The Use of Volvelles in Two Early Modern Cryptography Manuals

Corinne Bayerl
University of Oregon, USA
bayerl@uoregon.edu

Abstract

This paper examines the form and function of volvelles (rotating paper discs) used to represent cipher systems in Giambattista della Porta's *De furtivis literarum notis* (1563) and in the French translation of Trithemius' *Polygraphia* by Gabriel de Collange (1518, transl. 1561). I analyze the use of volvelles in cryptography handbooks within the larger context of their overall function in the Early Modern period, and I identify the factors that may account for an increasing use of volvelles in succeeding editions of della Porta's and Trithemius' works in the second half of the 16th century. Collange's expanded version of Trithemius' manual and della Porta's numerous amended editions of his own handbook indicate that changes in the material representation of cipher systems correlate with an increased level of public knowledge about encryption methods.

1 Introduction

In the 2015 Folger Library exhibition *Decoding the Renaissance: 500 Years of Codes and Ciphers*, the cipher wheel was called "the most iconic image in the history of cryptography" (Folgerpedia 2015). While the exhibit did not include any actual handheld encryption device, it prominently featured the first extant instructions for building a cipher wheel using two copper plates (Alberti, 1568), as well as 16th-century cryptography books with moveable cipher wheels. As part of books, such moveable wheels are called volvelles, constructed out of superimposed layers of paper in the Early Modern period. Prestigious, expensive books were sold with fully mounted rotating discs, whereas in cheaper editions the readers themselves had to cut out parts of the apparatus and attach it to a page in the book, which is why volvelles are viewed today as an early example of interactive book design. (Baird 2004, Karr Schmidt 2011, Ellison 2017, Crupi 2019)

When examining the use of volvelles in Early Modern cryptography manuals, it is helpful to take into consideration their overall prominence in science books of the period. Thus, volvelles abound in 16th-century treatises on astronomy and nautical navigation and are by no means specific to books on cryptography. Recent scholarship in the history of science has drawn our attention to the fact that printed illustrations heavily influenced approaches in newly formed scientific disciplines (Kusukawa 2012). Similarly, studies in the field of book history have argued that volvelles should be regarded as instruments of science, especially in cases when the books' authors had a firm grip on their creation, either by closely collaborating with the printer, or by fabricating the volvelles themselves, as did astronomer Peter Apian when he used his own press to print the visually stunning *Astronomicum Caesareum* (1540) that included no fewer than 38 octagonal papercut instruments (Crupi 2018). While Apian remains a rare case of an author actually maintainng full agency over the material form of his own printed book, the same desire to control the printed form of their work may be discerned among Early Modern cryptographers.

In the following, I will explore possible factors for the increased prominence of volvelles in two famous 16th-century cryptography treatises:

Giambattista della Porta's *De furtivis literarum notis*, and the French translation of Trithemius' *Polygraphia*, which contains volvelles that do not form part of the original text. By exploring possible factors for the increased use of volvelles in these two books, I seek to answer the broader question of how changes in the material form of cipher systems correlate with the changes in public knowledge of encryption methods.

2 Della Porta: Fighting Contraband editions with Improved Volvelles

Della Porta's handbook *De furtivis literarum notis* is a particularly compelling text with respect to the use of volvelles in cryptography manuals. A look at the successive editions of this bestseller reveals that in the second half of the 16th century volvelles had become a prominent feature of science books in general, and of cryptography manuals in particular. Within della Porta's lifetime the book was published in seven editions, starting with the initial version in 1562. In 1591, two contraband editions appeared in London in 1591—one of them with a false imprint of Naples to make it appear authentic, and both of them featuring new, visually stunning volvelles.

After the publication of the contraband editions, della Porta felt compelled to react. He reissued several revised editions of the book in 1593, 1602, 1603, and 1606, and notably improved the usefulness of the cipher wheels for his readers. He advertised his new editions by pointing out that he had included new examples and instructions, and he also retitled the text as *De occultis literarum notis,* probably in order to distinguish it from the contraband edition that circulated under the original title.

In striking contrast to the baroque, sexually charged decoration of the cipher wheels in the 1591 contraband editions, the volvelles in the 1593 edition that La Porta oversaw draw the reader's attention to the three circles of letters, numbers, and symbols. The visual language of these volvelles clearly marks cipher wheels as instruments to be used rather than being merely ornamental features to be enjoyed.

The changes that della Porta introduced after—and most likely in reaction to—the publication of the two contraband editions include obvious changes not only in the appearance but also in the status and usefulness of the book's cipher wheels:

Figure 1: Reader-assembled volvelle in contraband edition of *De furtivis literarum notis* (1591). Courtesy of Folger Library

Figure 2: Reader-assembled volvelle in revised edition of *De furtivis literarum notis* (1593). Courtesy of Folger Library

While the number of volvelles within the book remains unchanged at three, and the reader still needs to assemble these themselves, della Porta expands and enhances his instructions for assembling and using the cipher discs. This improvement is already emphasized in the printer's preface where della Porta is favorably compared to other cryptographers like Trithemius because of his capacity to provide his readers with clear explanations.

Under the title *Qua ratione ad scribendum instrumento uti possumus* [In this way we can use the writing tool], the reader finds a 40-line, step-by-step explanation of how writer and receiver of a secret message should proceed when using the first of three cipher wheels (della Porta, 1593). Precision is of utmost importance in the use of the volvelle as a functioning encryption tool, della Porta warns his readers: If the wheel is not rotated correctly, *qui scribit & qui nuncium accepturus est,* facile decipietur [both the person who writes and the person who is about to receive the message, will be easily deceived].

Compared to the first edition of *De furtivis literarum notis,* della Porta strengthens the interactive aspect of the manual, emphasizing the reader's agency in not only reading, but 'handling' the material. In contrast to the contraband editions of the manual, the revised editions present paper volvelles as highly efficient encryption tools for readers who, guided by a knowledgeable author, learn how to avoid errors when putting volvelles to use.

The changes in design of the cipher wheels that della Porta introduced between 1562 and 1593 do not correlate to a change in his proposed encryption methods. Instead, his expanded instructions to his readers detailing how to assemble and use cipher wheels reflect the fact that his cryptography manual had become a bestseller at European book fairs and that the author needed to protect it against forgeries by increasing its usefulness in the eyes of the reader.

3 Trithemius / Collange: Converting Substitution Tables into Cipher Wheels

In contrast to della Porta, Trithemius did not include cipher wheels in his *Polygraphia libri sex* (1518). Not the earliest, but the earliest *printed* Western work on cryptography, Trithemius' *Polygraphia* is known both for introducing a polygraphic system on the basis of cipher lists (books i through iv) and for establishing a polyalphabetic substitution method on the basis of a *tabula recta* (book v). Without doubt, Trithemius' focus on cipher lists and the *tabula recta* rather than cipher wheels was a conscious choice. We know from the earlier *Clavis steganographiae* (written c. 1499, published posthumously in 1606) that Trithemius was perfectly familiar with cipher wheels, so the encryption methods described in *Polygraphia* did not rely on their use. As Maximillian Gamer points out in his commentary to *Polygraphia,* the lack of cipher wheels does not in itself constitute a step back in the evolution of Trithemius' work on cryptography (Gamer 2022).

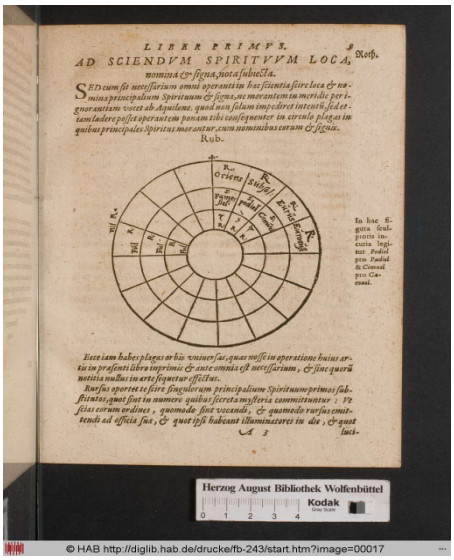

Figure 3: Printed, two-dimensional cipher wheel (not a volvelle) in Trithemius' *Steganographia* (1606). Courtesy of Herzog August Bibliothek, Wolfenbüttel

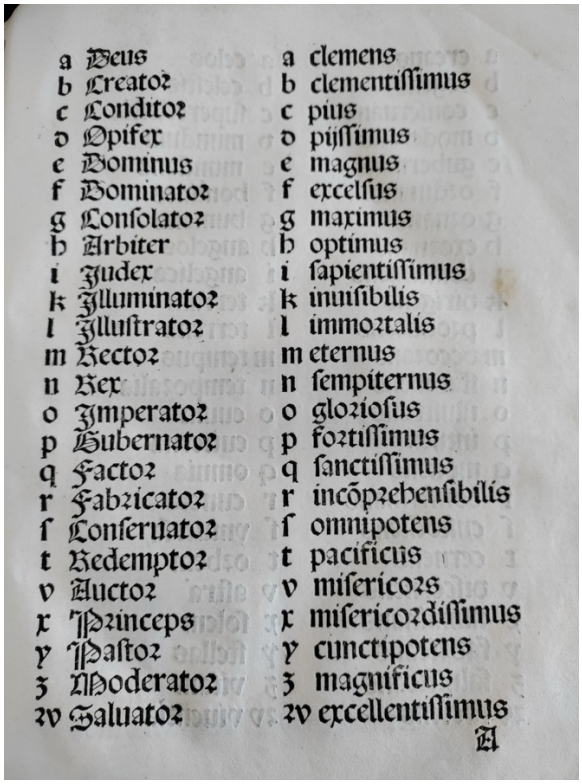

Figure 4: Latin cipher list in Trithemius' *Polygraphia* (1518), with each word in a column standing for one letter in the alphabet. Courtesy of Herzog August Bibliothek, Wolfenbüttel

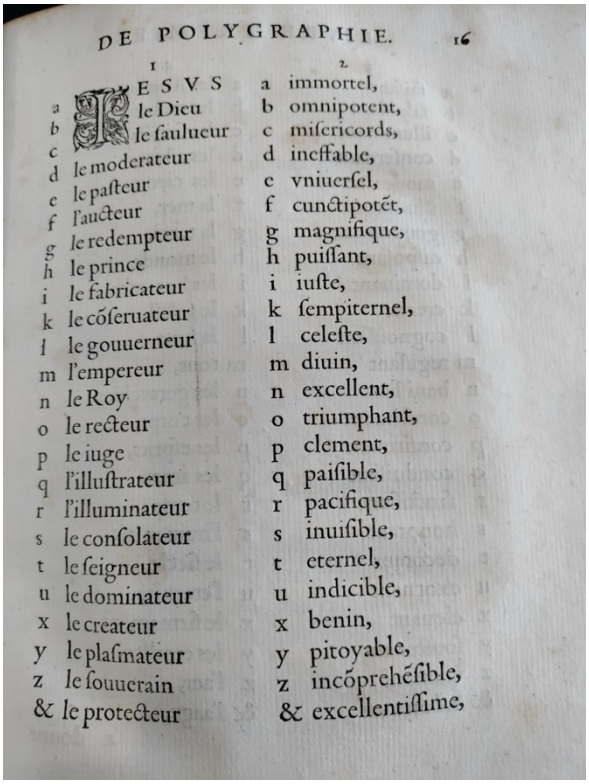

Figure 5: French cipher list by Collange in *Polygraphie, et Universelle escriture Cabalistique de M. J. Tritheme Abbé* (1561). Courtesy of Herzog August Bibliothek, Wolfenbüttel

One of the factors that helped further the fame of Trithemius' *Polygraphia* in 16th-century Europe was a widely circulated French version of the text by Gabriel de Collange, which proposed vernacular equivalents for the Latin cipher lists of books i through iv (see figure 5).

Yet it was not so much the translation of the cipher lists but rather an entirely new, 110-page long addendum to Trithemius' treatise that turned this French edition into one of the most coveted illustrated books of the Renaissance. In the last part of the work, entitled "Figures et tables planisphériques," de Collange suggests that Trithemius' tables may easily be converted into cipher wheels, an insight that reappears shortly later in della Porta's handbook.

De Collange's translation is a stunning example of an interactive Early Modern cryptography manual: The in-folio volume includes thirteen intricate, readily assembled volvelles, twelve of which are based on Trithemius' *tabulae rectae*.

Each volvelle is divided into 12 sectors forming a wheel with 12 spokes. The reader can rotate the disc under a vertical fixed strip that contains the two parts of the alphabet in their ordinary sequence (a to m, n to z; see figure 6). By turning the disc to a specific section against the fixed vertical paper strip, the reader is then able to find a letter that is part of the cipher text. De Collange explains that in order to create an equivalent of Trithemius' three *tabulae rectae* (containing 24 alphabets each), it was necessary to create twelve cipher wheels, with one wheel facilitating the representation of six alphabets.

Considering their choice of title—*Polygraphie, et Universelle escriture Cabalistique* (1561)—it would be worth exploring in detail what may have motivated the French translator Gabriel de Collange and the publisher Jacques Kerver to emphasize the occult aspects of Trithemius' work. While Kerver is known to have published important works in the history of secrecy and

occultism, de Collange's general interest in these matters is based on conjecture, not evidence. He is said to have translated Agrippa of Nettesheim' *De occulta philosophia* into French, but none of the several manuscript translations attributed to him shortly after his death in a biographical encyclopedia entry seem to have survived in French archives or libraries (Grudé 1584).

Whatever their motivation, it is clear that de Collange and Kerver introduce volvelles in their edition of Trithemius' *Polygraphia* in order to underline its proximity to occultism, as the volvelle's visual design clearly shows. Avid readers of Trithemius not only enjoyed the aesthetic qualities of the volvelles but understood their function as well, as we may glean from traces of their use, such as the handwritten corrections by Duke August the Younger (aka Gustavus Selenus) on one volvelle in his edition of de Collange's translation. (Strasser 1982)

4 Conclusion

This analysis of succeeding editions of della Porta's and Trithemius' works in the second half of the sixteenth century accounts for the increased prominence of volvelles in best-selling cryptography manuals. On the one hand, the growing demand for 'moveable', 'interactive' science books and the pressure on authors and printers to outdo contraband editions by improving the design of the legitimate edition(s) clearly contributed to the decision to prominently feature volvelles. On the other hand, the frequent inclusion of printed cipher wheels in cryptography manuals is also indicative of an evolving knowledge of encryption methods among a larger readership. Guided by detailed instructions on how to (not) use volvelles, Early Modern readers were enabled to gain experience in the practical use of the cipher wheel as important cryptographical tool.

Figure 6: Printer-assembled volvelle in *Polygraphie, et Universelle escriture Cabalistique de M. J. Tritheme Abbé* (1561). Courtesy of Bibliothèque Nationale de France

Figure 7: Detail view of printer-assembled volvelle in *Polygraphie, et Universelle escriture Cabalistique de M. J. Tritheme Abbé* (1561). Courtesy of Herzog August Bibliothek, Wolfenbüttel

References

Leon Battista Alberti. 1568. *Opusculi morali.* Bartoli, Venice.

Peter Apian. 1540. *Astronomicum Caesareum.* Apianus, Ingolstadt.

Davis Baird. 2004. Thing Knowledge. University of California Press, Berkeley.

Gianfranco Crupi, 2018. "Apianus e le volvelle del Cielo." *Paratesto* 15 (2018): 31-47.

Gianfranco Crupi. 2019. "Volvelles of knowledge. Origin and development of an instrument of scientific imagination (13th-17th centuries)", *JLIS.it*. 10 (2), 1–27.

Giambattista della Porta. 1563. *De furtivis literarum notis vulgo. De ziferis Libri IIII*. Scotus, Naples.

Giambattista della Porta. 1591. *De furtivis literarum notis vulgo. De ziferis Libri IIII*. John Wolfe, London.

Giambattista della Porta. 1593. *De occultis literarum notis* [new title for *De furtivis literarum notis*]. Lazarus Zetzner, Montbéliard

François Grudé, sieur de La Croix du Maine. 1584. *Bibliothèque Françoise*. 6 vls. Vol. 1. Abel l'Angelier, Paris, 111-112.

Katherine Ellison. 2017. *A Cultural History of Early Modern English Cryptography Manuals.* Routledge, Abingdon.

Folgerpedia. 2015. *Decoding The Renaissance: 500 Years of Codes and Ciphers exhibition item list.* https://folgerpedia.folger.edu/Decoding_the_Renaissance_exhibition_item_list#Disks_and_Volvelles

Maximilian Gamer. 2022. "Kommentar". *Die Polygraphia des Johannes Trithemius nach der handschriftlichen Fassung. Edition, Übersetzung und Kommentar*, vol. 1. Brill, Leiden, 133-207.

Suzanne Karr Schmidt and Kimberly Nichols. 2011. *Altered and Adorned: Using Renaissance Prints in Daily Life.* Yale University Press, Art Institute of Chicago.

Suchiko Kusukawa. 2012. *Picturing the Book of Nature: Image, Text and Argument in Sixteenth-Century Human Anatomy and Medical Botany.* University of Chicago Press, Chicago.

Gustavus Selenus. 1624. *Cryptomenytices et Cryptographiae Libri IX.* Stern, Lüneburg.

Gerhard F. Strasser. 1982. "Die kryptographische Sammlung Herzog Augusts: Vom Quellenmaterial für seine 'Cryptomenytices' zu einem Schwerpunkt in seiner Bibliothek." *Wolfenbütteler Beiträge* 5:83-121.

Johannes Trithemius. 1518. *Polygraphia libri sex.* Haselberg, Basel.

Johannes Trithemius and Gabriel de Collange (transl.) 1561. *Polygraphie et universelle escriture cabalistique*. Kerver, Paris.

Johannes Trithemius. 1608. Steganographia. Bernerus, Frankfurt.