LEIBNIZ’S MACHINA DECIPHRATORIA

(A SEVENTEENTH-CENTURY PROTO-ENIGMA)

1. LEIBNIZ’S DESCRIPTIONS OF HIS CRYPTOGRAPHIC MACHINE

 G. W. Leibniz (1646-1716) was the quintessential Renaissance man, a German Leonardo da Vinci. But with a difference. For instead of focusing on the plastic arts like Leonardo, Leibniz worked more abstractly—with mathematics. He invented the calculus, topology, determinants, binary arithmetic, symbolic logic, rational mechanics, and much else besides. But like Leonardo, Leibniz also constructed machines: wheels that ran on treads, windmills that worked by scoops, and an arithmetical machine that was—and still is—one of the wonders of the world of geared engineering. A great deal is known about Leibniz’s historical achievements, but there are still some surprises left.

 Early in 1679 Leibniz sent to his master, the reigning duke of Hanover-Calenberg, one of his occasional long memoranda regarding his achievements and projects. After discussing his now-famous calculating machine here, he continued as follows:

This arithmetical machine led me to think of another beautiful machine that would serve to encipher and decipher letters, and do this with great swiftness and in a manner indecipherable by others. For I have observed that the most commonly used cyphers are easy to decipher, while those difficult to decipher are generally so difficult to use that busy people abandon them. But with this machine an entire letter is almost as easy to encipher and decipher for one who uses it as it is to copy it over.[[1]](#footnote-1)

This representation to Duke John Frederick of February 1679 is echoed in the draft of another memorandum of that October of that year, where Leibniz notes that “I am going to have intensive work done on the machine arithmetica” and after hopefully remarking that “I have no doubt that your serene highness will provide [financial] assistance for this” and then ajoins the marginal comment: “and the same applies to the cypher machine.”[[2]](#footnote-2)

 As far as Hanover is concerned, however, this is the last we hear of it. And throughout his vast correspondence, Leibniz never discussed this device. But in late October of 1688 he was granted an audience in Vienna with the emperor Leopold I, realizing an aspiration he had entertained for decades.[[3]](#footnote-3) Leibniz went to great lengths to prepare for this audience. He wrote several versions—one running to about 30 printed pages—of the material he proposed to present to the emperor. These covered in great detail the entire range of what his own accomplishments were and projected a considerable series of projects for work contributing to imperial interests. Everything that we know about the nature of the *machina deciphratoria* is derived from these memoranda, since, for the rest, Leibniz enshielded his device in deep quiescence.

 In his notes preparatory for an audience with the emperor Leopold I in Vienna in August/September 1688 Leibniz wrote:

Then too there is my *machina deciphratoria* with which a ruler can concurrently correspond with different ministries, and without much effort both writes in a cypher that he wishes to use and comprehend a letter sent to him in cypher. This is done much as with suing a musical instrument or clavichord, so that the text appears by touching the piano-keys and only needs to be copied.[[4]](#footnote-4)

And in a short outline for his long memorandum Leibniz spoke of “My cryptographic machine, which places many ciphers at a ruler’s disposal and resembles a clavichord.”[[5]](#footnote-5)

 In amplifying these notes into a more elaborate memorandum, Leibniz wrote after discussing his calculating machine:

On a similar principle, though far simpler [than my calculator], I have discovered a *machina deciphratoria* for use by great personages. It is a smallish device (*machinula*) that is easy to transport. With it a great ruler (ein grosser herr) can concurrently use many virtually unsolvable ciphers and correspond with many ministries. While both encipherment and decipherment is [ordinarily] laborious, there is now a facility enabling one to get at the requisite ciphers or alphabetic-letters as easily as though one were playing on a clavichord or other [keyboard] instrument. The requisite letters will immediately stand out, and only need to be copied off.[[6]](#footnote-6)

While Leopold I requested Leibniz to pursue some of his proposals, the *machina deciphratoria* was not among them. In view of the effective work of his own black chamber in Vienna, Leopold was apparently not minded to spend money on its construction.

 Even the sparse indications of Leibniz’s memoranda provide a wealth of information about his *machina deciphratoria*:

1. It operates via a piano-like keyboard.

2. It functions equally well for enciphering and deciphering.

3. It readily admits of variable use of different enciperments.

4. It operates on the same principle (but far more simply) as Leibniz’s calculating machine.

5. It requires the user to copy off the result of its workings.

6. It is compact and portable.

This may not look like much to go on. But nevertheless given what is known about Leibniz’s calculating machine and about his ideas regarding cryptography, a conjectural reconstruction of his cryptographic machine is possible.

2. A RECONSTRUCTION OF LEIBNIZ’S MACHINA DECIPHRATORIA

 Late in the 15th century Johannes Trithemius (1462-1526), abbot of the monastery of Sponheim, introduced the idea of polyalphabetic encipherment with where each successive letter was encrypted by a different monalphbetic transposition.[[7]](#footnote-7) While such an encryption is quite difficult to break, it is also laborious to use, be it in encryption or decryption. But while still in his early thirties Leibniz conceived of an ingenious way of addressing this problem.

 As Leibniz described his cryptographic machine, its salient features appear to be as follows. It is operated via a piano-like keyboard that actuates (1) a display drum, and (2) an array of piano-like strikers that hold pointers instead of piano-hammers. The strikers are geared to the keyboard keys in a one-to-one correspondence.

 Viewed from the side the machine would look something like this:

 striker

 pointer

 keyboard

 rotating drum

 The keys of the keyboard bear the letters of the alphabet being encrypted. As the drum turns, different duly scrambled letter-display slides that are attached to it come into view.

 Seen from above the machine would look something like this:

 strikers

 changeable letter-display slide D E U S A B C D etc.

 permanent letter keyboard A B C D E F G H etc.

 The drum is a rotating cylinder that holds a series of removable (and thereby replaceable) wooden slats or slides, each of them bearing a monoalphabetic relettering of the alphabet. With such alphabetic slats inserted the drum would appear from the side as:

 The machine then functions as follows when the alphabetic slides are inserted into the outer drum:

(1) With each depression of the keyboard key the corresponding striker is activated and descends to have its pointer indicate the encypherment letter that results.

(2) After a certain number of keystrokes the rotating drum brings the next monoalphabetic encypherment slide into the striking position.

On this basis, the same monoalphabetic encription is never used for more than a few consecutive letters.

 The device operates as follows. The rotating drum is linked to the keyboard in such a way as to make a fraction of a 360° turn after the keys are struck a certain number of times.[[8]](#footnote-8) The effect if to put the next successive letter-slide at the top position after a certain number of keyboard strokes.

 The striking of a letter-input key produces two immediate results. The one is to lower the pointer so as to indicate the corresponding encrypted letter. This is a particularized result depending on just exactly which key has been struck. The second result is indifferently uniform across the input keys, namely to effect one step of (partial) rotation in the input rotor, Rotor No. 1. But there is also a second, different rotor (Rotor No. 2, the output rotor) which rotates the display drum. These two are linked by a stepped rotation device (the Leibnizian *Staffelwalze*) in such a way that only after a certain number of keystrokes—say N of them—will the output rotor (No. 2) be activated so as to bring the next letter slat to the top position. The gearing arrangement requisite here can be achieved by a *Staffelwalze* (“stepped roller”) of exactly the sort at work in Leibniz’s calculating machine of “carrying” in arithmetic—a gearing arrangement whereby gear A turns gear B in such a way that while a certain number of rotation-steps by A leaves B unaffected, A’s next rotation-step effects a pre-specified turning of B.[[9]](#footnote-9)

 In employing the machine, all that the user need do is to copy out the successive letters that are pointer-indicated as the plaintext is keyed in. And decipherment is achieved easily by exactly the same process, but with each alphabetic encypherment slides replaced by a corresponding decipherment slat.

 The machine is fitted out with a control that adjusts the number (N) of key-strokes that needs to be made before the next alphabetic slide comes into the top position. Accordingly, different settings for N will realize very different modes of encryption—even without changing the alphabetic slides.[[10]](#footnote-10) But of course greater cryptographic security can obviously be achieved by an occasional interchange among the encypherment slats—or by replacing them altogether.

 At the heart of his device lay the Leibnizian *Staffelwalze*—a stepped-drum mechanism that still called the “Leibniz-wheel,” that was the crux of his calculator—with its decimal carrying feature readjusted to produce a shift to the next alphabetic slide (until an eventual return to the first). Used in mechanical calculating machines for over 200 years, the Staffelwalze is custom-made for cryptographic employment in a stepped Trimethian encypherment where letters are successively encoded in a different monalphabetic cypher.

 It is clear that this reconstruction encapsulates all of Leibniz’s descriptive specifications for this machine. And such a device could readily be contained in a box sufficiently small to escape notice among the impedimenta of a travelling prince.

 The use of wooden letter slides from polyalphabetic encipherment goes back to the *Arce steganographica* of Kircher’s *Polygraphia nova et universalis ex Combinatica arte delecta* (Rome: Varesius, 1663).[[11]](#footnote-11) What Leibniz’s machine accomplished was to mechanize this process. It marks the transition from a cryptographic *device* (such as the cypher wheel) to a *machine*.

 Like the ENGIMA, Leibniz’s cryptographic machine takes alphabetic letter input, does its hocus-pocus work, and then provides an alphabetic letter output. Of course there are differences. In the one case the hocus-pocus is electrical, in the other mechanical. The one uses rotors, the other slats. The one has a typewriter the other a piano-style keyboard. The one delivers a printed output, the other requires writing. But all these simply reflect differences in the technological state of the art. In basic conception—in spirit—the two are machines kinsmen. But given the extent of the analogies at issue, no more than allowable exaggeration would be involved in characterizing Leibniz’s cryptographic machine as a proto-ENGIMA.

3. THE FATE OF LEIBNIZ’S CRYPTOLOGICAL BRAINSTORM

 In his memorandum for the audience with emperor Leopold II Leiibniz observes that:

The mechanisms I have thought out (except the arithmetical machine and those for improving clocks have for the most part been kept secret and mentioned to virtually no-one[[12]](#footnote-12)

It seems clear that Leibniz was not going to have this mechanism constructed unless and until some great prince showed an interest. He seems to have thought that the fewer who knew of it the better. Leibniz’s discussion of his cipher machine made it clear and explicitly that Leibniz intended it only for “a potentate or high person”. Accordingly, this apparatus was Leibniz’s most closely guarded secret. Although he was often prepared to boast of his innovations and inventions yet this one was only mentioned in private memoranda for viva vose presentations to princes. And as a result of this secrecy, virtually all that we know about the *machina deciphratoria* came from Leibniz’s pitch of it to the Emperor. It is, thus, questionable if the machine was ever actually constructed.[[13]](#footnote-13)

 In presenting Leibniz’s memoranda for Leopold I, the editors of the great Leibniz edition comment:

It yet remains unknown if Leibniz actually intended to construct such a [cryptographic] machine or eve brought it to reality.[[14]](#footnote-14)

In view of the secrecy in which he veiled this effort it is, however, unlikely that he did so.[[15]](#footnote-15)

 The conception of a cryptographic machine is one which, like many other ingenious ideas, makes its first appearance in the fertile mind of Leibniz. But very possibly, Leibniz was not quite alone in this regard. In early August of 1716 King George I made his first return visit to Hanover, and then went on to Bad Pyrmont to take the cure, Leibniz travelled there from Hanover to meet with him on 4 August. On that very day Johann Ludwig Zollmann came to Hanover to visit Leibniz, followed the next day by his son, Philip Heinrich.[[16]](#footnote-16) The younger Zollmann had been trained in Hanover’s black chamber, and upon following George Louis to Britain after his succession there, had entered the service of England’s Secret Office and had become one of London’s prime cryptographers.[[17]](#footnote-17) The Zollmann’s lodged in the same Schmiedestrasse house where Leibniz had been living since 1698, the prime object of their visit being to secure information about the latest, improved version of Leibniz’s calculating machine.[[18]](#footnote-18) A fortuitous mismatch of schedules destroyed the opportunity for informative interaction between Leibniz and the Zollmans regarding the potential of his great brainchild. It would thus seem that at least one contemporary was not blind to the potential use of Leibniz’s arithmetical machine for cryptographical purposes. A recent writer holds that “cryptology has consummated its union with mathematics through the computer.”[[19]](#footnote-19) It appears that Leibniz was already a matchmaker here, although his death only a few weeks later terminated any prospect of a productive union.

 It is clear in this connection that an intriguing historical opportunity was missed at this point. As things stand, Leibniz’s cryptographic machine was his most closely guarded secret —to be revealed only to princes. But it is possible that at this late hour of his life he might have described it to Zollmann who would certainly have taken it back to London’s black chamber. And what might have happened then stirs the imagination.

REFERENCES

Leibniz’s writings are cited after the monumental Leibniz edition of the *Deutsche Akademie der Wissenschaften* in the manner of: Series + volume + page(s).

Other cited Leibniz editions include:

GPhil: C. I Gerhardt (ed.), *Die philosophischen Schriften von G. W. Leibniz*, 7 vol’s (Berlin: Weidmann, 1875-90).

GMath: C. I Gerhardt (ed.), *Leibnizens Mathematische Schriften*, 7 vol’s (Berlin and Halls, 180-63).

Couturat, *Opuscules*: Louis Couturat (ed.), *Opuscules er fragments inédits de Leibniz* (Paris: F. Alcan, 1903).

The secondary references cited here include:

Bauer: Friedrich L Bauer, *Decrypted Secrets: Methods and Maims of Cryptology* (Berlin: Springer, 1997). 3rd ed. 2002.

Beeley: Philip Beeley, “Un des mes amis: On Leibniz’s Relation to the English Mathematician and Theologian John Wallis,” in P. Themister and S. Brown (eds.), *Leibniz and the English Speaking World* (Dordrecht: Springer, 2007.

Breger: Herbert, “Leibniz und die Kyptographie,” in H. Breger, J. Herbst, & S. Erdner (eds.), *Einhett in der Vielheit: Akten des VIII Internationalen Leibniz Congress* (Hanover, 2006), pp. 101-05.

Couturat, *Logique*: Louis Couturat, *Le Logique de Leibniz* (Paris: F. Alcan, 1901).

Couturat, *Opuscules*, Louis Couturat, *Fragments et opuscules inédits de Leibniz* (Paris: Alcan, 1903).

Davillé: Louis Davillé, *Leibniz Historien* (Paris: F. Alcan, 1907).

de Leeuw (1999): Karl de Leeuw. “The Black Chamber in the Dutch Republic during the War of the Spanish Succession and its Aftermath, 1707-1715,” *The Historical Journal*, vol. 42 (1999), pp. 133-156.

de Leeuw (2007). Karl de Leeuw, “Cryptology in the Dutch Republic,” in de Leeuw and Bergstra, pp. 327-67.

de Leeuw and Bergstra: Karl de Leeuw and Jan Bergstra (eds.), *The History of Information Secrecy* (Amsterdam: Elsevier, 2007).

Ellis: Kenneth Ellis, *The Post Office in the Eighteenth Century* (London: Oxford University Press, 1958).

Hoffman: J. E. Hoffman. “Leibniz und Wallis,” *Studia Leibnitiana,* vol. 5 (1973), pp. 245-81. [Focuses on issues related to the calculus and contains no mention of cryptanalysis.]

Kahn: David Kahn, *The Codebreakers* (New York: Macmillan, 1967).

Leary: Thomas (Penn) Leary, “Cryptology in the 16th and 17th Centuries,” *Cryptologia*, July 1966.

Müller & Krönert: Kurt Müller and Gisela Krönert, *Leben und Werk von G. W. Leibniz: Eine Chronik* (Frankfurt am Main: Vittorio Klosterman, 1969).

Persic: Peter Persic, “Secrets, Symbols, and Systems: Parallels between Cryptanalysis and Algebra, 1580-1700,” *Isis*, vol. 88 (1997), pp. 674-92.

Schnath: Georg Schnath, *Geschichte Hanovers im Zeitalter der neunten Kur und der englischen Zukzession: 1674-1714*, 4 vol’s (Hildesheim & Leipzig: August Laz, 1938-82).

Smith: D. E. Smith, “John Wallis as a Cryptographer,” *Bulletin of the American Mathematical Society*, vol. 24 (1917), pp. ???

Stein, Erwin, *Die Leibniz-Daueraustellung der Gottfried Wilhelm Leibniz Universität* (Hanover, 2006) [Exhibit catalogue available on the internet.]

Stephenson, Neal, The Baroque Cycle, 3 vols: *Quicksilver*, 2003, *The Confusion*, 2004, *The System of the World*, 2004 (New York: William Morrow).

Strasser (1988): Gerhard F. Strasser, *Lingua Universalis: Kryptologie und Theorie der Universalsprachen im 16. und 17. Jahrhundert* (Wiesbaden: Otto Harrasowitz, 1988).

Strasser (2007): Gerhard F. Strasser, “The Rise of Cryptology in the European Renaissance,” in in de Leeuw and Bergstra; pp. 277-325.

Türkel, Siegfried, *Chiffrieren mit Geräten und Maschinen* (Graz: Moser, 1927).

Vehse: Eduard Vehse, *Geschichte der Höfe des Hauses Braunschweig in Deutschland und England*, 5 vol’s (Hamburg: Hoffmann und Campe, 1853).

1. A I 2, p. 125. [↑](#footnote-ref-1)
2. A I 2, p. 223: October 1679. [↑](#footnote-ref-2)
3. Muller-Kronert, p. 92. [↑](#footnote-ref-3)
4. A IV 4, p. 27. [↑](#footnote-ref-4)
5. A IV 4, p. 45: August/September 1688. [↑](#footnote-ref-5)
6. A IV 4, p. 68. [↑](#footnote-ref-6)
7. Trithemius projected a *magia naturalis* developed in such works as his *Steganographia* (1500 but first published in 1606) and *Polygraphia* (1507 but first published in 1518). For him see W. Schneegans, *Abt Johannes Trithemius und Kloster Sponheim* (Kreuznach: R. Schmithals, 1882) and Wayne Schumaker, “ Johannes Trithemius and Cryptography,” *Renaissance curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language* (Binghamton, NY: Center for Medieval and Early Renaissance Studies, 1982). The mystification which Trithemius cast over his discussion led to its being placed on Rome’s index of prohibited books. [↑](#footnote-ref-7)
8. In principle, the turning rate could be lesser or greater. [↑](#footnote-ref-8)
9. For an animated illustration of this mechanism see the article “stepped reckoner” in *Wikipedia* (English version), as well as the article “Staffelwalze”. [↑](#footnote-ref-9)
10. The decipherment of intercepted messages is thus made very difficult because the decipherer has no way of knowing which part of the text is governed by which cypher. [↑](#footnote-ref-10)
11. See De Leeuw 2007, p. 361 and Strasser 2007, 315. On Kircher see Kahn, pp. 904-5 as well as the *Catholic Encyclopedia*. [↑](#footnote-ref-11)
12. A IV 4, p. 27. [↑](#footnote-ref-12)
13. In his memorandum for Duke John Friedrich of October 1679 (A I 2, p. 223) Leibniz says that he will “an der *Machina Arithmetica* eifrig arbeiten lassen” and then makes the marginal addendum: item die Machina zum dechiffrieren.” However, we have no indications that he did so. [↑](#footnote-ref-13)
14. A IV 4, p. 27, notes. [↑](#footnote-ref-14)
15. A I 2, p. 223 [↑](#footnote-ref-15)
16. Müller & Köenert, p. 260. [↑](#footnote-ref-16)
17. P. H. Zollman’s history is interesting. His father, a privy counselor in Zeitz and a Leibniz correspondent, recommended him to Leibniz. Highly capable he rose rapidly in Hanoverian officialdom, and transferred to London in 1714 where Baron Bothmer appointed him guardian of one of his sons. He worked in the Secret Office and in 1723 he was appointed foreign secretary to the Royal Society owing to “his skill in many languages”. In 1727 he became a fellow of the Royal Society. Initially the name was spelled Zollmann, but in England he dropped the second n. He died in 1748. (See Bodemann, *Briefwechsel*, p. 399, and especially Ellis.) In the late 1710s Zollmann corresponded frequently with Leibniz. [↑](#footnote-ref-17)
18. For a good account of Leibniz’s calculating machine and its potential see Stein 2006. All in all Leibniz spent roughly 20,000 gulden of his own money in the fabrication of his machine—well over a million dollars in present-day purchasing power. [↑](#footnote-ref-18)
19. Persic, p. 678. [↑](#footnote-ref-19)