Early Mechanical Cryptography and Binary Keying or The Possible Impact of the Damm Brothers on Leibniz's Machina Deciphratoria

Carola Dahlke
Deutsches Museum
c.dahlke@deutsches-museum.de

Magnus Ekhall
Independent Researcher
magnus.ekhall@gmail.com

Abstract

Mechanical cipher machines employing binary keying elements became widespread in the first half of the twentieth century. This paper examines the origins of binary keying in mechanical cryptography, motivated by Gottfried Wilhelm Leibniz's early work on binary arithmetic, his calculating machine (Machina Arithmetica), and his documented interest in cryptology.

By analysing Leibniz's surviving descriptions of a proposed cipher machine (Machina Deciphratoria), a reconstruction of this machine from 2012, and early cipher machines developed by Arvid Damm, we found no evidence that binary keying was intended in Leibniz's cryptographic ideas. Instead, binary keying appeared as a distinctly twentieth-century development.

The article highlights the possibility that reconstructions — when based on sparse sources — may unintentionally incorporate later design concepts into the reconstructed device, so that a historical device could be retroactively influenced by a modern idea.

1 Introduction

Mechanical cipher machines are often thought of as emerging in the early twentieth century, particularly those using a configurable and binary cipher key as well as some kind of stepping mechanism. In this context, a binary cipher key refers to a keying element composed of multiple components, each of which can assume one of two discrete states (e.g. active/inactive, tooth or no tooth, punched hole or no hole etc), thereby influencing the transformation applied during encryption. Examples of earlier mechanical devices used for cryptography certainly exist, but of simpler construction: cipher disks, slides, grilles or alphabet strips of various kinds.

In this paper, we distinguish between cryptographic devices and cryptographic machines. By "device" we mean an apparatus that assists the user in performing cryptographic operations without automating state changes between successive characters. By "machine" we refer to a mechanism that performs at least part of the cryptographic transformation automatically, typically through stepping, state progression, or key-controlled mechanical motion. In recent research there have been several cases where earlier devices have been interpreted as precursors of the modern mechanical cipher machine.

Our prime aim was to track down the point in time in the history of cryptography, where mechanical encryption started to become binary, i.e. when the cipher key is formed by a mechanism where parts or switches need to be set on or off. This paper reflects the detours and insights we made in this small study and the current state of our research.

2 Research Motivation and Initial Hypothesis

The initial hypothesis of this paper was to investigate the earliest use of a binary component used as a key in a cipher machine. It is well known that machines designed by Arvid Damm for the company AB Cryptograph in the early 1900s had this feature (Damm, 1917).

Basically, binary number systems were introduced to the European world by Gottfried Wilhelm Leibniz. It therefore made sense to start the search directly with Leibniz. Interestingly, his written estate contains references to a cipher machine, which was replicated a few years ago. Indeed, this recent reconstruction of Gottfried Wilhelm Leibniz' cipher device "Machina Deciphra-

toria", supposedly then more than 200 years prior to Damm's work, appeared to share several characteristics with the early machines of AB Cryptograph. A thorough comparison of the two devices was made. However, as the investigation progressed, it became clear that the evidential foundations for this comparison were uneven: the reconstructed "Machina Deciphratoria" was found to rely on a very limited set of primary, and only written sources. The path to Leibniz also led to other historical figures and machines (listed in the following section), which, although not helpful for the current question, nevertheless provided some interesting insights.

In this paper, the term *reconstruction* is used to describe the modern conceptual model of Leibniz's Machina Deciphratoria presented by Rescher et al. (2014). Given the very limited and vague nature of the surviving primary sources, this model should be understood as an interpretative construction rather than a historically correct mechanical design. Accordingly, references to a "reconstructed machine" in the following sections denote this conceptual model and do not imply that such a machine existed or was mechanically specified by Leibniz.

A research question was to investigate whether Damm might have been inspired by Leibniz. This was quickly found to be unlikely.[1] A closer look at an early Damm machine which has a binary type key can be found in section 6. Nevertheless, the two machines, i.e. the replica "Machina Deciphratoria" and the model A-1 machine from AB Cryptograph remained very similar, prompting the authors to investigate whether the replica of Leibniz's machine might even have been influenced by the work of the Damm brothers.

3 Sources and Methodology

This paper revisits the primary sources of Leibniz in order to collect the few texts that survive from Leibniz' own descriptions of his cipher machine idea. We also look at another early cipher device which has been attributed to being the world's first cipher machine: the "Chiffre-Machine" designed by Fredrik Gripenstierna. Primary sources in the form of letters sent to Arvid Damm by his older brother Ivar were investigated, as well as a manuscript on the subject of cryptology written by the two brothers together (National Security Agency, 2011), (National Security Agency, 2016). This material provided an insight on what the Damm brothers thought of contemporary cipher machines and that they strived to have a theoretical foundation for their work.

We briefly touch on other machines or inventors, such as the textile engineer Zschweigert, and the work of Vernam.

4 Leibniz's "Machina Deciphratoria": the Primary Sources

Starting in 1923 and still ongoing, Leibniz's very comprehensive and carefully sorted estate was and is still made fully accessible to the public by the Akademie-Ausgabe of the editing project Gottfried Wilhelm Leibniz. The publications have been edited using a historical-critical approach. This makes it convenient to trace his quotations on cryptography, and on a planned cipher machine.

The first time he mentions a Machina Deciphratoria is in a letter to Duke Johann Friedrich in February 1679. Previously, Leibniz describes his plan to construct a Machina Arithmetica. This is followed by this French[2] quote (see Figure 2 in appendix A) (Leibniz, 1679a):

> "This arithmetic machine makes me think of another beautiful machine that would be used to convert letters into encrypted letters and to decipher them: and this with great speed and in a way that is indecipherable to others. For I notice that most of the ciphers commonly used are easy to decipher; and those that are difficult to decipher are usually difficult to write, which causes busy people to abandon them. But with this machine, an entire letter could be converted into ciphers and deciphered almost as easily by the person who has the machine as it could be copied."

In the same year, Leibniz wrote a list of 16 issues in a memorial for Duke Johann Friedrich. Among them, he mentioned his plans to get work done on his Machina Arithmetica, and in this lines (see Figures 3 and 4 in appendix A) he added a

[1] Leibniz's ideas for a cipher machine can be found in his estate in letters and notes for a presentation. It is highly unlikely that Arvid Damm or his brother Ivar had access to the estate before it was gradually made public in 1923. However, it is certain that the Damm brothers knew the operating principles of the stepped drum.

[2] All translation were done by the authors

footnote about a machine for deciphering (Leibniz, 1679b):

> "Meanwhile, I wish to work diligently on the Machina Arithmetica (1), for which purpose I await a skilled craftsman, and I also wish to execute other matters. I have no doubt that Your Serene Highness will graciously assist me in this endeavour, as you have kindly offered to do."

And the footnote

> "(1) as well the machine for deciphering."

It is not until 1688 that the Machina Deciphratoria reappeared in his records. Leibniz was planning his important audience with Emperor Leopold I and listed all the scientific points he wanted to raise and to probably promote financial support. Needless to say, he prepared his presentation very thoroughly – there are a total of five versions for his audience in the documents, three of which mention the Machina Deciphratoria.

The first mention can be found in a version that is dated to August or September 1688 (Leibniz, 1688a) (see Figure 5 in appendix A):

> "What I have invented for Arcana in Mathesi Theoretica as well as Circa Leges Naturae et Causas Rerum is known to many, but the machines and useful practices that I have devised (except for the Arithmetic Machine and the improvements of clockworks) have mostly been kept secret and mentioned to almost no one, that I have them, waiting for an opportunity to present them in reality, so that they would not be published at an inopportune moment and exploited.
> Likewise, with my Machina Deciphratoria, a powerful man can correspond with many ministers in different ciphers, and without any effort, one can either write a cipher or understand what is sent to him in cipher, as if playing a musical instrument or clavichord, so that it is immediately available at the touch of a key and can simply be copied."

Attached to these lines written by Leibniz, the editors of Volume A IV,4 noted below (see Figure 6 in appendix A):

> "On the idea of the cipher machine, see also the remarks to Duke Johann Friedrich: our edition I,2 p.125 Z12-18; p. 223, line 30. It is not yet known whether Leibniz, who showed a sustained interest in the art of cryptography (cf. e.g. VI 4, note 239; I 13, p. 551, lines 12-16), continued to pursue his intention to construct such a machine or even put it into practice." [3]

The second mention can be taken from a small entry in August/September 1688 (Leibniz, 1688b) (see Figure 7 in appendix A):

> "Machines and useful practices: as my Machina Deciphratoria, the powerful man (potentate) has everything under control at once, as on the clavichord"

The third mention of the Machina Deciphratoria can be found in the second half of September 1688 (Leibniz, 1688c), and this is the most extensive description that Leibniz delivers of his idea, as far as the authors know (see Figure 8 in appendix A):

> "One of the most subtle inventions ever seen by humans is my Machina Arithmetica, which is admired in both the Royal Societies of London and Paris, even though only the effect has been seen in the poor model; but once I have the opportunity to employ craftsmen, I want to have several of them made to perfection for the chambers and observatories of great lords. A child can multiply and divide the most difficult examples on it, and everything happens in an instant, as it were, without any effort of the mind. And large numbers will be completed just as quickly as small ones. It is excellent for calculating entire tables, but it serves especially as a specimen of human mental power, in that a

[3] Following the suggestion of the editors, the authors as well checked the other mentioned entries on Leibniz' interest in cryptology. Just as mentioned by the editors, Leibniz is speaking about the art of cryptography. However, there is no other mention of a Machina Deciphratoria.

> machine can calculate what was otherwise considered proprium hominis.
>
> Based on the same principle, albeit much simpler, I have invented[4] a Machina Deciphratoria for persons of high rank. It is a small machine that is easy to carry. With it, a great lord can have many almost indissoluble ciphers at once and correspond with many ministers. However, since both the positioning in ciphers and the deciphering are laborious, the facility consists in the fact that one only has to grasp the given ciphers or letters as if one were playing on a clavicord or instrument, and the desired ones come out immediately and stand there; they only would have to be copied."

Leibniz does not seem to have elaborated on his ideas. No sketches or further descriptions have been found about how Leibniz imagined his machine would work. Although Leibniz reflects on the subject of cryptography and cryptanalysis in some of his correspondences and notes, his Machina Deciphratoria is not mentioned again, as far as the present volumes of the Academy edition reveal.

5 The Rescher Reconstruction of the Machina Deciphratoria

In 2012, Nicholas Rescher published a conceptual reconstruction of Leibniz's Machina Deciphratoria. The following description summarises the reconstructed machine as presented by Rescher, and does not imply that this design reflects a historically attested machine.[5]

The reconstructed machine is based around a horizontal hexagonal prism. On each of the six faces of the prism a slat with a scrambled alphabet is inserted. At any time, only the one side of the prism that is facing the operator is "active". The machine has a keyboard (as from a clavichord), one key per letter of the alphabet. When a key is pressed the corresponding letter on the scrambled alphabet slat is indicated. Additionally, the machine can change the active face of the prism by rotating it one step forward. Whether this is done or not is controlled by a Leibniz wheel with six pins.

A Leibniz wheel ("Staffelwalze, stepped drum") is a mechanical component invented by Leibniz and famously used in his Machina Arithmetica. It consists of a cylinder with a set of teeth (as on a cogwheel), but the teeth have varying length. Depending on how the Leibniz wheel is set up, different numbers of teeth can engage with other components.

In the case of the Rescher reconstruction, the wheel can be configured to rotate the prism in six different ways. This gives the machine a kind of irregular stepping between the alphabets (Rescher, 2012).

Rescher writes (2012) that "Leibniz's apparatus was in some regards akin to Arvid G. Damm's machine A-21 with its sliding revolving drum with 26 alphabetic faces". A better comparison is probably with Damm's A-1 from 1917.

It is worth pointing out again that there is no evidence that Leibniz's cipher machine was actually built during his lifetime. A comparison between Leibniz's surviving descriptions and the reconstructed machine shows that substantial extrapolation was required in order to derive a functioning mechanical design from the limited primary source material.

6 Fredrik Gripenstierna's "Chiffre-machine"

While the Leibniz reconstruction remains a modern conceptual model, the 18th-century work of Fredrik Gripenstierna (1728–1804) provides a concrete example of an early mechanical cryptographic device that was actually manufactured and demonstrated.

Gripenstierna was a Swedish military officer and nobleman who is credited with creating one of the first cipher machines (Beckman, 1999). His invention, which he calls a "Chiffre-Machine", consists of 57 wheels mounted on a single shaft. Each wheel is divided into two halves around its rim. One half bears the letters of the alphabet along with a few punctuation symbols, while the other half displays the numbers 00 to 99 arranged in a

[4] The original text uses the German word "ausgefunden" which is uncommon in modern German. It could mean either "discovered" or "invented" in this context. Please also compare the examples given in the Grimm DWB "Deutsches Wörterbuch by Jakob and Wilhelm Grimm", https://www.dwds.de/wb/dwb2/ausfinden

[5] More information on the exhibition in 2013, and pictures of the reconstructed machine, can be found e.g. on the website of the University of Pittsburgh: `https://pitt.libguides.com/c.php?g=12552&p=66419`

random order that is unique to each wheel.

The machine is operated by two people seated opposite each other. One person sees only the lettered halves of the wheels, while the other sees only the numbered halves. To encipher a message, the first person sets up a line of up to 57 letters, adjusting the wheels one by one. The second person then records the corresponding numbers visible on their side of the machine, producing the enciphered message (Beckman, 1999). This physical separation resembles the later 'red/black separation' principle in secure systems, in the limited sense that plaintext and ciphertext are handled in distinct operator domains.

The machine was accompanied by instructions describing how it should be used in such a way that the first wheel employed for enciphering the first letter was not always the same. The machine does not appear to have had a cipher key in the conventional sense, apart from these somewhat convoluted instructions determining where encryption should begin.

It is known that Gripenstierna's device was manufactured and demonstrated for the Swedish king Gustav III in 1786. Only one device is known to have been manufactured, no further mention of this device is known. The fate of the manufactured prototype is also unknown.

Gripenstierna himself wrote that he based his invention on principles he had received from his grandfather, Christopher Polhem (1661–1751) (Beckman, 1999). There are no known records on what part of the device that originates from Polhem and what Gripenstierna himself has contributed.

While it is evident that this device was actually constructed it is also worth pointing out that this apparatus is closer to a mechanical aid than an automated machine: there is no automatic stepping, no real cipher key (binary or otherwise). It is a manually operated polyalphabetic cipher device where the main feature being the separation of the cleartext and ciphertext domains.

7 Binary Keying in Early Damm Machines

The transition from such manual, mechanical aids to machines with true binary keying began in the early twentieth century with the collaborative work of Ivar and Arvid Damm.

Ivar Damm (1862–1917) was a Swedish mathematician and teacher. He studied at Uppsala university where he in 1896 presented his doctoral thesis "Bidrag till läran om kongruenser med primtalsmodyl" (Contributions to the Theory of Congruences with a Prime Modulus) (Thyselius, 1918). In 1899 he started work as a mathematics and physics teacher in Gävle, Sweden. His younger brother Arvid Gerhard Damm (1869–1927) trained and worked as an engineer working in the textile industry. Amongst other things he worked with Jacquard machines[6] at Vävskolan in Borås (Widman and Wik, 2017).

Both Arvid and Ivar had an interest in cryptology with Ivar perhaps having a more theoretical point of view (National Security Agency, 2011). In 1912 Arvid met George Lorimer Craig, a Scottish textile engineer, in Berlin and they developed several mechanical cipher machines together. There was not a lot of interest for these machines, but Arvid managed to gather enough interest for a patent consortium to be constructed in 1915 which later evolved into a company, AB Cryptograph, in 1916 (Widman and Wik, 2017).

During this time the Damm brothers exchanged correspondence in which they discussed various cipher methods and the theory behind them (National Security Agency, 2011). In 1917 they completed a manuscript titled "Kryptografiens grunddrag i systematisk framställning" (The fundamentals of cryptography in a systematic presentation). In this work, they define the terminology and theoretical foundations of cryptology, while also examining the practical use of ciphers in the form of machines and apparatus. Notably, none of Arvid Damm's machines are mentioned but at the same time almost all machines that are mentioned have their limitations and flaws highlighted (National Security Agency, 2016). The Damm brothers carefully studied the patents and other descriptions of contemporary cipher machines and devices. The highlighted limitations and flaws are not only of a cryptographic nature. In some cases it is instead related to a machine being difficult to use, or prone to having mechanical issues. Both the mathematical and engineering mindset has been used here (National Security Agency, 2016).

It is plausible that the experience with Jacquard machines and similar mechanical-digital equipment had an impact on the designs used for the

[6]The weaving patterns of Jacquard looms are fed with punch cards, an early form of programme control.

cipher machines designed by Arvid Damm. Ivar Damm's doctoral thesis deals with congruences with a prime modulus, an area of mathematics closely related to cryptology (Damm, 1896).

The early Damm machine models (starting with Cryptotyper in 1914) had a horizontal prism or cylinder that would step one step forward or backwards for each letter that was enciphered. The direction is determined by a chain which consists of a number of links. There are two types of links: high and low. The link type determines whether the stepping is forwards or backwards (Widman and Wik, 2017). The chain was configurable by the user and was a clear binary part of the cipher key.

Compared to Rescher's reconstruction of the Machina Deciphratoria, there are notable structural similarities. Like the reconstructed Leibniz machine, Damm's A-1 employs a prism carrying multiple cipher alphabets, with alphabet strips mounted on each face. The A-1 prism has 29 sides rather than six, but in both cases a single active alphabet is selected mechanically. Both designs incorporate a mechanism intended to produce irregular stepping of the prism: in the reconstructed Leibniz machine this role is assigned to a Leibniz wheel, while in Damm's A-1 the stepping behaviour is controlled by a configurable chain composed of high and low links. Although the historical evidence for such a mechanism in Leibniz's original conception is limited, the reconstructed machine closely resembles that of Damm's early machines. A photo of the A-1 with a covering hood removed can be seen in Figure 1.

Arvid Damm is not the only example of a cipher machine inventor coming from the textile industry of the early twentieth century. Rudolf Zschweigert, a German textile engineer, applied for a patent in 1919 for a mechanical cipher machine based on a permutation cipher (Schmeh, 2020).

Yet another example of early use of a binary cipher key is with the "Cipher Printing Telegraph System" described by Gilbert Vernam as being invented during the Great War. The system described used two punched paper tapes, one for the message and one for the key, which were binary added. A "machine perforator" was used to produce a third punched paper tape with the resulting enciphered message (Vernam, 1926). Used correctly, this system can implement what is now known as a one-time-pad: the only theoretically provable secure cipher. Vernam's system therefore represents one of the earliest clearly documented implementations of a binary keying mechanism in cryptographic machinery.

Figure 1: A photograph of the A-1 with the protective cover removed, exposing the prism with 29 alphabet strips (Häll, 2016).

8 Discussion: Leibniz and Binary Cryptography

Leibniz's well-known work on binary arithmetic makes it understandable that later interpretations have sought to associate his cryptographic ideas with binary mechanisms. However, while binary representation was of clear mathematical importance to Leibniz, there is no explicit evidence in the surviving sources that binary principles were intended to play a role in the Machina Deciphratoria.

On page 37, and in the footnote 229 on page 88, Rescher (2012) explains that Leibniz's memoranda give "a wealth of information" about his Machina Deciphratoria. "Given this detail, and considering what is known about Leibniz' calculating machine — and also about his ideas regarding cryptography — a conjectural reconstruction of his cryptographic machine is readily possible. [footnote 229]" Following this footnote 229 leads to Rescher's explanation on page 88:

> "However, this possibility only came to light in 2001 with the publication of A IV 4. In its wake, I have been able to devise a conceptual reconstruction of the apparatus with the assistance of my en-

Machine / Device	Year	Type	Main Properties	Binary Keying?
Machina Deciphratoria (Leibniz)	1679, 1688	Conceptual	Described as keyboard-operated (like a clavichord) to automate letter conversion.	No
Chiffre-Machine (Gripenstierna)	1786	Device	57 wheels on a single shaft. Featured physical domain separation ("red/black") between plaintext and ciphertext.	No
Model A-1 (A. Damm)	1917	Machine	29-sided prism with automatic, irregular stepping controlled by a configurable chain.	Yes
Vernam's System	1917	Machine	Utilized binary addition (XOR principle) of message and key via punched paper tapes.	Yes
Zschweigert's Machine	1919	Machine	Mechanical permutation cipher designed by a German textile engineer.	Yes
Rescher's Reconstruction	2012	Machine	Conceptual model using a 6-sided prism and a Leibniz wheel with pins to control stepping.	Yes (Interpretive)

Table 1: Summary of historical cryptographic devices and machines and the presence of binary keying.

> gineer friend Richard K. Arrangements are under way for a physical model of the machine to be fashioned by Messers Klaus B. and Wolfgang R. of Hannover who have expertise with the construction and operation of Leibniz's calculating machine."

When reading these quotations without researching the original passages in the Leibniz edition, it was easy to believe that much more than just the passages quoted above formed the basis for the Machina Deciphratoria.

As well, in Rescher's translation of the limited primary sources, subtle wording choices occasionally strengthen the impression that Leibniz's cipher machine was a concrete, realised artefact. For example, the French passage beginning "Mais par cette machine…" is rendered as "But with this machine of mine…" (Rescher, 2012). The possessive construction is not explicit in the original text and may suggest a degree of realisation or ownership that is not directly supported by the surviving sources. While minor in isolation, such translation choices contribute to an overall interpretation in which the Machina Deciphratoria appears better specified than the primary evidence suggests.

The connection to the Damm brothers is made in a footnote that Rescher links to on page 41 (Rescher, 2012). There he writes: "Various comparisons are suggestive. [Footnote 237]". Following this footnote to page 89, Rescher thanks two anonymous reviewers of his article in Cryptologia (Rescher, 2014): Both the Gripenstierna Chiffre-machine and the early Damm machines are referred to as "later analogues of Leibniz's apparatus". Even though Rescher himself was probably unfamiliar with the historical Swedish exhibits, the question remains whether the designers who worked with Rescher on the replica were subsequently influenced by their knowledge of existing machines. The fact is that neither Gripenstierna nor the Damm brothers could have copied the Leibniz machine, because it never existed - not even as a description, sketch or construction drawing.

In a review of Rescher's publication "Leibniz and Cryptography", Philip Beeley points out the weak link between the primary sources and the reconstructed machine. The fact that Rescher compares the reconstructed machine to the twentieth century Enigma machine is likened to "throwing all caution to the wind" (Beeley, 2014). As well, a critical essay from Fabian Dombrowski (2022) can be found on the matter. Dombrowski also addresses the scarcity of sources and raises the speculative question of whether the Machina Deciphratoria was perhaps never actually intended to be built, but was instead designed to secure funding from the rulers.

Rescher designed a machine based on the few surviving lines in which Leibniz refers to such a device. The construction was carried out with the assistance of experts experienced in the Machina Arithmetica, as well as collaborators who could have access to present-day knowledge of historical cipher machines. In this light, Rescher's later

description of the machine as an early Enigma is notable, as it invokes a comparison originating in much later cryptographic practice.

It seems to happen more often in the history of cryptology that big names can lead to a kind of glorification. For example, a similar uncertainty applies to Fredrik Gripenstierna's Chiffre-Machine. Although Gripenstierna explicitly attributes the underlying idea to his famous grandfather, Christopher Polhem, the surviving sources do not allow a clear distinction between what was originally Polhem's idea and what was developed or implemented by Gripenstierna himself. While the device was demonstrably constructed, the origin of its design principles therefore remains somewhat uncertain.

Concluding, Rescher's machine could be seen as an interesting mind game: Was it possible after all that Leibniz had been able to have such a machine constructed in theory? Leibniz invented the stepped drum, and by his extensive research and correspondence, he drew on a wealth of knowledge and tirelessly refined great ideas, as can be seen in his extensive estate. According to Dombrowski (2022) who refers to Leibniz (1682–1688), it is fairly certain that Leibniz was well acquainted with contemporary works on cryptography such as the Cryptomenytices from Selenus (Selenus, 1624). However, it seems to be historical fiction that Leibniz was the first to place permuted alphabets on a cylindrical form. We attribute this step to Gripenstierna (or possibly Polhem), and thereafter to Thomas Jefferson, as long as there is no earlier historical evidence.

Table 1 contains an overview of the majority of devices discussed in this paper.

9 Conclusion

This study finds no evidence that binary keying was part of Leibniz's ideas about cryptography. Instead, binary keying appears to be a development of the early twentieth century. The reconstructed Machina Deciphratoria, together with its exhibition and catalogue, shows how reconstructions based on limited sources can unintentionally create convincing but misleading interpretations.

This highlights the importance of returning to original sources and clearly separating historical evidence from later reconstructions, as failure to do so may contribute to the formation of myths in the history of cryptology.

Acknowledgments

The authors would like to thank the library of the Deutsches Museum, in particular Florian Preiss, for his help in obtaining historical sources. As well, we would like to thank three anonymous reviewers for their valuable comments and suggestions which we gratefully included to enhance our submission.

References

Bengt Beckman. 1999. *Världens första kryptomaskin*. FRA.

Philip Beeley. 2014. Leibniz and Cryptography: An account on the occasion of the initial exhibition of the reconstruction of Leibniz's cipher by Nicholas Rescher. *Leibniz Review*, 24:111–122.

Ivar Damm. 1896. *Bidrag till läran om kongruenser med primtalsmodyl*. Phd thesis, Uppsala Universitet.

Arvid Gerhard Damm. 1917. Apparatus for Producing Series of Signs. U.S. Patent US1233035A. Filed July 21, 1915; granted July 10, 1917.

Fabian Dombrowski. 2022. Kein Geheimnis. Leibniz und die Kryptologie des 17. Jahrhunderts. *Die junge Mommsen*, 4.

Peter Häll. 2016. Digitalt museum, eks0029825. Creative Commons Attribution 4.0 International (CC BY 4.0).

Gottfried Wilhelm Leibniz. 1679a. Nr. 110: Leibniz an Herzog Johann Friedrich, Februar (?) 1679, Eigenh. Konzept A (Hannover). In Leibniz-Archiv / Leibniz-Forschungsstelle Hannover, editor, *A I 2. Allgemeiner, politischer und historischer Briefwechsel*, page 125. Akademie Verlag 1927, Berlin. Akademie-Ausgabe.

Gottfried Wilhelm Leibniz. 1679b. Nr. 184: Leibniz für Herzog Johann Friedrich, Memorial. Oktober 1679, Eigenh. Konzept B (Hannover). In Leibniz-Archiv / Leibniz-Forschungsstelle Hannover, editor, *A I 2. Allgemeiner, politischer und historischer Briefwechsel*, page 223. Akademie Verlag 1927, Berlin. Akademie-Ausgabe.

Gottfried Wilhelm Leibniz. 1688a. Nr. 6: Aufzeichnung für die Audienz bei Kaiser Leopold i. August/September 1688. In Leibniz-Edition Potsdam der Berlin-Brandenburgischen Akademie der Wissenschaften, editor, *A IV 4. Politische Schriften*, page 27. Akademie Verlag 2001, Berlin. Akademie-Ausgabe.

Gottfried Wilhelm Leibniz. 1688b. Nr. 7: Kurzfassung einiger Ausführungen vor Kaiser Leopold i.

August/September 1688. In Leibniz-Edition Potsdam der Berlin-Brandenburgischen Akademie der Wissenschaften, editor, *A IV 4. Politische Schriften*, page 45. Akademie Verlag 2001, Berlin. Akademie-Ausgabe.

Gottfried Wilhelm Leibniz. 1688c. Nr. 8: Ausführliche Aufzeichnung für den Vortrag bei Kaiser Leopold i. Second half of September 1688. In Leibniz-Edition Potsdam der Berlin-Brandenburgischen Akademie der Wissenschaften, editor, *A IV 4. Politische Schriften*, page 68. Akademie Verlag 2001, Berlin. Akademie-Ausgabe.

National Security Agency. 2011. Papers on cryptography: Nemochiffer, linjalchiffer. Z104.D12. NSA Historical Archive, ID 2011.0101.0515.

National Security Agency. 2016. Kryptografins grundrag (handwritten manuscript). Z104.D13M 1917. NSA Historical Archive, ID 2016.0101.2213.

Nicholas Rescher. 2012. *Leibniz and Cryptography: An Account on the Occasion of the Initial Exhibition of the Reconstruction of Leibniz's Cipher Machine*. Office of Scholarly Communication and Publishing, University of Pittsburgh Library System, University of Pittsburgh.

Nicholas Rescher. 2014. Leibniz's Machina Deciphratoria. A Seventeenth-Century Proto-Enigma. *Cryptologia*, 28(2):103–115.

Klaus Schmeh. 2020. The Zschweigert cryptograph – a remarkable early encryption machine. In *Proceedings of the 3rd International Conference on Historical Cryptology HistoCrypt 2020*, pages 126–134. Linköping University Electronic Press.

Gustavus Selenus. 1624. *Cryptomenytices et cryptographiae libri IX*. Lunaeburgi: Exscriptum typis & impensis Johannis & Henrici fratrum, der Sternen, bibliopolarum Lunaeburgensium. Pseudonym of August von Braunschweig-Lüneburg.

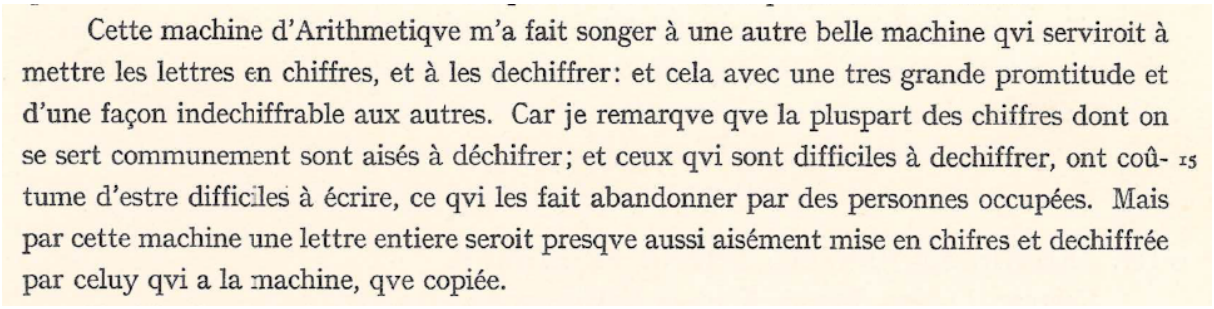
Erik Thyselius. 1918. *Vem är det?* P. A. Norstedt & söners förlag.

G. S. Vernam. 1926. Cipher printing telegraph systems. In *American Institute of Electrical Engineers proceedings*. Declassified copy hosted by the U.S. National Security Agency (NSA), Friedman Documents, Patent and Equipment Records, Folder 545, Document ID A4148856.

Kjell-Owe Widman and Anders Wik. 2017. *Damm och AB Cryptograph*. FRA.

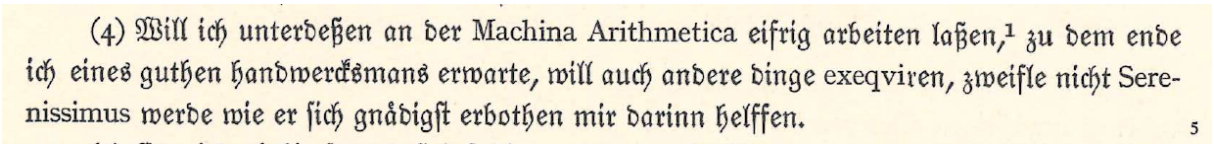
A Primary Sources by Leibniz on the Machina Deciphratoria

This appendix reproduces excerpts of the primary source material by Leibniz as discussed in the paper.



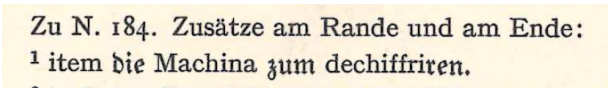
Cette machine d'Arithmetiqve m'a fait songer à une autre belle machine qvi serviroit à mettre les lettres en chiffres, et à les dechiffrer: et cela avec une tres grande promtitude et d'une façon indechiffrable aux autres. Car je remarqve qve la pluspart des chiffres dont on se sert communement sont aisés à déchifrer; et ceux qvi sont difficiles à dechiffrer, ont coûtume d'estre difficiles à écrire, ce qvi les fait abandonner par des personnes occupées. Mais par cette machine une lettre entiere seroit presqve aussi aisément mise en chifres et dechiffrée par celuy qvi a la machine, qve copiée.

Figure 2: Excerpt from A I,2 1697, p.125; please note that the expression "m'a fait songer à" marks his cipher machine as a product that exists only in his mind and not in reality - at least at this point in time. The same holds true for the use of the conditional to describe the machine ("par cette machine une lettre entière seroit ...")



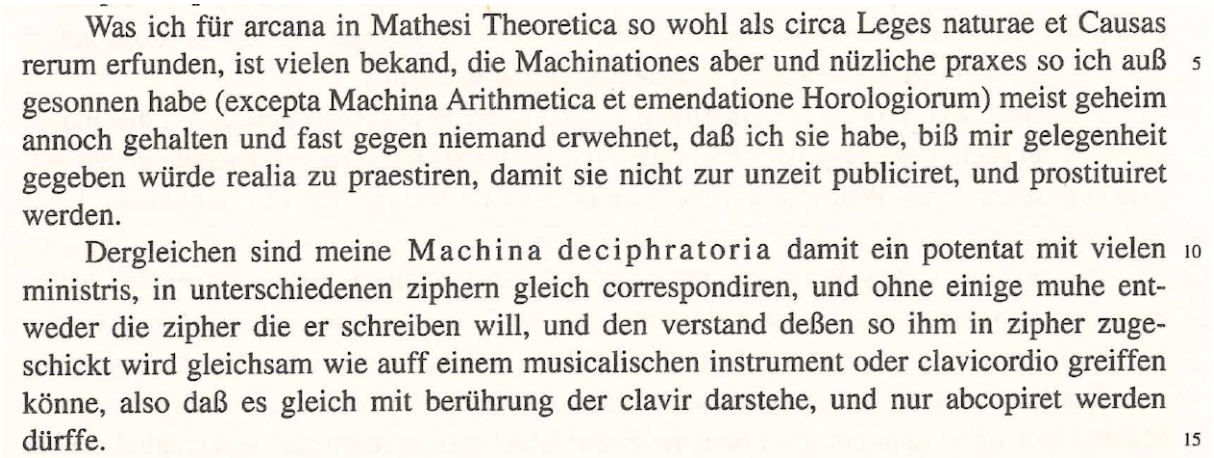
(4) Will ich unterdeßen an der Machina Arithmetica eifrig arbeiten laßen,[1] zu dem ende ich eines guthen handwercksmans erwarte, will auch andere dinge exeqviren, zweifle nicht Serenissimus werde wie er ſich gnädigſt erbothen mir darinn helffen.

Figure 3: Excerpt from A I,2 1679, p.223



Zu N. 184. Zusätze am Rande und am Ende:
[1] item die Machina zum dechiffriren.

Figure 4: Excerpt from A I,2 1679, p.223



Was ich für arcana in Mathesi Theoretica so wohl als circa Leges naturae et Causas rerum erfunden, ist vielen bekand, die Machinationes aber und nüzliche praxes so ich auß gesonnen habe (excepta Machina Arithmetica et emendatione Horologiorum) meist geheim annoch gehalten und fast gegen niemand erwehnet, daß ich sie habe, biß mir gelegenheit gegeben würde realia zu praestiren, damit sie nicht zur unzeit publiciret, und prostituiret werden.

Dergleichen sind meine Machina deciphratoria damit ein potentat mit vielen ministris, in unterschiedenen ziphern gleich correspondiren, und ohne einige muhe entweder die zipher die er schreiben will, und den verstand deßen so ihm in zipher zugeschickt wird gleichsam wie auff einem musicalischen instrument oder clavicordio greiffen könne, also daß es gleich mit berührung der clavir darstehe, und nur abcopiret werden dürffe.

Figure 5: Excerpt from A IV,4 1688, p.27

10 deciphratoria: Über die Idee der Dechiffriermaschine vgl. auch die Bemerkungen gegenüber Herzog Johann Friedrich: unsere Ausgabe I,2 S. 125, Z. 12–18; S. 223, Z. 30. Ob Leibniz, der an der Dechiffrierkunst anhaltendes Interesse zeigte (vgl. z. B. VI,4 N. 239; I,13 S. 551, Z. 12–16), die Absicht, eine solche Maschine zu konstruieren, weiter verfolgt oder sogar in die Tat umgesetzt hat, ist noch nicht bekannt. 23 lasten: vgl.

Figure 6: Excerpt from A IV,4 1688, p.27

Machinae und Nuzliche praxes: als Machina mea deciphratoria[,] potentat hat darinn viel ziphern zugleich alles im griff, wie aufm Clavicordio

Figure 7: Excerpt from A IV,4 1688, p.45

Eine der Subtilsten Inventionen so von Menschen gesehen worden, ist meine Machina Arithmetica so man in den beyden koniglichen Societäten zu London und Paris admiriret, da man doch nur die würckung in dem Schlechten Modell gesehen; wenn ich aber einmahl gelegenheit habe Handwercks leute zu halten, will ich deren etliche in Vollkommenheit vor großer Herren kammern und observatoria machen laßen, ein kind kan darauff die schwehrsten Exempel multipliciren und dividiren, und geschicht alles gleichsam in einem augenblick ohne arbeit des gemüths. Und große Zahlen werden eben sobald fertig als kleine. Ist treflich ganze tafeln auszurechnen, dienet aber sonderlich als ein Specimen der Menschlichen gemüthskraffte dadurch zu wege zu bringen daß eine Machina rechnen kan, welches sonsten proprium hominis gehalten worden.

Aus gleichen principio wiewohl viel leichter, habe eine Machinam deciphratoriam vor hohe Personen ausgefunden. Ist eine kleine Machinula die leicht bey sich zu fuhren. Darauff kan ein großer herr viele fast unauflößliche Ciphern zugleich haben, und mit vielen Ministris correspondiren; weilen aber sowohl die stellung in Ziphern als das deciphriren mühsam, so bestehet die facilitat darinn, daß man die gegebene Ziphern oder buchstaben nur greiffen darff als wenn man auff einem clavicordio oder Instrument spielte, so kommen die begehrten augenblicklich herauß und stehen da; durffen denn nur abgeschrieben werden[.]

Figure 8: Excerpt from A IV,4 1688, p.68