CRYPTOLOGIA
2023, VOL. 47, NO. 2, 97–100
https://doi.org/10.1080/01611194.2023.2170158

Taylor & Francis
Taylor & Francis Group

The new golden age of decipherment

Craig P. Bauer, *Editor-in-Chief*

In the second issue of *Cryptologia*, way back in 1977, a contributor noted, "The golden age of decipherment may have been the first half of the nineteenth century, when the ancient tongues of the Near East were loosened." This, of course, refers to writings that were not intended for secrecy, such as Egyptian hieroglyphs, but became unreadable when the last humans familiar with these scripts died. Some such scripts remain unreadable today, but progress is being made. A notable recent example is "The Decipherment of Linear Elamite Writing" by François Desset, Kambiz Tabibzadeh, Matthieu Kervran, Gian Pietro Basello, and Gianni Marchesi.[1]

But there's a new and different golden age of decipherment that we are presently in the midst of, namely the recovery of messages intended to be kept secret and therefore hidden behind the best ciphers of the time. Custom computer programs often play a key role in such decipherments. The first issue of *Cryptologia* contained an article on an old, but only recently broken, cipher: "Poe Challenge Cipher Finally Broken."[2] A computer wasn't used in this particular recovery, but the second issue of *Cryptologia* featured the piece "Automated Analysis of Cryptograms."[3]

As the editor-in-chief of *Cryptologia*, the submission categories that bring me the greatest pleasure deal with cryptanalysis. While I enjoy seeing attacks on any system, my absolute favorite is when the attack is not merely theoretical, but actually reveals messages of some historic interest. That is, modern cracking of historical ciphers, typically made possible by clever computer programs. Examples, span the centuries. There are solutions to a cipher created by Trithemius and hidden in plain sight in his book *Steganographia* for hundreds of years,[4] ciphers from other famous

CONTACT Craig P. Bauer ✉ cbauer@ycp.edu

[1] Desset, François, Tabibzadeh, Kambiz, Kervran, Matthieu, Basello, Gian Pietro and Marchesi, and Gianni. "The Decipherment of Linear Elamite Writing," *Zeitschrift für Assyriologie und vorderasiatische Archäologie*, Vol. 112, No. 1, 2022, pp. 11–60.

[2] Winkel, Brian J., "Poe Challenge Cipher Finally Broken," *Cryptologia*, Vol. 1, No. 1, pp. 93–96, 1977. For the solution see "Poe Challenge Cipher Solutions," *Cryptologia*, Vol. 1, No. 4, 1977, pp. 318–325.

[3] Schatz, Bruce R., "Automated Analysis of Cryptograms," *Cryptologia*, Vol. 1, No. 2, 1977, pp. 116–142.

[4] Reeds, Jim, "Solved: The Ciphers in Book III of Trithemius's Steganographia," *Cryptologia*, Vol. 22, No. 4 1998, pp. 291–317 and Ernst, Thomas, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia," *Cryptologia*, Vol. 22, No. 4, 1998, pp. 318–341.

historical figures such as Marie-Antoinette,[5] Maximilian II,[6] and Giouan Battista Bellaso,[7] Papal ciphers,[8] the Rohonc Codex,[9] a Masonic cipher,[10] and ciphers created by Klansmen[11] and 20th century serial killers.[12] There was even a cipher created in an attempt to provide evidence of an afterlife that was revealed by a computer program rather than a spirit.[13] Many ciphers from past wars were fairly recently cracked. These include ciphers from the American Revolutionary War,[14] both sides of the American Civil War,[15] even ciphers connected with Robert E. Lee[16] and Jefferson Davis,[17] the War of 1812,[18] German diplomatic ciphers from 1900 to 1915,[19] World War I,[20] World War II,[21] and the Biafran War.[22]

I've even had the pleasure of seeing solutions to some previously unsolved ciphers that I detailed in a book[23] come forth. They were an Irish Republican Army (IRA) cipher,[24] another afterlife cipher,[25] and the Zodiac

[5] Patarin, Jacques and Valérie Nachef, "I Shall Love You Until Death" (Marie-Antoinette to Axel von Fersen)," *Cryptologia*, Vol. 34, No. 2, 2010, pp. 104–114.

[6] Kopal, Nils and Michelle Waldispühl "Deciphering three diplomatic letters sent by Maximilian II in 1575," *Cryptologia*, Vol. 46, No. 2, 2022 pp. 103–127.

[7] Biermann, Norbert, "Analysis of Giouan Battista Bellaso's cipher challenges of 1555," *Cryptologia*, Vol. 42, No. 5, 2018, pp. 381–407.

[8] Lasry, George, Beáta Megyesi & Nils Kopal, "Deciphering papal ciphers from the 16th to the 18th Century," *Cryptologia*, Vol. 45, No. 6, 2021, pp. 479–540.

[9] Király, Levente Zoltán and Gábor Tokai, "Cracking the code of the Rohonc Codex," Cryptologia, Vol. 42, No. 4, 2018, pp. 285–315.

[10] Bennett, Donald H., "An Unsolved Puzzle Solved," *Cryptologia*, Vol. 7, No. 3, 1983, pp. 218–234.

[11] Deavours, C. A., "A Ku Klux Klan Cipher," *Cryptologia,* Vol. 13, No. 3, 1989, pp. 210–214.

[12] Anderson, Jeanne, "Breaking the BTK Killer's Cipher," *Cryptologia*, Vol. 37, No. 3, 2013, pp. 204–209 and Anderson, Jeanne, "Kaczynski's Ciphers," *Cryptologia*, Vol. 39, No. 3, 2015, pp. 203–209.

[13] Gillogly, James J. and Larry Harnisch, "Cryptograms from the Crypt," *Cryptologia*, Vol. 20, No. 4 1996, pp. 325–329.

[14] Fagone, Peter P., "A Message in Cipher Written by General Cornwallis During the Revolutionary War," *Cryptologia*, Vol. 1, No. 4, 1977, pp. 392–395. The solution was left for readers to uncover, but sufficient hints were given.

[15] Boklan, Kent D., "How I Broke the Confederate Code (137 Years Too Late)," *Cryptologia*, Vol. 30, No. 4, 2006, pp. 340–345 and Assarpour, Ali and Kent D. Boklan "How We Broke the Union Code (148 Years Too Late)," *Cryptologia*, Vol. 34, No. 3, 2010, pp. 200–210.

[16] Boklan, Kent D., "How I deciphered a Robert E. Lee letter—and a note on the power of context in short polyalphabetic ciphers," *Cryptologia*, Vol. 40, No. 5, 2016, pp. 406–410.

[17] Boklan, Kent D., "How I Decrypted a Confederate Diary—And the Question of the Race of Mrs. Jefferson Davis," *Cryptologia*, Vol. 38, No. 4, 2014, pp. 333–347.

[18] Boklan, Kent D., "How I Broke an Encrypted Diary from the War of 1812," *Cryptologia*, Vol. 32, No. 4, 2008, pp. 299–310.

[19] Lasry, George, Ingo Niebel, and Torbjörn Andersson, "Deciphering German diplomatic and naval attaché messages from 1900-1915," *Cryptologia*, Vol. 45, No. 5 2021, pp. 383–425.

[20] Lasry, George, Ingo Niebel, Nils Kopal, and Arno Wacker, "Deciphering ADFGVX messages from the Eastern Front of World War I," *Cryptologia*, Vol. 41, No. 2, 2017, pp. 101–136.

[21] Sullivan, Geoff and Frode Weierud, "Breaking German Army Ciphers," *Cryptologia*, Vol. 29, No. 3, 2005, pp. 193–232 and Ostwald, Olaf and Frode Weierud, "Modern breaking of Enigma ciphertexts," *Cryptologia*, Vol. 41, No. 5 2017, pp. 395–421.

[22] Bean, Richard W., George Lasry & Frode Weierud, "Eavesdropping on the Biafra-Lisbon link – breaking historical ciphers from the Biafran war," *Cryptologia*, Vol. 46, No. 1, 2022, pp. 1–66.

[23] Bauer, Craig P., *Unsolved! The History and Mystery of these World's Greatest Ciphers from Ancient Egypt to Online Secret Societies*, Princeton University Press, Princeton, New Jersey, 2017.

[24] Bean, Richard, "The Use of Project Gutenberg and Hexagram Statistics to Help Solve Famous Unsolved Ciphers," *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*, Linköping University Electronic Press, Linköping, Sweden.

[25] Ibid.

340 cipher.[26] While these latter examples saw print elsewhere (and, in one case, went public on YouTube), *Cryptologia* is typically where such results first appear.

The special issue you are now holding (or reading online) consists of an especially intriguing example of modern cracking of historical ciphers, as it reveals 50 previously unread ciphers from Mary Stuart, aka, Mary, Queen of Scots. Mary is a famous tragic historical figure, who was recently brought back to attention with a feature movie,[27] books,[28] and expositions.[29] Bringing to light such a large quantity of her letters is likely to generate a lot of interest! Mary Stuart is also well-known for having her fate sealed when her letters on the Babington plot were intercepted and deciphered by Francis Walsingham and his agents. Her life story, with an emphasis placed on the Babington plot, is exciting enough to warrant pole position (the first chapter) in Simon Singh's highly entertaining introductory history of cryptology, *The Code Book*[30] and coverage in David Kahn's *The Codebreakers*.[31] The decipherments presented in this issue cover 1578–1584, a few years before this fatal plot, and except for the letters after July 1583, they were never intercepted (and therefore, not kept in British archives). Also, plaintext copies were not preserved in French archives. Thus, those letters were considered to be lost by John Bossy, the leading scholar who researched Walsingham's penetration of the French embassy.[32] In addition to the great historic interest of Mary Stuart, the plaintexts revealed are voluminous, weighing in at nearly 50,000 words. John Guy, the leading expert on Mary Queen of Scots, considers this discovery to be "a literary and historical sensation" and "the most important new find on Mary Queen of Scots for 100 years".[33]

Deciphering historical documents has immense value, not just for the history of cryptography, but for historical research as well. The work presented in this issue is a great example. And there is a larger picture to consider. The study of historical ciphers and their decipherment have, in recent years, become organized professionally at an international level. There are the HistoCrypt conferences,[34] the Cryptologic History Symposia sponsored by NSA's Center for Cryptologic History (CCH), and the

[26] Oranchak, David, "Let's Crack Zodiac – Episode 5 – The 340 Is Solved!" https://www.youtube.com/watch?v=-1oQLPRE21o, published Dec 11, 2020. Also see http://zodiackillerciphers.com/wiki/index.php?title=Compilation_of_news_reports_about_the_solution for news articles on the solution.

[27] See https://www.imdb.com/title/tt2328900/.

[28] Guy, John, *Mary Queen of Scots: The True Life of Mary Stuart*, Mariner Books, Boston, Massachusetts, paperback, 2018.

[29] See https://www.bl.uk/events/elizabeth-and-mary.

[30] Singh, Simon, *The Code Book*, Doubleday, New York, 1999.

[31] Kahn, David, *The Codebreakers: The Story of Secret Writing*, MacMillan, New York, 1967, pp. 121–124.

[32] Bossy, John, *Under the Molehill: An Elizabethan Spy Story*, Yale University Press, New Haven, Connecticut, 2001.

[33] Private correspondence with the authors.

[34] See https://histocrypt.org/.

National Cryptologic Foundation (NCF),[35] the DECRYPT project,[36] Satoshi Tomokiyo's Cryptiana website, the richest source of information on ciphers from the 16th through the18th centuries,[37] and Klaus Schmeh's popular blog, which is frequently updated and always interesting and entertaining.[38] All of the above are supported by a friendly, passionate, and inspiring community of historical crypto experts and fans. I am honored to have met many of them in-person and am grateful that they have made *Cryptologia* their home.

One more thing I love about the article you are about to read is that it represents a team effort. Cryptology has a rich history of teamwork. Diffie-Hellman key exchange is an example, and Whit Diffie has remarked "Two people can work on a problem better than one." In some cases, it takes three. RSA, as regular readers of this journal know, is named after the famous trio Ron Rivest, Adi Shamir, and Leonard Adleman. And three was the magic number for the present article. The authors have emphasized to me that this article was truly a team effort. All three made critical contributions and breakthroughs. Their multidisciplinary skills worked to their advantage. Their fields are computer science (George Lasry), music (Norbert Biermann), and astrophysics (Satoshi Tomokiyo), and they are all passionate about historical ciphers and lucky to read French, the language of the newly deciphered letters. I hope that their joining forces on this monumental and fascinating project inspires others to combine their skills and efforts. We are at our best when we work together!

[35] See https://www.nsa.gov/History/Cryptologic-History/Cryptologic-History-Symposium/.

[36] See https://de-crypt.org/ and Megyesi, Beáta, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker & Michelle Waldispühl, "Decryption of historical manuscripts: the DECRYPT project," *Cryptologia*, Vol. 44, No. 6, 2020, pp. 545–559.

[37] See http://cryptiana.web.fc2.com/code/crypto.htm.

[38] See https://scienceblogs.de/klausis-krypto-kolumne/. A new URL has likely replaced this one prior to this introduction seeing print.