

# APPENDIX A

## Bibliography

- Giovanni Tritemio, “*Clavis Steganographiae*”, Firenze 1982; italian translation by Aurora Duprè.
- Giovanni Tritemio, “*Steganografia*”, Firenze 1982; italian translation by Fabrizio Benedetti.
- Johanne Trithemio, “*Steganographia*”, Frankfurt 1606; published by Mattia Becker.
- Jim Reeds, “*Solved: The Ciphers in Book III of Trithemius's Steganographia*”, 1998.
- Gustavus Selenus, “*Cryptomenytices*”, 1624; english translation from latin by Dr. John William Henry Walden.

## Note on the Edition

This annotated edition is based on the HTML edition by Joseph H. Peterson (1997) based on the Darmstadt 1621 edition.

The decryption of codes and messages are illustrated following the book by Selenius which used:

- Frankfurt 1606 edition;
- a manuscript in his "*possession, which was copied in 1520 from a very old copy belonging to Johann Von Woesbroech, Manager of the Custom-house at Brieg*".

Selenius text has been checked by Walden which gives:

- as marginal references the pages of Selenius's quotation from Frankfurt 1606;
- as note, the differences with Darmstadt edition.

# APPENDIX B

## Cryptosystems Summary

### LIBER PRIMUS

- 1) **Pamersiel**: I have made use of the following precaution: the initial letters of the successive words, when read in order, produce for you the secret meaning. - Take the first letter of each word.
- 2) **Padiel**: The first letter of the first word and the third word; and let him say the rest in like fashion. - Let him take the first letters alternately.
- 3) **Camuel**: The first is idle alternately: that is, alternate words, beginning with the first word, are idle. - Idle words include the significant word.
- 4) **Asiel**: After one idle, two are valid. - One is idle, two solve.
- 5) **Barmiel**: One being idle, two are valid for the secret; it closes with an idle. - After one idle, two are valid; the last not.
- 6) **Gediel**: Always after two idle words, two solve. - After two, take two.
- 7) **Asiriel**: After two, two, and one is completed by one. - After two, two are valid, and one after one.
- 8) **Maseriel**: Three being idle, three are valid, and so through the whole. - After three, three are valid.
- 9) **Malgaras**: Three after three, two are completed by two, one is completed by one. - After three, three are valid, after two, two, and one after one; i.e. after two valid, two are idle, etc.
- 10) **Dorothiel**: Four are idle, and then four are valid. - After four, take four throughout.
- 11) **Usiel**: Before twice two, the like number; before three, the like number; before two, two; and before one, one is idle; i.e. before twice two idle, the like number are valid, etc. - As is said above, so be it done.
- 12) **Cabariel**: After five, five are valid. - Do as is said above.
- 13) **Raysiel**: Five after five, four after four, three after three, two after two, one after one is idle. - Do thus, as I have said above.
- 14) **Symiel**: Between two idle, stands the meaning of the secret. - As I have said, so do.
- 15) **Armadiel**: From one to eight, as many are idle as are valid, and again through the same the descent is made. - Do as I have shown you above.
- 16) **Baruchas**: It begins with an idle, as the preceding with a significant. - One being idle, afterwards valid and idle alike.
- 17) **Carnesiel**: The first line is all idle; in the other lines, between two idle, three are valid. - After the first line, before three one is idle.
- 18) **Caspiel**: Two lines are idle; afterwards, between two, twice two signify. - As had been said, so do, that there be two lines idle.
- 19) **Amenadiel**: After three lines, between three idle, five solve, or "are significant". - As I have said, so do.
- 20) **Demoriel**: After four lines and four words, six are valid. - As has been said above, so do.
- 21) **Geradiel**: Take the second; after that, the first; then the fourth; then the third; then the sixth; then the fifth; and so on. - As has been said, so be it done.
- 22) **Buriel**: Begin at the end, and there the first being idle, it is solved alternately. - Begin at the end, as has been said.
- 23) **Hydriel**: After one idle from the end, two are valid backward. - After one, two are valid from the end.
- 24) **Pyrichiel**: At first, the first alternately from the end; afterwards another towards the beginning. - As has been said, so be it done.
- 25) **Emoniel**: After one idle, two are valid backward. - Do in that way, as has been said.
- 26) **Icosiel**: After one idle. Three are valid from the end. - As has been said above, so do.

- 27) **Soleviel**: From the end two are idle, two are valid; the valid being filled out, the non-significant also are valid. - As has been said, so do.
- 28) **Menadiel**: From the end three times the trip is made, always by jumping two, to the beginning. - As has been said, so be it done.
- 29) **Macariel**: In the first order, the fourth; after that, the third; after that, the second; after that goes the first, from the end. - As has been said above, so do.
- 30) **Uriel**: From the end and to the beginning: always so, the first is idle, the second, valid. - Do as has been said above.
- 31) **Bydiel**: From the beginning two are idle and two are valid; afterwards, the others also are valid. - Two are valid alternately throughout.

## LIBER SECUNDUS

- 1) **Samael**: For each letter take the next following. - None is idle, all are valid.
- 2) **Anael**: The third letter is first, and after one idle one is valid. - The second is valid alternately.
- 3) **Vequaniel**: The fourth is the first in the alphabet. - After two, two are valid.
- 4) **Vathmiel**: The fifth is the first; so further. - After one, one is valid.
- 5) **Sasquiel**: The sixth is now the first, and all are valid. - None is idle.
- 6) **Samiel**: The seventh letter is the first. - All are valid.
- 7) **Barquiel**: The eighth letter is the first. - One is idle, the next valid.
- 8) **Osmadael**: The ninth letter is here the first. - After one idle, one is valid.
- 9) **Quabriel**: The tenth is taken for the first. - Alternately the first is idle.
- 10) **Oriel**: The eleventh is now the first. - The first is idle alternately.
- 11) **Bariel**: Now the eleventh letter is the first. - They are valid alternately.
- 12) **Berathiel**: The thirteenth is the first here. - One after the other.
- 13) **Sabrathan**: The fourteenth is the first in the alphabet. - One is idle alternately.
- 14) **Tartys**: Here the fifteenth is the first. - Alternately as above.
- 15) **Serquanich**: The sixteenth letter is the first. - Alternately one is idle.
- 16) **Jefischa**: The seventeenth is the first letter of the alphabet. - The first is idle alternately.
- 17) **Abasdarhon**: The eighteenth letter of the alphabet is the first. - Alternately as above.
- 18) **Zaazenach**: The nineteenth letter is now the first. - One after the other, as before.
- 19) **Mendrion**: The twentieth letter of the alphabet is now the first. - One after the other, as above.
- 20) **Narconiel**: The next to the last letter is now the first in the alphabet. - Alternately, as before.
- 21) **Pamiel**: Now the last letter of the alphabet is the first. - The first is idle, as in the others.
- 22) **Jasguarim**: The first three and the last three lines are idle; then the first syllable of each word, alternately, is idle, the first syllable of every other word solving. - Three lines are idle before and after.
- 23) **Dardariel**: At the beginning and at the end three lines are idle; in the other lines, note the second and the next to the last words; for they give the sense.
- 24) **Sarandiel**: Begin from the end, after the manner of the preceding chapter.

# APPENDIX C

## A Mathematical Approach

Assuming that the secret is hidden in the text with a sequence  $xyxyxy$ , where  $x$  is the number of the idle words and  $y$  is the number of the valid ones, we can enumerate all the words with the integer  $i$  (from  $1$  to  $n$ ).

The valid words are so chosen with the following formula

$$\text{hidden} = i + x \cdot \left\lceil \frac{i + (y-1)}{y} \right\rceil \quad [1]$$

For example, if the text is in the form  $xxxYYYYYxxxYYYYY\dots$ , we have

$$x = 3$$

$$y = 5$$

and so, the formula 1 above become

$$\text{hidden} = i + 3 \cdot \left\lceil \frac{i + 4}{5} \right\rceil$$

and the number of the valid words is so determined:

i	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	...
hidden	04	05	06	07	08	12	13	14	15	16	20	21	22	23	24	...

As a particular case, if we have  $x=y$ , we can assume

$$\text{hidden} = 2 \cdot i + (x-i) \bmod(x) \quad [2]$$

For example, if the text is in the form  $xxxYYYxxxYYY\dots$ , we have

$$x = y = 3$$

and so, the formula 2 above become

$$\text{hidden} = 2 \cdot i + (-i) \bmod(3)$$

and the number of the valid words is so determined:

i	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	...
hidden	04	05	06	10	11	12	16	17	18	22	23	24	28	29	30	...

# INDEX

STEGANOGRAPHIA .....	7
Introduction .....	8
LIBER PRIMUS .....	9
Notes .....	10
Cap. I - Pamersiel .....	14
Cap. II - Padiel .....	19
Cap. III - Camuel .....	22
Cap. IV - Asieliel .....	25
Cap. V - Barmiel .....	27
Cap. VI - Gediel .....	30
Cap. VII - Asiriel .....	32
Cap. VIII - Maseriel .....	35
Cap. IX - Malgaras .....	38
Cap. X - Dorothiel .....	41
Cap. XI - Usiel .....	43
Cap. XII - Cabariel .....	46
Cap. XIII - Raysiel .....	48
Cap. XIV - Symiel .....	51
Cap. XV - Armadiel .....	53
Cap. XVI - Baruchas .....	55
Cap. XVII - Carnesiel .....	57
Cap. XVIII - Caspiel .....	60
Cap. XIX - Amenadiel .....	62
Cap. XX - Demoriel .....	64
Cap. XXI - Geradiel .....	66
Cap. XXII - Buriel .....	68
Cap. XXIII - Hydriel .....	70
Cap. XXIV - Pyrichiel .....	72
Cap. XXV - Emoniel .....	74
Cap. XXVI - Icosiel .....	76
Cap. XXVII - Soleviel .....	78
Cap. XXVIII - Menadiel .....	80
Cap. XXIX - Macariel .....	82
Cap. XXX - Uriel .....	84
Cap. XXXI - Bydiel .....	86
Cap. XXXII .....	88
LIBER SECUNDUS .....	91
Notes .....	92
Cap. I - Samael .....	93
Cap. II - Anael .....	95
Cap. III - Vequaniel .....	97
Cap. IV - Vathmiel .....	99
Cap. V - Sasquiel .....	101
Cap. VI - Samiel .....	103
Cap. VII - Barquiel .....	105
Cap. VIII - Osmadael .....	107
Cap. IX - Quabriel .....	109
Cap. X - Oriel .....	111

Cap. XI - Bariel .....	113
Cap. XII - Berathiel .....	115
Cap. XIII - Sabrathan .....	117
Cap. XIV - Tartys .....	119
Cap. XV - Serquanich .....	121
Cap. XVI - Jefischa .....	123
Cap. XVII - Abasdarhon .....	125
Cap. XVIII - Zaazenach .....	127
Cap. XIX - Mendrion .....	129
Cap. XX - Narconiel .....	131
Cap. XXI - Pamiel .....	133
Cap. XXII - Jasguarim .....	135
Cap. XXIII - Dardariel .....	137
Cap. XXIV - Sarandiel .....	139
Cap. XXV .....	141
LIBER TERTIUS .....	143
Notes .....	146
Cap. I .....	147
Appendix A .....	160
Appendix B .....	161
Appendix C .....	163