Young, 1953).

13 The error was pointed out in Jeff Calof, Jeff Hill, and Moshe Rubin, "Chaocipher Exhibit 5: History, Analysis, and Solution of *Cryptologia*'s 1990 Challenge," *Cryptologia* 38, no. 1 (January 2014): 1–25.

Chapter 9: More Challenge Ciphers

1 For a fuller account of this episode of government censorship, see Craig Bauer and Joel Burkholder, "From the Archives: Reading Stimson's Mail," *Cryptologia* 31, no. 2 (April 2007): 179–84.

2 Alexander d'Agapeyeff, *Codes and Ciphers* (London: Oxford University Press, 1939), front inside dust jacket.

3 d'Agapeyeff, *Codes and Ciphers*, 62–63.

4 J 77/2621/1445, Divorce Court File: 1445. Appellant: Josephine Christian Lilian Passy d'Agapeyeff. Respondent: Alexander d'Agapeyeff. Type: Wife's petition for divorce [WD], 1929, The National Archives, Kew, England.

5 Ralph Erskine and John Gallehawk located and photographed d'Agapeyeff's SOE file for me, but it didn't indicate why he was turned down. The reference is Special Operations Executive: Personnel Files (PF Series). Alexander d'Agapeyeff, Collection: Records of Special Operations Executive, 01 January 1939–31 December 1946, HS 9/9/5, The National Archives, Kew, England. Erskine thought it was doubtful that d'Agapeyeff was turned down because of the adultery. He pointed out, "Sir Stewart Menzies, head of the UK SIS, had at least 1 mistress, and was also divorced. Hinsley said privately that Godfrey, the Director of Naval Intelligence had a number of women." On the other hand, when interviewing potential new hires, NSA

Psychical Research 24, no. 2 (April 2001): 82–91, available online at http://www.innerknowing.net/research.html.

Schwartz, Gary E., with William L. Simon, foreword by Deepak Chopra. *The Afterlife Experiments, Breakthrough Scientific Evidence of Life After Death* (New York: Pocket Books, 2002).

Smith, Susy (pen name of Ethel Elizabeth Smith). Introduction by Gary E. R. Schwartz and Linda G. S. Russek. *The Afterlife Codes: Searching for Evidence of the Survival of the Human Soul* (Charlottesville, VA: Hampton Roads Publishing Company, Inc., 2000).

Stevenson, Ian. "The Combination Lock Test for Survival." *Journal of the American Society for Psychical Research* 62 (1968): 246–54.

Stevenson, Ian. "Further Observations on the Combination Lock Test for Survival." *Journal of the American Society for Psychical Research* 70 (1976): 219–29.

Stevenson, Ian, Arthur T. Oram, and Betty Markwick. "Two Tests of Survival After Death: Report on Negative Results." *Journal of the Society for Psychical Research* 55, no. 815 (April 1989): 329–36.

Thouless, Robert H. "A Test of Survival." *Proceedings of the Society for Psychical Research* 48 (July 1948): 253–63.

Thouless, Robert H. "Additional Notes on a Test of Survival." *Proceedings of the American Society for Psychical Research* 48 (1948): 342–43.

Tribbe, Frank C. "The Tribbe/Mulders Code." *Journal of the Academy of Religion and Psychical Research* 3, no. 1 (January 1980): 44–46.

Winkel, Brian J. "A Tribute to Alf Mongé." *Cryptologia* 2, no. 2 (April 1978): 178–85.

Wood, T. E. "A Further Test for Survival." *Proceedings of the Society for Psychical Research* 49 (1950): 105–6.

Chapter 8

Bauer, Craig. *Secret History: The Story of Cryptology* (Boca Raton, FL: Chapman and Hall/CRC, 2013).

Bauer, Craig, and Elliott Gottloeb. "Results of an Automated Attack on the Running Key Cipher." *Cryptologia* 29, no. 3 (July 2005): 248–54.

Bauer, Craig, and Christian N. S. Tate. "A Statistical Attack on the Running Key Cipher." *Cryptologia* 26, no. 4 (October 2002): 274–82.

Bellovin, Steven M. "Frank Miller: Inventor of the One-Time Pad." *Cryptologia* 35, no. 3 (July 2011): 203–22.

Byrne, John F. *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* (New York: Farrar, Straus and Young, 1953).

Byrne, John, Cipher A. Deavours, and Louis Kruh. "Chaocipher Enters the Computer Age When Its Method Is Disclosed to *Cryptologia* Editors." *Cryptologia* 14, no. 3 (July 1990): 193–98.

Calof, Jeff, Jeff Hill, and Moshe Rubin. "Chaocipher Exhibit 5: History, Analysis, and Solution of *Cryptologia*'s 1990 Challenge." *Cryptologia* 38, no. 1 (January 2014): 1–25.

Friedman, William F. "The Cryptanalyst Accepts a Challenge." *The Signal Corps Bulletin* 103 (January–March 1939).

Griffing, Alexander. "Solving the Running Key Cipher with the Viterbi Algorithm." *Cryptologia* 30, no. 4 (October 2006): 361–67. This is the best paper on the topic of breaking running key ciphers.

"Historical Survey of Strip Cipher Systems." This is available from NARA; NSA Historical Collections 190/37/7/1, NR 3525 CBRK24 12957A 19450000.

"History of Army Strip Cipher, SRH-366." This is available from NARA; RG 0457: NSA/CSS Finding Aid A1, 9020 U.S. Navy Records Relating to Cryptology 1918–1950 Stack 190 Begin Loc 36/12/04 Location 1-19.

Kruh, Louis. "The Genesis of the Jefferson/Bazeries Cipher Devices." *Cryptologia* 5, no. 4 (October 1981): 193–208.

Kruh, Louis (under his ACA pen name, MEROKE). "The M-94 Test Messages." *The Cryptogram* XLVIII, no. 6 (July–August 1982): 4–5, available online at http://www.prc68.com/I/M94TM.htm.

Kruh, Louis (under his ACA pen name, MEROKE). "A 77-Year-Old Challenge Cipher." *The Cryptogram* (March/April 1991): 7.

Kruh, Louis. "A 77-Year-Old Challenge Cipher." *Cryptologia* 17, no. 2 (April 1993): 172–74. Note: Mauborgne is misspelled in this paper, and the reference to the paper in *The Cryptogram* leads one to look in early 1992 issues, when it is actually March/April 1991.

Kruh, Louis. "Riverbank Laboratory Correspondence, 1919 (SRH-50)." *Cryptologia* 19, no. 3 (July 1995): 236–46.

Mauborgne, Joseph O. *Practical Uses of the Wave Meter in Wireless Telegraphy* (New York: McGraw-Hill Book Co., 1913).

Mauborgne, Joseph O. *An Advanced Problem in Cryptography and Its Solution* (Fort Leavenworth, KS: Press of the Army Services Schools, 1914). A second edition appeared in 1918.

Mauborgne, Joseph O. *Data for the Solution of German Ciphers: Also a Diagram of Cipher Analysis* (Fort Leavenworth, KS: Army Service School Press, 1917).

Mauborgne, Joseph O. "One Method of Solution of the Schooling 'Absolutely Indecipherable' Cryptogram." *The Signal Corps Bulletin* 104 (April–June 1939): 27–40.

Mauborgne, Joseph O. "Reminiscences of Joseph Oswald Mauborgne: Oral History." 1971 (held in Columbia University Library's rare book collection).

Smoot, Betsy Rohaly. "Parker Hitt's First Cylinder Device and the Genesis of U.S. Army Cylinder and Strip Devices." *Cryptologia* 39, no. 4 (October 2015): 315–21. It was long believed that Hitt came up with his version of the cipher wheel in 1913. This paper shows that it was 1912. So, it shouldn't surprise anyone if Mauborgne's version turns out to be a little older than believed as well!

Wesencraft, Fenwick (under his ACA pen name TRIO). "Solutions of the M-94 Test Messages." *The Cryptogram* XLVIII no. 8 (November–December 1982): 6–7, available online at http://www.prc68.com/I/M94S.htm.

Chapter 9

ON D'AGAPEYEFF'S CIPHER

Barker, Wayne G. "The Unsolved d'Agapeyeff Cipher." *Cryptologia* 2, no. 2 (April 1978): 144–47.

d'Agapeyeff, Alexander. *Codes and Ciphers* (London: Oxford University Press, 1939).

d'Agapeyeff, Alexander. *Maps* (London: Oxford University Press, 1942). Some online sources claim that this book appeared before d'Agapeyeff's *Codes and Ciphers*, but that's not correct.

d'Agapeyeff cryptogram revisited, http://www.rodinbook.nl/dagapeyeff.html.