SOLVED: THE CIPHERS IN BOOK III OF TRITHEMIUS'S STEGANOGRAPHIA

Jim Reeds

ADDRESS: Room C229, AT&T Labs — Research, 180 Park Avenue, Building 103, Florham Park NJ 07932 USA. reeds@research.att.com.

ABSTRACT: Book III of Trithemius's *Steganographia* (written ca. 1500) contains hidden cipher messages within what is ostensibly a work on magic. After almost 500 years these cryptograms have been detected and solved. (Since 1606 it was known that similar ciphers were present in Books I and II.) As a result the *Steganographia* can no longer be regarded as one of the main early modern demonological treatises but instead stands unambiguously revealed as the first book-length treatment of cryptography in Europe.

KEYWORDS: Trithemius. steganographia. history of cryptography.

> *Quis divinabit, quid in hoc libro tertio Steganographiae scripsit & scripturus erat Trithemius?*[1]

1. JOHANNES TRITHEMIUS AND THE STEGANOGRAPHIA CONTROVERSY

Johannes Trithemius (1462–1516), as author of the first printed work on cryptography, the *Polygraphia* published in 1518, is secure in his reputation as one of the founders of modern cryptography.[2] His earlier work, the three books of *Steganographia*, composed ca. 1499–1500 but not printed until 1606, has been the

[1] Wolfgang Ernest Heidel, *Johannis Trithemii ... Steganographia. Quae hucusque à nemine intellecta, sed passim ut supposititia, perniciosa, magica et necromantica, rejecta, elusa, damnata & sententiam Inquisitionis passa; Nunc tandem vindicata reserata et illustrata. Vbi post vindicias Trithemii clarissime explicantur conjurantiones spirituum ex arabicis, hebraicis, chaldaicis & graecis spirituum nominibus juxta quosdam conglobatae, aut secundum alios ex barbaris & nihil significantibus verbis concinnatae. Deinde solvuntur & exhibentur artificia nova steganographica a Trithemio in literis ad Arnoldum Bostium & polygraphia promissa, in hunc diem à nemine capta, sed pro paradoxis et impossibilibus habita & summe desiderata.* (Mainz: Joannes Petrus Zubrodt, 1676) and (Nürnberg: J. F. Rudiger, 1721), p. 120.

[2] Johannes Trithemius, *Polygraphia libri sex* (Oppenheim, 1518). See David Kahn, *The Codebreakers* (New York: Macmillan, 1967), pp. 132–137 for Trithemius's influence on modern cryptography. Noel L. Brann, *The Abbot Trithemius (1462–1516): The Renaissance of Monastic Humanism* (Leiden: E. J. Brill, 1981) and Klaus Arnold, *Johannes Trithemius (1462–1516)* (Würzburg: Kommissionsverlag Ferdinand Schöningh, 1971; 2nd ed. 1991) are the two standard modern accounts of Trithemius's life.

uncertain foundation of a different reputation: black magic.[3] *Uncertain,* because the *Steganographia* is, at least on first reading, deeply ambiguous. The work itself seems to be about using spirits — angels and demons — to send secret messages. But the preface to Book I of the *Steganographia* explains that the cryptographic techniques are purely natural. These are valuable techniques of statecraft and in order to keep them out of the hands of the enemies of the state (planning conspiracies) and adulterers (planning trysts) they are disguised by the use of a figurative language of demonology.

Most readers of the *Steganographia* have chosen to ignore its preface, discounting it as the author's evasive attempt to protect his demonology book from criticism. To them, Trithemius is one of the main figures in the occult movement of the 16th century and his *Steganographia* is one of the main early modern demonological treatises. Other readers, however, taking the preface at face value, see the *Steganographia* as a work of cryptography oddly expressed. To them, Trithemius is a cryptologist whose writings are misunderstood by occultists. These two different readings of the *Steganographia* have given rise to a long-running controversy about Trithemius's role in the rise of interest in magic and Hermeticism in the Renaissance: is the *Steganographia* primarily an exposition of cryptographic techniques disguised as angel magic, or is it primarily a magic work disguised as cryptography?[4]

[3] Johannes Trithemius, *Steganographia: Hoc est : Ars per occvltam scriptvram animi svi volvntatem absentibvs aperiendi certa; avthore reverendissimo et clarissimo viro, Joanne Trithemio...* (Frankfurt: Johannes Berner, 1606), often bound together with *Clavis Steganographiae Ioannis Trithemii Abbatis Spanheimensis* (Frankfurt: Johannes Berner, 1606) and the very short *Clavis generalis triplex in libros steganographicos Ioannis Trithemii abbatis Spanheimensis: ab ipso authore conscripta, et amatoribus huius artis gratitudinem declaraturis & secreto retentibus communicanda* (Frankfurt: Johannes Berner, 1606), of 192, 70, and 10 pages, respectively. There were confusingly many 17th century editions and translations; see the discussions in Joseph S. Galland, *An Historical and Analytical Bibliography of the Literature of Cryptology* (Evanston, Illinois: Northwestern University Press, 1945) and in David Shulman, *An Annotated Bibliography of Cryptography* (New York: Garland, 1976). I follow the pagination of the 1608 Frankfurt edition. I rely on photocopies of the 1608 and to some extent the 1606 Frankfurt editions of the *Steganographia* and the *Clavis*, and on a modern translation of Books I and III into English: *The Steganographia of Johannes Trithemius*, Fiona Tait and Christopher Upton, trans. (Edinburgh: Magnum Opus Hermetic Sourceworks, 1982). Continuing the confusion of editions into modern times is the fact that the translation of Book III in the 1982 Edinburgh edition is reprinted from an undated early 20th century otherwise unpublished translation by John William Henry Walden, *The cryptomenytics and cryptography of Gustavus Selenus: in nine books: wherein is also contained a most clear elucidation of the Steganographia, a book at one time composed in magic and enigmatic form by Johannes Trithemius ...*, a carbon copy typescript of which is item 12 in the Fabyan Collection of the Library of Congress.

[4] Accounts of the *Steganographia* controversy, differing only in amount of detail supplied, can be found in, for example: Lynn Thorndike, *History of Magic & Experimental Science*, 8 vols, (New York: Columbia University Press, 1923–1958), vol. 4, chap. 60, and scattered references throughout vols. 5 and 6; Arnold, 180–189; D. P. Walker, *Spiritual and Demonic Magic from Ficino to Campanella* (London: Warburg Institute, 1958), chap. 4, pp. 86–89; and more recently Wayne Shumaker, *Renaissance Curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language*, Medieval and Renaissance Texts and Studies, 8 (Binghampton, New York: Center for Medieval and Early Renaissance Studies, 1982), chap. 3, "Johannes Trithemius and Cryptography," and Ioan P. Couliano, *Eros et magie à la Renaissance, 1484* (Paris: Flammarion, 1984), the translation of which I rely

To understand the details of the controversy and to assess the arguments we have to look more closely at the book itself. Ostensibly the *Steganographia* explains how to employ spirits to send secret messages over distances. A large share of the book is devoted to recitation of the various ranks of spirits: their names, numbers, subordinates, and the particular compass directions, times of days, planets, and constellations they are associated with. Much of the book is devoted to texts of invocations, by which the spirits' aid is obtained.[5]

Books I and II include long turgid cover letters full of innocent sounding pieties; the shorter Book III has tables of numbers, whose columns are headed by zodiac and planetary symbols. Books I and II say that the way of sending a secret message begins: write an innocent cover letter on a piece of paper, invoke (with proper ritual) angelic help by reciting an incantation like

> Padiel aporsy mesarpon omeuas peludyn malpreaxo. Condusen, vlearo thersephi bayl merphon, paroys gebuly mailthomyon ilthear tamarson acrimy lon peatha Casmy Chertiel, medony reabdo, lasonti iaciel mal arti bulomeon abry pathulmon theoma pathormyn.[6]

A spirit messenger or two will turn up. Hand over the cover letter. On receipt of the cover letter one's correspondent goes through similar angelic ritual, with a similar but different magical spell, and straight away he knows the sense of the secret message. In Book III the way of sending a secret message is similar, with these differences: the spoken invocation is de-emphasized and lacks the long strings of demonic names, much study of the current astronomical situation is required, reference must be made to the special astronomical data appropriate to the particular spirits involved, one undertakes elaborate calculations, and there is no cover letter. One's secret message is conveyed without letters to one's correspondent, as if by telepathy.

Controversy over the character of the *Steganographia* began even before Trithemius finished writing it, with Trithemius's 1499 letter to his friend Arnoldus Bostius, describing the new book he was writing, the *Steganographia*. But Bostius had died by the time the letter arrived. His colleagues read and published its contents, which said that the book would be full of marvels, including over a hundred kinds of secret writing, a method for communicating one's thoughts by fire over a distance, a method for teaching rude uneducated people Latin and Greek, and a method for expressing thoughts to another while eating, sitting, or

on: *Eros and Magic in the Renaissance*, trans. Margaret Cook, (Chicago: University of Chicago Press, 1987) pp. 162–175.

[5] The best general description of the contents of the *Steganographia* is Shumaker, *Renaissance Curiosa*, chap. 3, "Johannes Trithemius and Cryptography."

[6] *Steganographia*, I, chap. 2, p. 8.

walking, without words, signs or nods, and many other things which are not to be divulged publicly. Trithemius, it was alleged, was either a liar or (if he really could do these things) an employer of demons.[7]

In 1500, possibly in reaction to this charge, Trithemius abandoned work on the book, but not, as the *Polygraphia* reveals, his interest in cryptography. Another letter, of 1509, from the mathematician Carolus Bovillus (1479–1567) to Germanus de Ganay (also a correspondent of Trithemius's), described a 1504 visit to Trithemius, who had shown Bovillus his *Steganographia.* Shocked by the strange names of spirits or demons, Bovillus asserted that the book should be burned and that Trithemius must have consorted with demons. This letter was published in 1510 and the Trithemius's reputation as an occultist was established, in spite of Trithemius's denials in the preface to his *Polygraphia.*[8] This reputation probably helped attract the attention of such figures as John Dee (1527–1608), Giordano Bruno (1548–1600), and Agrippa of Nettesheim (1486–1535).[9]

The controversy intensified with the 1606 printing of the *Steganographia,* the shorter *Clavis Steganographiae* and *Clavis Generalis,* presumably also by Trithemius or a confidant of his. The *Clavis Steganographiae* explained, in baldest cook-book fashion, how the ciphers of Books I and II of the *Steganographia* worked. The incantations were actually encrypted instructions for concealing a secret message within the cover letters. To read out the secret meaning of either, one selects a special subsequence of the letters, such as (in the case of the incantation quoted above) every other letter of every other word:

padiel aPoRsY mesarpon oMeUaS peludyn mAlPrEaXo ...

that is, *primus apex* ... Books I and II of the *Steganographia* contain a mind-numbing variety of such examples, some combined with monoalphabetic ciphers, almost all of them explained in the *Clavis.*[10]

The *Clavis* did not discuss the nature of Book III, which remained mysterious. Of the 180 numbered pages of the 1608 edition of the *Steganographia,* 159 are in Books I and II, leaving 21 in Book III, (i.e., 12% of the whole). Book III contains

[7] Paraphrased from Thorndike, 4: 524–525 and Couliano, 168.

[8] Paraphrased from Thorndike, 6: 438–441, Couliano, 169, and Brann, 29–30, 43–45.

[9] Dee's interest in the *Steganographia* is a fixture of Deistic writing. John E. Bailey, "Dee and Trithemius's 'Steganography,' " *Notes and Queries,* 5th series, 11 (1879), 401–402, 422–433 cites a letter of Dee's of 16 February 1563, describing his obtaining a manuscript copy of the *Steganographia,* "a boke for which many a lerned man hath long sowght and dayly yet doth seeke." Bruno's interest in the *Steganographia* is described in Frances Yates, *Giordano Bruno and the Hermetic Tradition* (London: Routledge and Kegan Paul, 1964), p. 258. Agrippa and Trithemius corresponded, and Agrippa possessed a copy of the *Steganographia* as well: Thorndike, 5: 131.

[10] A very clear explanation of all of these can be found in Shumaker, 100–105.

a preface and just a single truncated chapter, in striking contrast to the dozens of chapters found in the earlier books.

Then in 1624 the erudite Duke August II of Braunschweig–Lüneburg published his monumental work on cryptography, the *Cryptomenytices*, under the pseudonym Gustavus Selenus.[11] Book III of Selenus's book publicized the information in the *Clavis*, reorganizing the information to make it clearer. Selenus was unable to supply a cryptographic interpretation to Book III of the *Steganographia*, but in case some future reader might make sense of it, he reprinted the entire Book III in his book.[12]

Selenus's account of the *Steganographia* was followed by essentially all seventeenth century German books on cryptography: both purely technical treatises and Trithemius *apologetica.* These books — whose titles often contain phrases like *Trithemius vindicated* — explain the *Steganographia* as cryptography and thereby acquit its author of magic.[13] In one such book, published in 1676 in Mainz, W. E. Heidel claims to have discovered the true cryptographic meaning to Book III, and presents it in the form of a series of cryptograms. It is easy to guess that Heidel was bluffing, hoping to gain the glory for figuring out what Trithemius was doing in Book III without actually doing the work.[14]

Thus the controversy centers on the 21 pages of the incomplete Book III.

The modern scholarly majority or consensus opinion about the *Steganographia* is expressed by D. P. Walker:

> There is little doubt that the first two Books of the *Steganographia* do treat of cryptography, and that the angels and spirits in them can be satisfactorily explained as descriptions of the methods of encipherment . . . .

[11] Gustavus Selenus (August II, Duke of Braunschweig–Lüneburg), *Gustavi Seleni Cryptomenytices et Cryptographiae libri IX. in quibus & planissima Steganographiae à Johanne Trithemio . . . magicè & aenigmaticèe olim conscriptae, enodatio traditur* (Lüneburg, 1624). Gerhard Strasser, "The Noblest Cryptologist: Duke August the Younger of Brunswick-Luneburg (Gustavus Selenus) and his cryptological activities," *Cryptologia,* 9 (1983), pp. 193–217 gives a splendid treatment of his hero, the eponymous patron and enlarger of the great library at Wolfenbüttel. According to Strasser Selenus was a careful and thorough, if unoriginal, student of his subject.

[12] Selenus's edition of Trithemius's Book III is in *Cryptomenytices,* III, chap. 16. Selenus's book has a much higher standard of typography than the 1606 edition of Trithemius. Since Selenus consulted two different printed edtions of the *Steganographia* and a somewhat differing manuscript copy made in 1520 (as he explains in *Cryptomenytices,* III, chap. 15, p. 108; presumably this is the current Wolfenbüttel Codex 91.1), and since there does not seem to be any modern critical edition of the *Steganographia*, Selenus's version of Trithemius's Book III is very useful.

[13] As can be seen by scanning Galland's *Historical Bibliography.* The authors of these books include: Caramuel, Dullinger, Kircher, and Schott. Arnold, 190, cites Johannes d'Espieres, *Specimen steganographiae Joannis Trithemii . . . , quo auctoris ingenuitas demonstratur et opus a superstititione absolvitur, cum vindiciis Trithemianis* (Douai, 1641), which is not in Galland.

[14] Heidel, *Steganographia vindicata*, 122-123.

> But the Third Book, which is unfinished, does not, like the other two, contain any examples of enciphered messages; one is told to say the message over the picture of a planetary angel at the moment determined by complicated astronomical calculations. It seems most unlikely that these could be disguised directions for encipherment or any kind of secret writing.[15]

Therefore, Walker concludes, the work is primarily occult. This consensus view is also shared by modern occultists, according to whom Trithemius taught not just cryptographic secrets to his esoteric pupils Agrippa and Paracelsus.[16]

A minority of historians follow Wayne Shumaker in dissent, interpreting the same evidence differently.[17] According to Shumaker, all three books could be cryptographic, even though we lack direct evidence for Book III. The role of magic is uniform throughout the *Steganographia*: a metaphor and a disguise for cryptography. The structural role played by those elements present only in Book III, namely the planetary spirits and associated astronomical data, is precisely the same as that played by those found only in Books I and II, namely, the long spoken conjurations and the innocent-sounding cover letters. Just as the latter turned out to be vehicles for concealed cryptography, so the former must be, too.[18] Both Walker's and Shumaker's positions are, I think, tenable interpretations of the evidence available at the time. Shumaker's position had the advantage that it made the *Steganographia* a book with a single, unified theme, but it had the disadvantage that it lacked evidence for cryptography in Book III.

A few hold the agnostic compromise, that we cannot tell because Book III is so short and is probably incomplete. This is another form of contradiction of Walker's interpretation, for without the evidence of Book III, Walker has no

[15] Walker, 87. Walker's conclusions are based largely on his inability to solve Heidel's cryptograms, which he, understandably, suspects are bogus. He seems unaware of Selenus's book. Yates, 145, slyly exaggerates Walker to the point of contradiction, insinuating that Books I and II are not about cryptography, either: "The *Steganographia* purports to be, and perhaps really is to some extent about cryptography or ways of writing in cipher," citing the same locus in Walker, whom she usually believes. Couliano, who exaggerates Walker to the point of parody, relies on Heidel's description of the *Steganographia*.

[16] Such views are expressed in Adam McLean's introduction to the 1982 Edinburgh translation *The Steganographia of Johannes Trithemius*, and in the annotations by Donald Tyson in his edition of the London 1651 translation by J[ohn] F[rench] of Henry Cornelius Agrippa of Nettesheim, *Three Books of Occult Philosophy* (St. Paul, Minn.: Llewellyn Publications, 1995).

[17] Shumaker, 106 and 131, although throughout Chapter 3 Shumaker's exasperation with Walker is clear, especially on p. 98. Shumaker is followed by Strasser, "The Noblest Cryptologist."

[18] Shumaker, 106, points out that the numerical values in the astronomical tables in Book III are suspicious, since most exceed 360, the largest possible angular measurement in degrees. There, and on 131, he speculates that these numbers conceal cryptograms. See my note 26 below.

evidence.[19] A detailed study of the modern reception of the *Steganographia* would expose more variety of response yet.[20]

In the following sections of this paper I describe the contents of Book III in greater detail, outline the steps by which I found and solved cryptograms in Book III, and sketch some implications this discovery has for the study of the *Steganographia* and its author.

2. SYNOPSIS OF BOOK III

Book III begins (on page 160 of the 1606 edition) with a preface announcing the goal of presenting a method of transmitting messages afar without use of words, books, or messenger, which Trithemius had read about in a book by an ancient philosopher called Menastor.[21] Trithemius warns us that he will express himself obscurely:

> This I did that to men of learning and men deeply engaged in the study of magic, it might, by the Grace of God, be in some degree intelligible, while on the other hand, to the thick-skinned turnip-eaters (*imperitis Rapophagis*) it might for all time remain a hidden secret, and be to their dull intellects a sealed book forever.[22]

The method is based entirely on the seven planetary spirits and their twenty-one subordinate spirits. The preface continues on page 162 with a table, which I call the Preface Table, headed *Mansiones spirituum cum planetis vr. M. L. n. c.*, which gives data about these planets and spirits, illustrated in my Figure 1. This

[19] With regard to authorial intention, as opposed to reception of the *Steganographia*, the following seem true: An agnostic ignores Book III: it might as well not exist. For an agnostic uninterested in cryptography, the *Steganographia* might as well not exist. This seems to be close to Brann's position, who distances himself from the Walker consensus without actually joining the Shumaker camp. For the cryptographer Kahn, *The Codebreakers*, Book III should be ignored as a mental aberration, but the remainder of the *Steganographia* is of definite cryptographic interest. Of course both kinds of agnostic are potentially interested in the ways Book III of the *Steganographia* was read and understood.

[20] Only following the publication of Walker's *Spiritual and Demonic Magic* and Yates's *Giordano Bruno and the Hermetic Tradition* has demonic magic become recognized as an interesting category in early modern thought. It is not surprising, then, to find Trithemius elevated to a position of importance in such recent works as Couliano's *Eros and Magic*, where half of chapter 7, on "demonomagic," is devoted to him. Before the Warburg renaissance of magic, Trithemius was less important to modern historians. For Thorndike, writing in the first part of this century, Trithemius serves as a litmus-test for the credulity or sagacity of the many 16th- and 17th-century authors who expressed opinions for or against Trithemius.

[21] *Inueni in quodam libro cuiusdam antiqui Philosophi, qui dictus est Menastor, esse possibile, ut quadam arte mentis nostrae conceptum amico notum faciamus, quantumlibet absenti, in 24. horis, sine verbis, sine libris, & sine nuncio, perfectissime, latisssime & secretissime.* There is no entry for Menastor in *Paulys real-encyclopädie;* I suspect that he is a fabricated authority.

[22] *Steganographia* (Frankfurt, 1608), p. 161. J. W. H. Walden's translation, reprinted in the 1982 Edinburgh edition. All translations in this section are Walden's, in spite — as in this case — of its occasional oddness (perhaps for Walden to have a thick skin was to have a thick skull); all cited page numbers refer to the 1608 edition.

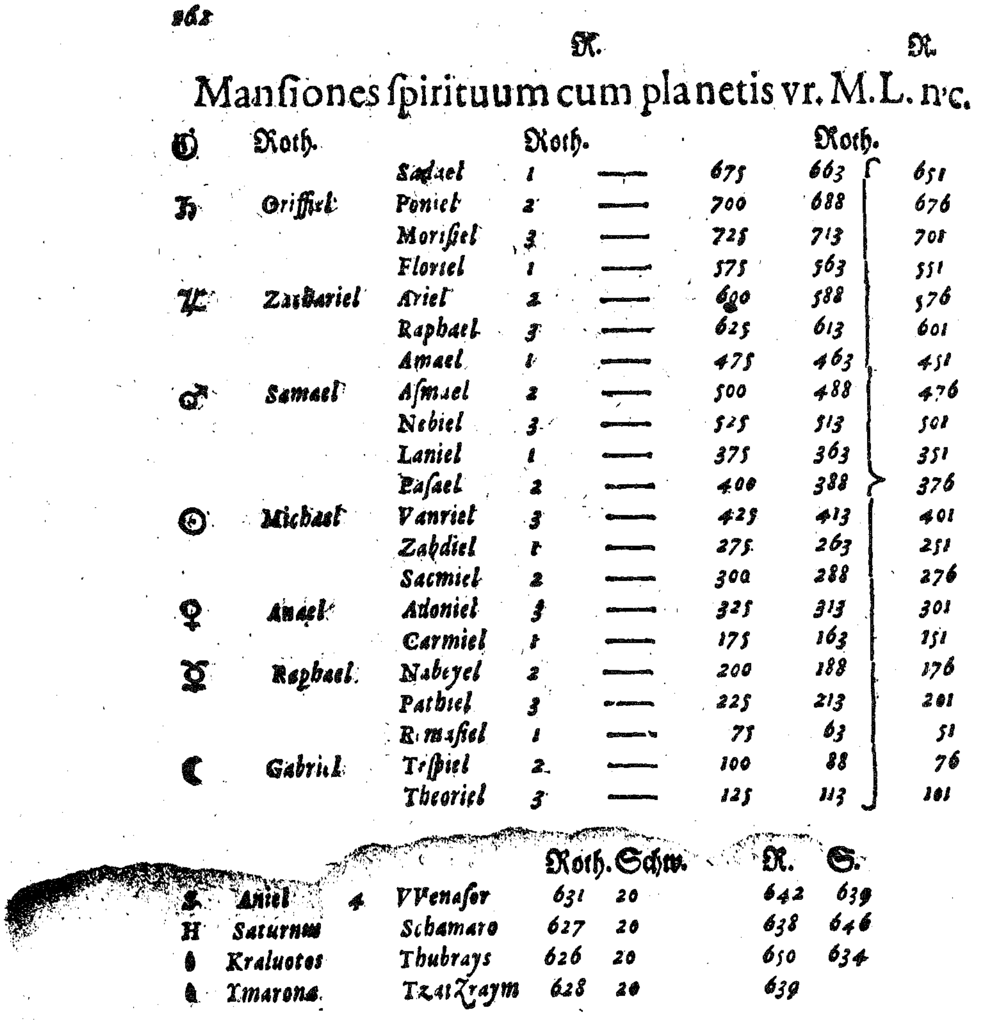
table, the first of eight in Book III, is laid out like a modern printed spread-sheet, that is, with easy-to-recognize rows and columns, each with its characteristic kind of data. The top portion of the table lists 21 subordinate spirit names, grouped by threes under their governing planets. For each spirit there are three numbers, the first of which is always a multiple of 25, the second of which is exactly 12 less than the first, and the third of which is always exactly 24 less than the first. The bottom portion has four lines. The first three of these lines has two spirit names and then four numbers; the last has three numbers. This time there is no simple arithmetical relationship between the numbers in a row, but the second number is always 20.

Evidently the data in the Preface Table is to be taken as generally descriptive of the entire technique of Book III. The preface concludes by promising seven chapters in all, one per planet, from Saturn to the Moon. In fact, only the first is given.

Chapter 1 begins on page 164. Its subject is how, with Saturn's help, one can secretly communicate with or without letters to a friend who shares our knowledge of the techniques. The plan of the chapter is generalities first, then examples.

Much of the general information is contained in four tables of planetary data. Each of three examples is accompanied by a table of its own. For convenience of reference I have labeled these seven Tables A through G. Unlike the Preface Table, Tables A through G lack row-and-column organization. Instead, the data is assembled into columns or column segments, but there does not seem to be any intention for the items in adjacent columns to necessarily line up into rows. The tables present the appearance of newspaper clippings pinned to a board: each clipping (column segment) has a clear enough succession of lines (data items) but clippings next to each other on the board are not perfectly aligned. Almost all of the data items within the columns are two- and three-digit numbers, but occasionally a word or astronomical symbol appears there, too. The columns are often headed with what are obviously labels (sometimes words, sometimes astronomical symbols) and other labels occur next to the column segments. Most of the tables appear very cluttered because in addition, what appears to be copy-editors' printing instructions for color of ink — instead of being followed by the printer — have somehow ended up in the printed text. These take the form of large German letters, either "S" or "R," or spelled out, "Schw." and "Roth" next to each column segment and each label, together with very large curly brackets typically spanning the length of a column.

Chapter 1 explains that one must know everything that astronomy ordinarily teaches about planetary motion: pure motion, proper motion, mixed, direct,



162

R. R.

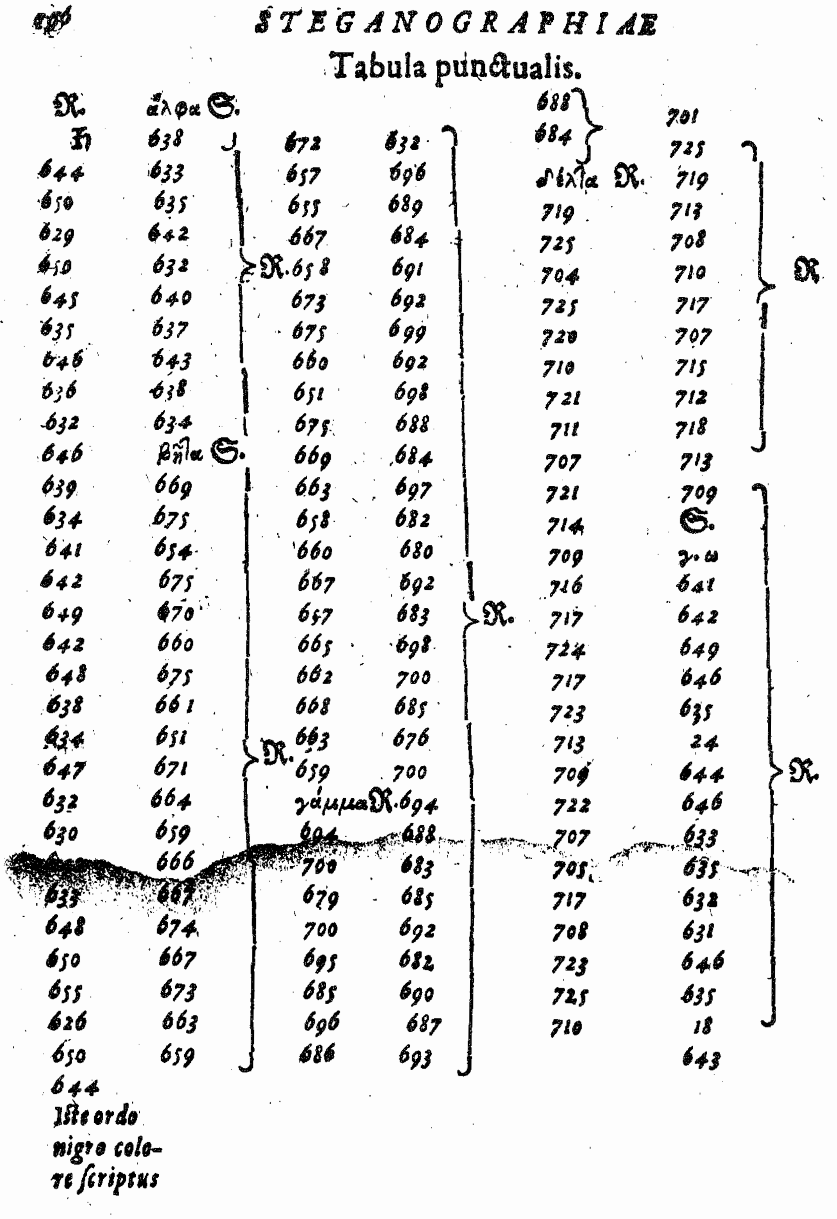
Manſiones ſpirituum cum planetis vr. M.L. n'c.

Ö	Roth.		Roth.			Roth.	
		Sadael	1	—	675	663	651
♄	Oriffiel	Poniel	2	—	700	688	676
		Moriſiel	3	—	725	713	701
		Floriel	1	—	575	563	551
♃	Zachariel	Ariel	2	—	600	588	576
		Raphael	3	—	625	613	601
		Amael	1	—	475	463	451
♂	Samael	Aſmael	2	—	500	488	476
		Nebiel	3	—	525	513	501
		Laniel	1	—	375	363	351
		Paſael	2	—	400	388	376
☉	Michael	Vanriel	3	—	425	413	401
		Zabdiel	1	—	275	263	251
		Sacmiel	2	—	300	288	276
♀	Anael	Adoniel	3	—	325	313	301
		Carmiel	1	—	175	163	151
☿	Raphael.	Nabeyel	2	—	200	188	176
		Pathiel	3	—	225	213	201
		Rimaſiel	1	—	75	63	51
☾	Gabriel	Teſpiel	2	—	100	88	76
		Theoriel	3	—	125	113	101

				Roth.	Schw.	R.	S.
	Aniel	4	VVenaſor	631	20	642	639
H	Saturnus		Schamaro	627	20	638	646
	Kraluotes		Thubrays	626	20	650	634
	Xmarona.		TzaiZraym	628	20	639	

Figure 1. "Preface table," *Steganographia*, p. 162.

Photograph courtesy of David Kahn.



166 STEGANOGRAPHIAE

Tabula punctualis.

𝔑.
ℌ
644
650
629
650
645
635
646
636
632
646
639
634
641
642
649
642
648
638
634
647
632
630
[illegible]
633
648
650
655
626
650
644
Iſte ordo
nigro colore ſcriptus

ἄλφα 𝔖.
638
633
635
642
632
640
637
643
638
634
βῆτα 𝔖.
669
675
654
675
670
660
675
661
651
671
664
659
666
667
674
667
673
663
659

𝔑.

𝔑.

672
657
655
667
𝔑.658
673
675
660
651
675
669
663
658
660
667
657
665
662
668
663
659
γάμμα 𝔑.694
694
700
679
700
695
685
696
686

632
696
689
684
691
692
699
692
698
688
684
697
682
680
692
683
698
700
685
676
700
688
683
685
692
682
690
687
693

𝔑.

688
684
δέλτα 𝔑.
719
725
704
725
720
710
721
711
707
721
714
709
716
717
724
717
723
713
709
722
707
705
717
708
723
725
710

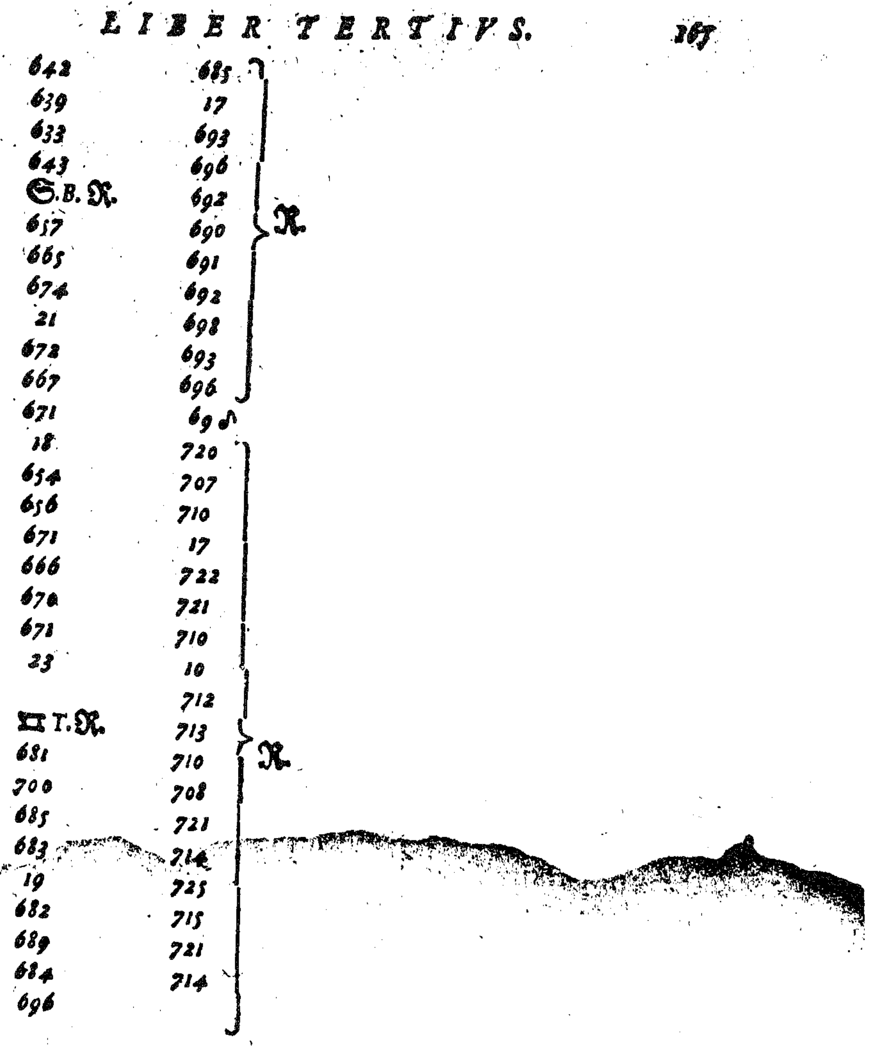
701
725
719
713
708
710
717
707
715
712
718
713
709
𝔖.
γ·ω
641
642
649
646
635
24
644
646
633
635
632
631
646
635
18
643

𝔑.

𝔑.

Figure 2. "Table A," *Steganographia*, pp. 166-167.

Photograph courtesy of David Kahn.



LIBER TERTIVS. 167

642
639
633
643
𝔖.B.ℜ.
657
665
674
21
672
667
671
18
654
656
671
666
670
671
23
♊ T.ℜ.
681
700
685
683
19
682
689
684
696

685
17
693
696
692
690 ℜ.
691
692
698
693
696
69∂
720
707
710
17
722
721
710
10
712
713 ℜ.
710
708
721
714
725
715
721
714

Figure 2. Continued

Photograph courtesy of David Kahn.

retrograde, and perplexed. But one also needs the added detail found in the first of the data tables, the *tabula punctualis* of pages 166 and 167, which I call Table A, illustrated as my Figure 1. After a page or so of text insisting that utmost care and precision be used in applying Table A, it turns out that A applies only when Saturn is in the ascendant, and that Table B (*tabula prima*, page 169) tells what to do when Saturn isn't. Immediately following B are Tables C (marked plain *tabula*, page 170) and D (marked *Motus planetarum purus*, page 171, illustrated as my Figure 3).

The discussion resumes on page 172 under the heading *De vario motu Planetarum, & interpretatione Tabularum.* All the data, it seems, are at hand, but to practice the message-sending art one must perform calculations of great intricacy:

> And unless one be thoroughly experienced in all these operations and know perfectly the mean motions of the planets themselves as also the smallest punctual divisions arising from the quarters, thirds, seconds, minutes, and degrees, which are all unequal and most minutely subdivided, he may easily fall into real errors and will hardly escape without grave peril.[23]

But, if you have read and understood everything, Trithemius promises at the top of page 175, it all works. To send a message without writing (*sine scriptis*) you perform the special calculations appropriate to the current astronomical situation and perform a ritual involving two pieces of paper, one with the calculations and the other with "the concept of your mind, whatever it is that you wish your distant friend to know."

The rest of the chapter is arranged into three examples, each with its own section heading and its own table.

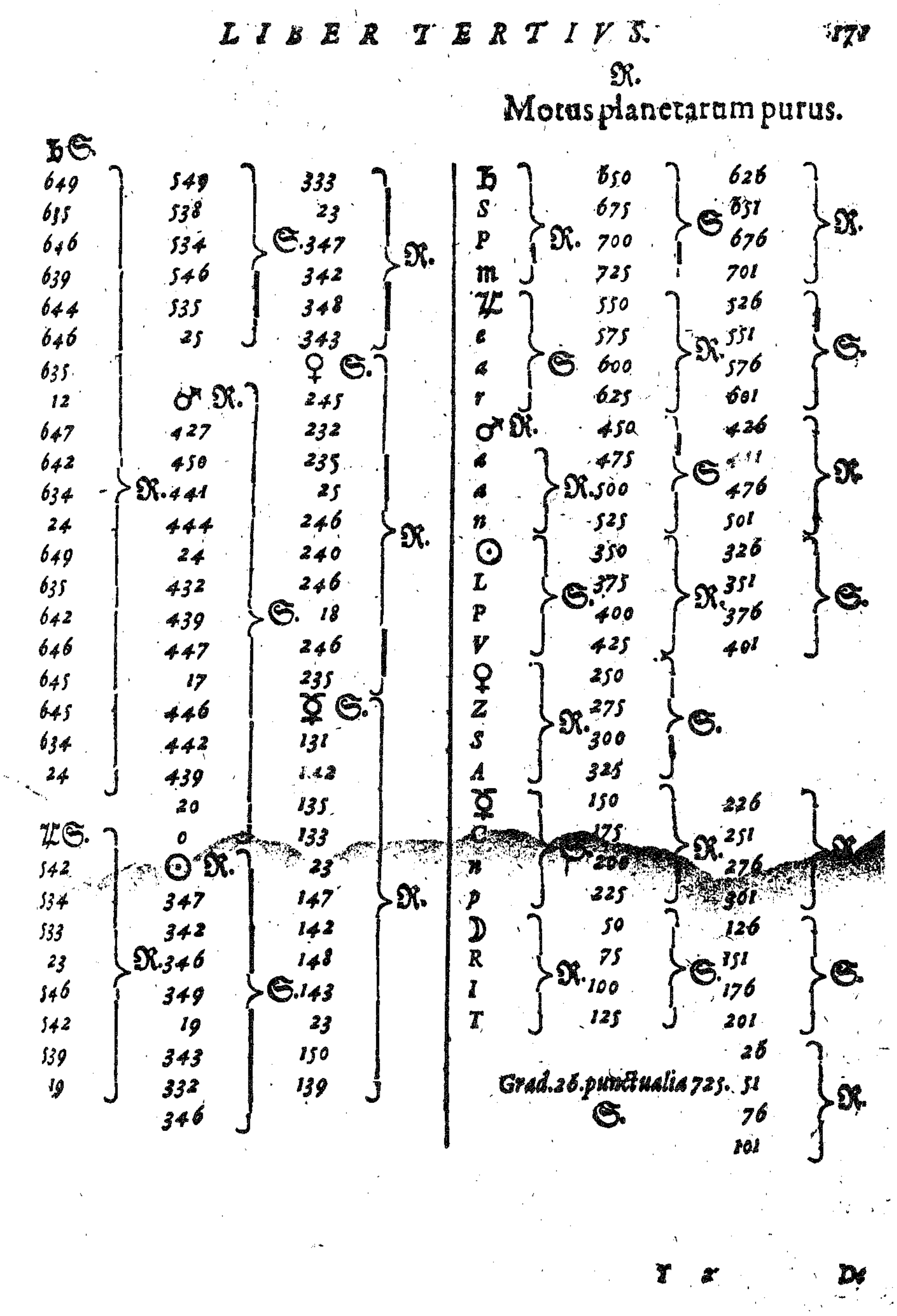
The first of these, headed *De primo Angelo Saturni, qui est principalis, & vocatur Orifiel, qui primam quartam Saturni obseruat,* starts on page 175. The astronomical calculations appropriate to the day of writing, 28 April 1500, are presented in Table E on page 176. The variations on the ritual appropriate to Orifiel are discussed: they involve pictures of Orifiel and of your distant friend, and a "movable vessel which the wise men of India call a *pharnat abronda.*"[24]

Picking up pace, the next section, *De secundo Angelo Saturni, qui est primus sub Orifiele & vocatur Sadael, praesidens secundae quartae Saturni* starts on page 178, and concludes with Table F and appropriate ritual on page 179.

The final section, *De tertio Angelo Saturni, qui est secundus sub Orifiele, & vocatur Pomiel, praesidens tertiae quartae Saturni*, occupies page 180, the last in

[23] *Steganographia*, p. 172.

[24] Much more detail about the rituals involved is given in Couliano, 172–173.



LIBER TERTIVS. 171

𝔑.

Motus planetarum purus.

♄𝔖.			
649	549	333	
635	538	23	
646	534	𝔖.347	𝔑.
639	546	342	
644	535	348	
646	25	343	
635		♀ 𝔖.	
12	♂ 𝔑.	245	
647	427	232	
642	450	235	
634	𝔑.441	25	
24	444	246	𝔑.
649	24	240	
635	432	246	
642	439	𝔖. 18	
646	447	246	
645	17	235	
645	446	☿ 𝔖.	
634	442	131	
24	439	142	
	20	135	
♃𝔖.	0	133	
542	☉ 𝔑.	23	
534	347	147	𝔑.
533	342	142	
23	𝔑.346	148	
546	349	𝔖.143	
542	19	23	
539	343	150	
19	332	139	
	346		

♄		650		626	
S		675	𝔖	631	𝔑.
P	𝔑.	700		676	
m		725		701	
♃		550		526	
e		575	𝔑.	551	𝔖.
a	𝔖	600		576	
r		625		601	
♂ 𝔑.		450		426	
a		475	𝔖	[illegible]	𝔑.
a	𝔑.	500		476	
n		525		501	
☉		350		326	
L	𝔖.	375	𝔑.	351	𝔖.
P		400		376	
V		425		401	
♀		250			
Z	𝔑.	275	𝔖.		
S		300			
A		325			
☿		150		226	
C		175	𝔑.	251	𝔑.
n	𝔖.	200		276	
p		225		301	
☽		50		126	
R	𝔑.	75	𝔖.	151	𝔖.
I		100		176	
T		125		201	
				26	
Grad.26.punctualia 725.				51	𝔑.
	𝔖.			76	
				101	

Y z De

Figure 3. "Table D," *Steganographia*, p. 171.

Photograph courtesy of David Kahn.

the book. Its calculation is given in Table G, and the ritual receives a perfunctory two lines.

Of the promised seven chapters only the first is present, and that evidently in truncated form, for the section covering Morisiel and the fourth quarter of Saturn is missing.

3. CRYPTANALYSIS

On receiving a photocopy of the *Steganographia*, I decided to see if I could find any hidden messages in Book III. I knew that Book III was probably in a draft state. Hence, it might be missing important information; the printed version had of course not received the author's proof corrections. If Book III was anything like Books I and II, it was probably pointless to try to follow the instructions given in the text. Moreover, I could expect that any plaintexts would be short and banal.

Unlike Books I and II, Book III did not offer much material to work with. Where they contain dozens of examples and stretch over 159 pages, Book III seemed to contain three examples covered in 21 pages.

Finally, if the tables were important, it would not be clear how to read them, nor what role the copy-editors' ink color notations or the astronomical symbols would play.

3.1 A guess

Somehow, a guess formed in my mind that turned out to be lucky. Perhaps a recent success in finding previously unnoticed structure in the contents of some early modern magic tables led me to this guess, or at least gave me courage to pursue it.[25] My guess had several parts: the cipher was numerical (this was easy, since the numerical tables in Book III were the only obvious places to *put* a ciphertext), the tables were to be read in columns vertically, and the Preface Table was a form of key.[26] I read the successive lines of the Preface Table as describing ranges or blocks of 25 numbers each, each one of which might somehow specify a distinct letters-to-numbers encryption formula.

[25] J. Reeds, "John Dee and the Magic Tables in the *Book of Soyga*," to appear, 1999.

[26] I was partly anticipated by Shumaker, *Renaissance Curiosa*, pp. 106 and 131. The background for Shumaker's guess is amplified in Gerhard F. Strasser, *Lingua Unversalis, Kryptologie und Theorie der Universalsprachen im 16. und 17. Jahrhundert*, Wolfenbütteler Forschungen, 38 (Wiesbaden: In Kommission bei Otto Harrassowitz, 1988), pp. 174–176, which I saw only after solving the Book III cryptograms. Strasser describes a cipher of Athanasius Kircher, *Polygraphia nova et vniversalis ex combinatoria arte detecta* (Rome: Varesius, 1663), pp. 132–134, (which I have not seen) that is almost identical with Trithemius's.

With this hunch I looked at the numerical tables in the main part of Book III, transcribing as best I could the numerical data in the columns, transposing it as I went so each column in the original became a row.[27] I rigorously excluded all data not appearing in columns, including column headings.

On pages 166–167 appears Table A, the *Tabula punctualis*, with eight columns, as follows.

(A1) / 644 650 629 650 645 635 646 636 632 646 639 634 641 642 649 642 648 638 634 647 632 630 642 633 648 650 655 626 650 644

(A2) 638 633 635 642 632 640 637 643 638 634 / 669 675 654 675 670 660 675 661 651 671 664 659 666 667 674 667 673 663 659

(A3) 672 657 655 667 658 673 675 660 651 675 669 663 658 660 667 637 665 662 668 663 659 / 694 700 679 700 695 685 696 686

(A4) 632 696 689 684 691 692 699 692 698 688 684 697 682 680 692 683 698 700 685 676 700 694 688 683 685 602 682 690 687 693

(A5) 688 684 / 719 725 704 725 720 710 721 711 707 721 714 709 716 717 724 717 723 713 709 722 707 705 717 708 723 725 710

(A6) 701 725 719 713 708 710 717 707 715 712 718 713 709 / 641 642 649 646 635 24 644 646 633 635 632 631 646 635 18 643

(A7) 642 639 633 643 / 657 665 674 21 672 667 671 18 654 656 671 666 670 671 23 / 681 700 685 683 19 682 689 684 696

(A8) 685 17 693 696 692 690 691 692 698 693 696 696 720 707 710 17 722 721 710 10 712 713 710 708 721 714 725 715 721 714

Here, and in all the following examples, I put a / sign in place of any nonnumerical data. I have given each transcribed column a letter and number in parentheses for ease of reference later in the paper. The rest of the numerical data is given in an appendix.

I noticed that the four intrusive nonnumerical data items, marked with / signs in the first five columns (to wit: the astronomical sign for Saturn, and the words — spelled out in Greek letters — *βητα*, *γαμμα*, and *δελτα*) were regularly spaced: they divided the first 160 numbers into four blocks of exactly 40 numbers each. Moreover, almost all the numbers in the first block of 40 were in the numerical range 626 – 650, almost all those in the second block were in the numerical range 651 – 675, those in the third block in the range 676 – 700, and those in the fourth block in the range 701 – 725. That the latter three of these ranges appeared in the first three rows of the Preface Table encouraged me.

[27] I used photocopies of the 1608 Frankfurt edition of the *Steganographia*, and where that was unclear, of the 1624 edition of Selenus.

So I wrote these four blocks of 40 numbers each, the first 160 numbers in A1 through A5, in four rows of 40, one underneath the other, in order to see if there was any parallelism or similarity of structure between the blocks, as follows (showing the first 10 numbers in each row):

(R1)	644	650	629	650	645	635	646	636	632	646 ...
(R2)	669	675	654	675	670	660	675	661	651	671 ...
(R3)	694	700	679	700	695	685	696	686	632	696 ...
(R4)	719	725	704	725	720	710	721	711	707	721 ...

It was then evident that with only a few exceptions the numbers in R2 are 25 greater than the corresponding numbers in R1, that those in R3 are 25 greater than the corresponding entries in R2 and 50 greater than those of R1, and so on. That is, most of the columns of this diagram form little arithmetic progressions, incrementing by 25s. Reading horizontally, the pattern in R1 was repeated in R2 but with an additive offset of 25, in R3 with an offset of 50, and in R4 with an offset of 75. In cryptanalysts' jargon, when I wrote the data out "on a width of 40," I discovered repetition"in depth," with additive offsets which were multiples of 25.

Although I still did not know that there was a cipher present, it was clear from the emergence of this pattern that there was enough truth in my initial guesses about column reading and the importance of the number 25 to continue further, in particular, to continue transcribing the data.

And if there *were* a cipher present, this finding would surely be due to the presence of four copies of an *isolog*: four copies of the same plaintext encrypted in different but related ways. I could probably put the separate blocks of numerical ranges on "common base" by reducing them modulo 25. That is, if I knew how to read those parts of the text encoded with numbers in the range 626 through 650, I could probably use the same recipe to read those parts encoded with numbers in the range 651 through 675: simply subtract 25 from each number, thereby putting them into the range 626–650, and proceed as before, and so on.

3.2 First plaintext

The simplest possible cipher I could imagine applying to the 40 numbers in R1 was a simple, or monoalphabetic, substitution. Such ciphers can typically be solved (and uniquely so) given a cipher text sample as short as about 30 letters.[28]

[28] William F. and Elizebeth S. Friedman, *The Shakespearean Ciphers Examined* (Cambridge: Cambridge University Press, 1958), pp. 22–23 address precisely this point, with regard to ciphers in English: "about twenty-five letters are needed before the cryptanalyst can be sure that his solution of a mono-alphabetic substitution cipher is the only possible solution," relying on their own vast experience as practicing cryptanalysts and

The first step of solution is to prepare a frequency count of the cipher symbols. Of the 40 numbers in R1, 39 were in the range from 626 through 650. Their frequency count was

626	1	631		636	1	641	1	646	2
627		632	3	637	1	642	4	647	1
628		633	2	638	3	643	1	648	2
629	1	634	3	639	1	644	2	649	1
630	1	635	2	640	1	645	1	650	4

which seemed uneven enough to be consistent with a Latin or German plaintext. Since the presumed cipher symbols had a natural numerical ordering, it seemed prudent to check out the possibility that the cipher values were assigned to the plaintext letters in alphabetic order or backwards alphabetic order. So I considered fitting direct and reversed alphabets to this frequency distribution. The word "retrograde" in a passage on page 164 seemed to suggest the possibility of a reversed alphabet:

> Thus if you wish to operate in Steganography . . . you must first of all acquaint yourself with his [Saturn's] various and diverse motions; and first the various motions, pure, proper, mixed, direct, retrograde and perplexed.

But I was unsure about the precise composition of the alphabet. In the *Clavis*, chapter 2, a Latin alphabet of 22 letters is used (with Y dropped) and in the *Polygraphia* a 24-letter alphabet is used (with W appended after the usual 23).

A few minutes of experimentation showed that a reversed 22-letter alphabet seemed to fit this frequency distribution well (with α, β, and γ being stand-in names for the three letters past Z):

626	1	γ	631		X	636	1	Q	641	1	L	646	2	E
627		β	632	3	U	637	1	P	642	4	I	647	1	D
628		α	633	2	T	638	3	O	643	1	H	648	2	C
629	1	Z	634	3	S	639	1	N	644	2	G	649	1	B
630	1	Y	635	2	R	640	1	M	645	1	F	650	4	A

on theoretical calculations (which were some of the first fruits of the then-new information theory) of C. E. Shannon, "Communications Theory of Secrecy Systems," *Bell System Technical Journal*, 28 (1949), 657–715 and "Prediction and Entropy of Printed English," *Ibid.*, 30 (1951), 50–64. The longer the cryptogram the easier it is to solve, and the more certain we can be that the solution is the only one possible. Latin, according to a crude calculation of mine based on the text of the Vulgate Bible and on the corpus of all the Sherlock Holmes stories, has a slightly lower entropy than English does. Hence substitution ciphers of this type are somewhat easier to solve in Latin than in English. By increasing Friedmans' 25 letters to 30 letters and by replacing English by Latin, I make the cryptanalysis task easier and the uniqueness claim for the solution more certain.

This guess, applied to the 40 letters of R1, yielded the following trial plaintext: *gazafrequenslibicosduyitca?γagotriumphos* which, meaningless as it was to me, still seemed perfectly pronounceable, with the sort of vowel-consonant alternation found in the conjurations in Books I and II of the *Steganographia.* Here the ? symbol corresponds to the one number in R1 which was not in the range 626 – 650, namely the 655 near the end of column A1. The sequence *frequens* was particularly encouraging to me, and, I must confess, the sequence *triumphos* reflected my feelings precisely. I felt I was still on the right track, even if I could not yet understand the plaintext.

3.3 Key recovery

Encouraged by the results so far, I guessed at the following decryption recipe: cipher numbers greater than 25 were to be reduced modulo 25 and understood by the reversed alphabet given above. Cipher numbers 25 or less are treated as nulls. Assigning the values α, β, and γ to the three letters past Z, and breaking words at nulls (and occasionally arbitrarily, to make them legible), the corpus of transcribed cipher numbers in Tables A–G yielded the following tentative plaintext:

> *gaza frequens libicos duyit cayγago triumphos gaza fraqγens libicos duyit carγago triumphos gaza frequens libicos duyit carγago triumphos gaza frequens libicos duyit carγago triumphos liber getruxer hinthumb die zxelfe xart unser heimlicheefur der portenamen*
>
> *nit lais duher zu mir noit gch andel us zudas ich lden brenge ail xeis soch behalt*
>
> *commest noch hintxan is duet habe ein grosenrichten mit dir dir hab mit dirund sehddis allesgeben zuals dunust uqrebi dirserehahx*
>
> *brenger dis brieffs ist ein boser βalg und ein dieb huet dichfur eme erxirt dich an*
>
> *miserere mei deus secundu magnum donum tuum amenaγ*
>
> *gaza frequens libicos duyit carγago triumphos xαβ*
>
> *gaza frequens libicos durγago yit catriumphos β*

The initial four repetitions of *gaza frequens* ... (which I broke into "words" arbitrarily) are, of course, R1 through R4. I read the immediately following text as a distorted form of *Liber getruwer,* (i.e., *Lieber getreuer*) a phrase that Trithemius uses to begin many of his plaintexts in Books I and II. So what I had thought was an *x* was really a *w*. Towards the end of this jumble of tentative plaintext is the phrase *brenger dis brieffs ist ein boser βalg und ein dieb,* which means something like ... *bringer of this letter is a bad* ___ *and a thief.* A glance at a German-English dictionary turned up the entry Schalk = rogue, so it was safe to guess that the second letter past Z, which I had written as β, was really the common German letter sequence *sch.*

At this point I was able to go systematically through the whole text of Book III and see in what contexts the various snippets of plaintext appeared.

The bottom section of the Preface Table has some numbers in columns 5, 7, and 8 which could be cipher values:

col 1.	col. 2	col. 3	col. 4	col 5.	col. 6	col. 7	col. 8
S	Aniel	4	Wenasor	631	20	642	639
H	Saturnus		Schamaryo	627	20	638	646
	Kraluotos		Thubrays	626	20	650	634
	Ymarona		Tzatzraym	628	20	639	

On applying the decryption formula as derived so far, the bottom of the table now looked like:

col 1.	col. 2	col. 3	col. 4	col 5.	col. 6	col. 7	col. 8
S	Aniel	4	Wenasor	W	20	I	N
H	Saturnus		Schamaryo	Sch	20	O	E
	Kraluotos		Thubrays	γ	20	A	S
	Ymarona		Tzatzraym	α	20	N	

I noticed that the identified values in column 5 matched the initial letters of the spirit names in column 4. This allowed me to fill in the two remaining holes in the deciphering formula: α, the letter after Z, is *tz*, the letter after that, β, is *sch* (which I had already concluded) and the letter after that, γ, is *th.* Presumably this bottom section of the table was intended to serve as a memory aid, showing where the cipher alphabet must be augmented to handle the German language.

And I saw the author's signature in columns 7 and 8: IOANNES.

One final piece of luck cinched the identification of the cipher alphabet. I submitted the two-word phrase *gaza frequens* to an internet web search engine, and back came the report that the words *Gaza frequens Libycos duxit Carthago triumphos* ... occur as an *incipit* in a manuscript (Cod. 1796) in the great monastic library in Melk, Austria.[29] This confirmed the γ=*th* conclusion and

[29] The sentence *Gaza frequens Libycos duxit Karthago triumphos*, I realized later, uses every letter of the Latin alphabet, and so is an equivalent to our *The quick brown fox jumps over the lazy dog.* It means, roughly, "Crowded with treasure, Carthage held Libyan triumphal processions." As such it is a convenient plaintext to use for illustrative purposes, as e.g., Selenus does in *Cryptomenytices*, p. 249. It was used in the Middle Ages as a writing exercise; see Berhard Bischoff, "Elementarunterricht und Probationes Pennae in der ersten Hälfte des Mittelalters," appearing in his *Mittelalterliche Studien: Ausgewählte Aufsätze zur Schriftkunde und Literaturgeschichte* (Stuttgart: Anton Hiersemann, 1966), 1:74–87.

told me that what I thought was a *y* might well be *x*, the *y* of the plaintext *Libycos* being replaced by *i*.

Thus, the complete deciphering rule is: numbers greater than 25 are significant, and their plaintext value depends only on their remainder upon division by 25, and in particular, only on the right-hand two digits of the number. The following table gives the mapping. The two right-hand-most digits of the cipher number are found in the bottom portion of the table, the letter or letter combination above it is the plain equivalent.

Th	Sch	Tz	Z	X	W	U	T	S	R	Q	P	O
01	02	03	04	05	06	07	08	09	10	11	12	13
26	27	28	29	30	31	32	33	34	35	36	37	38
51	52	53	54	55	56	57	58	59	60	61	62	63
76	77	78	79	80	81	82	83	84	85	86	87	88

N	M	L	I	H	G	F	E	D	C	B	A
14	15	16	17	18	19	20	21	22	23	24	25
39	40	41	42	43	44	45	46	47	48	49	50
64	65	66	67	68	69	70	71	72	73	74	75
89	90	91	92	93	94	95	96	97	98	99	00

In short: the Book III ciphers are numerical substitution ciphers, with multiple numerical equivalents supplied for each plaintext letter. The cipher is actually used in a piece-wise monoalphabetic fashion, shifting ranges of cipher numbers after every few letters.

One could interpret it as a primitive form of polyalphabetic encryption: an alternation between any of a variety of monoalphabetic substitutions, but with the special feature that the cipher equivalents in the several monoalphabetic alphabets do not overlap. A more secure cipher was described in Trithemius's later *Polygraphia*, where the cipher equivalents of the various alphabets *do* overlap. From this point of view, the Preface Table, and the numerical ranges implied by its 6th and 8th columns, can be regarded as a primitive form of Vigenère table, examples of which appear in Book V of the *Polygraphia*.

3.4 Plaintexts

We have seen that the Preface Table contained the enciphered signature *Ioannes* and the four isolated letters and letter sequences *W, Sch, Th, Tz* in a diagram context rather than a prose context. Applying the key to the various transcribed ciphertexts of Tables A–G yields the following passages of plaintext. I render null characters (that is, those with numerical values of 25 or less) with a /, and supply additional word breaks as needed.

A. Pages 166–167, *Tabula punctualis.*

> *gaza frequens libicos duxit caxthago triumphos gaza fraqthens libicos duxit carthago triumphos gaza frequens libicos duxit carthago triumphos gaza frequens libicos duxit carthago triumphos*
>
> *liber / getruwer / hinthumb / die / zwelfe / wart / unser / heimliche efur / der / porten amen*

B. Page 169.

> *nit / lais / duher / zu / mir / / noit / gch / / andel / us / zudas / ich / lden / brenge / ail / weis / soch / behalt*

C. Page 170. Columns not very clearly laid out, so plaintext scrambled.

> *commest / noch / hintwan / is / duet / habe / ein / grosen richten / mit / dir / / dir / hab / mit / dir und / sehd dis / alles geben / zuals / dunust / uqrebi / dir sere hahw*

The columns are laid out somewhat differently in Selenus (p. 123), resulting in the following reading (adding word breaks at the ends of column segments):

> *commest / noch / hint wan / is / duet / ha habe / ein / grosen sere richten / mit / dir / / h dir / hab / geben / zu mit / dir als / du w und / sehd nust / uqre dis / alles bi / dir*

Neither reading is satisfactory. It seems likely that some text was lost, and what survives is thus an incomplete collection of isolated sentence fragments.

D. Page 171, the first three columns of the *Motus planetarum purus.*

> *brenger / dis / brieffs / ist / ein / boser / schalg / und / ein / / dieb / huet / dich fur / eme / er wirt / dich / an*

The text seems to break off. *Eme* is presumably *ihm.*

E. Page 176, *Tabula.*

> *miserere / mei / deus / / / / / / / / secundu / magnum / donum tuum amen ath*

This seems close to Psalm 51.

F. Page 179, unnamed table.

gaza / frequens / libicos / duxit / carthago / triumphos wtzsch

G. Page 180, unnamed table.

gaza / frequens / libicos / du rthago / xit / ca triumphos / / sch

This text is somewhat scrambled. If column G6 is read before column G5 the usual version emerges. The column headings for G1 through G8 are (in that order) labeled *horae* 7, 8, 9, 7, 9, 8, 7, 8, but if G5 and G6 are interchanged the column headings are for *horae* 7, 8, 9, 7, 8, 9, 7, 8. This permutation could be either part of Trithemius's cipher which I did not diagnose properly, or the result of careless typography.

One could wish for more interesting plaintexts. Although it is possible that a manuscript copy of the *Steganographia* with fewer garbles might be found, allowing better readings of B and C, it is also possible that the garbles originated with Trithemius, and no correct versions of the ciphertexts ever existed. In any case, the concealed messages of Book III are clearly no more interesting than those of Books I and II.

CONCLUSIONS

Book III contains cryptograms. Like those in Books I and II, they are disguised, and presented in a context of angelic magic. The cryptographic technique is different: instead of the plaintext letters being hidden within a larger mass of letters as in Books I and II, in Book III they are represented by numbers disguised as astronomical data. As in the previous books, the text of Book III can be understood as a description of the cryptographic process only if interpreted figuratively. For these reasons it seems safe to conclude that the author's intent and method of exposition is uniform throughout the *Steganographia*, and that only at the level of technical details (spirit names and attributes at the occult level, numbers of letters to skip or letter-to-number equivalents at the cryptographic level) is there any variation. This contradicts the view of D. P. Walker, according to which Books I and II were cryptography and Book III purely magic, without cryptography.

When we focus on the narrow question of the intent of the *Steganographia* and disregard the larger questions of Trithemius's interest in magic and his influence on magic, the past five centuries of the *Steganographia* controversy can be understood as an ongoing legal process, whose terms and standards of evidence have remained unchanged. Charges that the *Steganographia* was magical were brought in the 16th century, informally by Bovillus and later more formally, resulting in the prohibition of 1609.[30] Placement on the Index was in effect an interim judgment: the *Steganographia* is a magic book. Appeals were lodged by Selenus and Heidel and others in the 17th century, on the grounds that Books I and II were not magic, citing the evidence in the *Clavis*. These appeals were ruled upon favorably in 1958 by Walker, but only to the extent that the evidence for magic in the cases of Books I and II was ambiguous and hence inadmissible. But Heidel's 1676 expert testimony that Book III is also cryptographic is found inadmissible, on the completely reasonable grounds that it is incomprehensible: expert testimony (if it is to be believed) should not be given in the form of insoluble cryptograms. The ostensible purpose of Book III clearly *is* magic, so the conviction of the *Steganographia* still holds. Shumaker in 1982 protested this judgment: in the case of Book III, Walker was applying the dangerous argument from the absence of evidence to prove the contrary. Shumaker, however, was unable to excuse the magic elements of Book III, except by analogy with those of the previous books: just as they turned out innocent, no doubt Book III would too. Finally, this paper brings new evidence to the matter: proof of cryptography in Book III, which therefore should make that book, too, inadmissible as evidence for the original charge that the *Steganographia* is a magical book.

Of course, over the centuries the prosecutors' motives and the consequences of conviction have changed. In 1609 it was desired to protect the faithful from dangerous ideas, while in 1958 it was desired to reassess and rebuild the place of magic in the historiography of early modern thought. In 1609, proving the *Steganographia* was a book of magic meant condemnation of the author. In our time, it has instead enhanced its author's reputation as an interesting figure in intellectual history.

It is not for me to say how Trithemius's position in the history of early modern magic will need to be adjusted, other than to suppose it will be downgraded. Nor it it exactly clear to me why, in 1958, Walker felt it necessary to revisit the narrow matter of the actual intent of the *Steganographia*, as opposed to its 16th and 17th century reception. But whatever historiographical advantage was gained by Walker's interim judgement that the *Steganographia* was primarily magical will — it seems to me, a nonhistorian — have to be relinquished.

Although this demonstration of Trithemius's sustained cryptographic purpose

[30] Arnold, 185, cites Martinus Delrio, *Disquisitionem magicarum libri sex* (Louvain, 1599), citing p. 111 of the 1679 Cologne edition: "Steganographiae, periculi et superstitionis plenissimae . . . , quod nondum prohibitis ab Ecclesia libris sit insertum," and Heinrich Reusch, *Der Index der verbotenen Bücher, ein Beitrag zur Kirchen- und Literaturgeschichte,* 2 vols. (Bonn: Verlag von Max Cohen, 1885), 2: 183, paraphrases Antonius Possevinus, *Apparatus sacer,* 3 vols., (Venice, 1603–1606), 1: 945 as holding that "est sei nicht eine clavis polygraphiae, sondern superstitionis et periculi plenissimum magiamque sapit, non naturalem illam, quo tamen nomine plerique suas sordes tegunt, verum etiam ipsam, quae cum a S. Rom. Ecclesia prohibita sit una cum ejusmodi libris in Rom. Indice, haud dubium quin et istud sit ablegandum."

throughout the *Steganographia* may undermine Trithemius's importance in the history of early modern magic from one point of view, it increases the interest in his book from another. The question now is: why did Trithemius so thoroughly embrace the rhetoric of magic for such a nonmagical — as we regard it — purpose? Did *he* regard cryptography as inherently magical, or was his choice of that language a solution to the stylistic problem that all authors of cryptographic exposition have to solve: how to sustain the reader's interest through example after example of usually tedious plaintexts, possibly tedious explanations of cryptographic techniques, and always tedious ciphertexts? Trithemius's use of angel language might thus be a rhetorical strategy to engage the reader's interest. If so, he was vastly successful, even if he completely miscalculated how his book would be received.

ADDED IN PROOF

After submitting this paper for publication I became aware of a long article by Thomas Ernst, "Schwarzweiße Magie: Der Schlüssel zum dritten Buch der Steganographia des Trithemius," *Daphnis: Zeitschrift für Mittlere Deutsche Literatur* 25, no. 1 (1996): 1–205, which was also published as a separate book (Amsterdam: Rodopi, 1996). In this magisterial article Ernst reaches exactly the same cryptographic conclusions that I did, but three years earlier, and in greater detail.[31] Ernst, working from manuscript copies of Book III in Wolfenbüttel and in the Vatican, for which he provides a critical edition, is able to complete the sentence in Table D. He too sees the cipher of Book III as a transitional form between the monoalphabetic ciphers of classical antiquity and the middle ages and the truly polyalphabetic ciphers of Trithemius's *Polygraphia.* Ernst persuasively argues that the *Clavis Steganographiae* is an earlier version or draft of the *Steganographia.* Finally, Ernst was able to solve Heidel's cryptograms, which show that Heidel had indeed also solved Trithemius's Book III ciphers.

Thus "Thomas Ernst" is the answer to Heidel's question, quoted as the epigraph of this paper: "Who will divine, what Trithemius wrote in this third book of *Steganography*, and what he would have written?"

ACKNOWLEDGEMENTS

I am most grateful to Clay Holden for helping me obtain photocopies of the texts, to Drs. S. Clucas, David Ganz, J. V. Field, K. M. Reeds, and G. F. Strasser for help with the exposition and to Professor Elaine Tennant for help with the

[31] Chronology: I received my *Steganographia* photocopy on 2 March 1998, had my first plaintext on 5 March, the first draft of this paper on 9 March, learned about the existence of Ernst's paper on 1 April 1998 and received confirmation that it indeed solved Trithemius's Book III cipher on 3 April.

German. Thanks also to J. C. Lagarias, Doug McIlroy, Mario Szegedy, and Ross Eckler.

APPENDIX: REMAINING CIPHER DATA

B. On page 169 there is a *Tabula prima*:

(B1) 639 642 633 23 641 650 642 634 24 647 632
(B2) 693 696 685 25 679 682 22 690 692 685 25
(B3) 16 639 638 642 633 13 644 648 643 23 0
(B4) 700 689 697 696 691 21 682 684 24 679 682
(B5) 647 650 634 24 642 648 643 6
(B6) 716 722 721 714 24 724 710 721 714 719 721 21
(B7) 700 692 691 21 681 696 692 684 24
(B8) 634 / 663 673 668 18 674 671 668 675 666 658

C. On page 170, there is a *Tabula* whose columns are somewhat confusingly laid out:

(C1) 673 663 665 665 671 659 633 23 664 663 673 668 18 668 667 664 658
(C2) 706 725 714 24 717 709 19 722 707 721 708 18
(C3) 668 675 674 671 21 671 667 664 24 669 660 663 659 671 664
(C4) 710 717 723 718 708 721 714 24 715 717 708 18 722 717 710 20 0
(C5) 672 667 660 20 668 675 674 24
(C6) 640 642 633 23 647 642 635
(C7) 707 714 722 12 709 721 718 72
(C8) 697 692 684 24 700 691 691 696 684
(C9) 694 696 699 696 689 19 679 682
(C10) 675 666 659 19 672 657
(C11) 639 632 634 633 23 632 636 635 646
(C12) 724 717 17 722 717 710
(C13) 634 646 635 646
(C14) 718 725
(C15) 693
(C16) 681

D. On page 171 there is an elaborate chart, *Motus Planetarum purus*, with six columns, the first three of which look like the other presumed cipher data, and last three of which look like a reprise of the Preface Table.

(D1) 649 635 646 639 644 646 635 12 647 642 634 24 649 635 642 646 645 645 634 24 / 542 534 533 23 546 542 539 19

(D2) 549 538 534 546 535 25 / 427 450 441 444 24 432 439 447 17 446 442 439 20 0 / 347 342 346 349 19 343 332 346

(D3) 333 23 347 342 348 343 / 245 232 235 25 246 240 246 18 246 235 / 131 142 135 133 23 147 142 148 143 23 150 139

E. On page 176, a *Tabula*,

(E1) 640 642 634 646 635 646

(E2) 635 646 25 640 646 642

(E3) 22 647 646 632 634 12

(E4) 25 3 2 1 4 1 5

(E5) 634 646 648 632 639 647

(E6) 632 23 640 650 644 639

(E7) 632 640 24 647 638 639

(E8) 632 640 633 632 632 640

(E9) 650 640 646 639 650 626

F. Page 179, an unnamed table:

(F1) 669 675 654 675 25 670

(F2) 660 671 661 657 671 664

(F3) 634 24 666 667 674 667

(F4) 673 663 659 23 672 657

(F5) 655 667 658 18 673 675

(F6) 660 651 675 69 663 23

(F7) 658 660 667 657 665 662

(F8) 668 663 659 556 653 652

G. On the last page of the book, p. 180, another unnamed table:

(G1) 694 700 679 700 24 695

(G2) 685 696 686 682 696 689

(G3) 684 12 691 692 699 692

(G4) 698 688 684 24 697 682

(G5) 685 676 700 694 688 18
(G6) 680 692 683 23 698 700
(G7) 683 685 692 682 690 687
(G8) 693 688 684 24 0 677

BIOGRAPHICAL SKETCH

Jim Reeds was born in 1947 and received an education in mathematics (Michigan AB, 1970, Brandeis MA, 1972) and statistics (Harvard PhD, 1976). He has been interested in cryptology since childhood. He first became aware of the continuing *Steganographia* controversy after reading Walker's and Yates's books in the early 1970s, but beyond making a fruitless attempt to solve the Heidel cryptograms four years ago, did nothing about it until this spring. Jim works in the Information Sciences Research Center of AT&T Labs, occasionally on cryptographic problems.