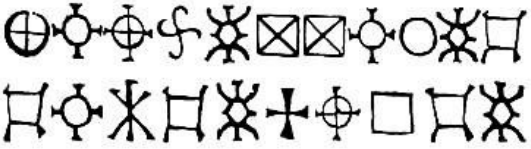
A Brief History of Period Substitution Ciphers and Their Operation



Lord Melchior zum grauen Wolf

Abstract

The science of encoding secret messages experienced a breakthrough in the mid-16th century. To that point the arts and sciences of writing secret messages had been either a closely kept knowledge or intertwined with works of engineering, math, or the occult. This paper reviews one of the most common forms of ciphers to be documented in period, the substitution cipher. Through the works of luminaries such as: Leon Battista Alberti (1467), Giovan Battista Bellaso (1553), Jean Baptiste Porta (1563), and Blaise de Vigenère (1583), we review the evolution the substitution cipher from a simple character based replacement scheme, n-graph or context replacement, and finally to what would come to be acknowledged as the zenith of medieval cryptographic achievement, the polyalphabetic cipher. This paper examines the evolution, strengths, and methods of period (pre 17th century) cryptographic systems. Finally, we present a new and novel cryptographic system based on the application of period techniques.[1]

Keywords: cryptology, cryptography, ciphers, math, boobies, medieval, science

[1] For those readers that are familiar with academic writing and the APA 6.0+ format: This document closely resembles, and is not entirely indifferent to, but is completely different from it. I have made a few modifications to the style to make it more accessible to the general reader. Please accept my apologies for any confusion, and for the time you have spent in academia. The struggle is real.

Substitution Ciphers

What they are and how they work

Substitution ciphers provide a simplistic mechanism for obfuscating messages where a given letter, word, or even a predetermined message, is replaced with another symbol. In the most basic form of this technique one letter is simple replaced with a different letter. Atbash is one of the earliest well documented examples of this technique being used and has been identified throughout period (600-1600 AD), to include being found in the old testament[2] (Singh, 1999). In its original form Atbash simply swapped the first letter of the alphabet with the last letter of the alphabet. This parity is the reason Atbash is sometimes referred to as a 'mirror cipher'[3]. This type of enciphering is known as a monoalphabetic as each character maps to exactly one other character.

---

[2] See Figure 1

[3] See Figure 2

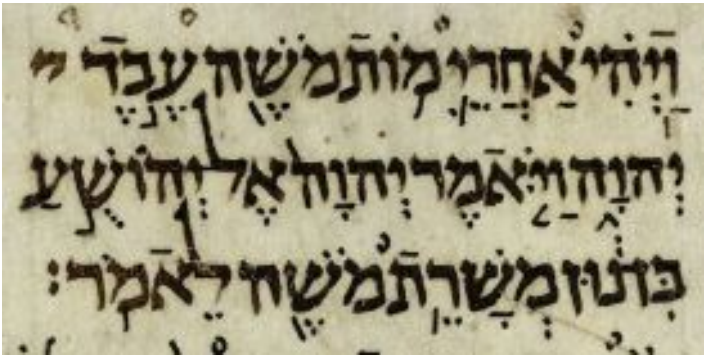


Figure 1: Atbash, a period example (Singh, 1999**)**

11	10	9	8	7	6	5	4	3	2	1
ל	י	ט	ח	ז	ו	ה	ד	ג	ב	א
12	13	14	15	16	17	18	19	20	21	22

Figure 2: Atbash, substitution key

Alphabets with an even number of characters, `a mod 2 = 0`, such as ancient Hebrew and modern English, are well suited to this type of transformation as all characters receive a cipher value. Asymmetric alphabets may also be employed but may require modifications such as padding or a known offset to be used in the same manner as Atbash. Consider a hypothetical

alphabet N consisting of any set of values amounting to `N mod 2 = 1`, for example `[a, b, c]`. Applying the Atbash pattern to such a set produces a cipher set as follows `N[a:=c, b:=b, c:=a]`. This is, obviously, less than optimal as the central character graph is not enciphered. The modern English alphabet, based on the classical Latin alphabet, shares the mod 2 characteristic therefore it will be used for the examples and calculations below.

While the Atbash example is simple to understand, this concept of encryption or decryption can be applied to any monoalphabetic system. The Affine ciphers, of which Atbash is an example of, are ones in which a given letter is mapped to its numeric equivalent to perform a transformation, encryption, based on known modifiers (Beutelspacher & Fisher, 1994). This approach to substitution provides a mathematically sound mechanism by which a known alphabet may be enciphered. Atbash adheres to this model as `n:=n-1, n+1:=n-2,` etc.

This makes it possible to use the known Affine encryption and decryption functions to describe Atbash in a way that is functional for extrapolation to other monoalphabetic systems. This direct substitution system, while simplistic, provides a generally accessible foundation by which other simplistic ciphers may be understood. All additive, or Caesar style (discussed in a later section), shifting cipher systems will use this basic approach to encryption and decryption (Beutelspacher & Fisher, 1994). The function we will use for this purpose is as follows: $E(x)=D(x)=((-x \bmod |N|)+1)$. You will immediately notice that the encryption and decryption functions are the same. These are simplistic examples but understanding the workings of these basic substitution ciphers is fundamental to understanding more advanced concepts such as polyalphabetic cipher systems. This mathematical technique is applied below to, for the purposes of demonstration, to introduce this science. Having laid this foundation we will then

explore, in more broad terms, other substation ciphers of note up to approximately 1600 C.E.

Assume N is a set of integers, starting with 1, which corresponds to the number of characters in the target alphabet.

$$E(x) = D(x) = ((-x \bmod |N|) + 1) \quad (1)$$

$$E(1) = ((-1 \bmod 26) + 1) \quad (2)$$

$$E(1) = (25 + 1) \quad (3)$$

$$N\{1\} = N\{26\} \quad (4)$$

$$a = z \quad (5)$$

$$D(26) = ((-26 \bmod 26) + 1) \quad (6)$$

$$D(26) = (0 + 1) \quad (7)$$

$$N\{26\} = N\{1\} \quad (8)$$

$$z = a \quad (9)$$

$$a = z \therefore z = a \quad (10)$$

A Brief History

Now that we have established the mathematical foundation for the operation of the basic substitution cipher we will examine the application of these techniques in period ciphers. Fortunately, many of the encipherment techniques discussed in period literature were clearly established prior to the first published works on ‘cryptography’, of the early 16th century. For example: Johannes Trithemius’s *Polygraphia* (1518), which is regarded as the first western publication dedicated to the topic of cryptography, or Jacopo Silvestri’s *Opus Novum* (1526) are not shy to refer to ‘ancient’ modes of encipherment. While it does require additional research to uncover the point of origin for many of these ciphers, if one can be clearly identified, the ubiquity of examples referenced in those early works firmly reestablishes a foundation upon which advances may be made.

By the mid 16th century cryptography had began to establish itself as field of science, separate from its often esoteric 'European roots'. Notable works of this time, namely Giovan Battista Bellaso's *La Cifra del Sig* (1553) and Girolamo Cardano's *Subtilitas de Subtilitate rerum* (1554) either expanded upon that foundation by employing more contemporary methods execution, such as Cardano's 'grilles'[4], or radically rethinking the encoding mechanisms themselves, as seen in Ballaso's breakthrough work on the auto-key (polyalphabetic) cipher (1553).

Blaise de Vigenère is credited with the invention of the auto-key cipher in 1586 because early researchers on the topic were LAZY. The auto-key encipherment approach was one of

[4] The Cardano Grille is not a substitution cipher but was very popular with the aristocracy for its simplicity. It also shows that a robust discussion about the most effective means of effective clandestine communication was underway in related circles of the time. Cryptography of the middle ages was a vast and open domain of exploration for the intellectuals of the day.

the most significant advancements in the field of cryptography in a thousand years possibly for another thousand years to come (Gaines, 1956). Vigenère's primary contribution to this advance was his popularization of the method (Smith, 1955). Basically the guy was good at marketing the idea and people were more receptive to its utility 30 years after Bellaso's first described it.

By the close of the 16th century numerous advances in the field of cryptography had been published. While advances such as the auto-key encipherment mechanism are generally known to modern scholars there were other advances in the field that were truly revolutionary for their time. An example of this can be seen in Francis Bacon's 1593 description of a 'bi-literal cipher'. Bacon was far from the first person to use alternate scripts to conceal messages. This technique was discussed, in considerable length, prior to the publication of *Polygraphia* (see Alberti, 1467; Aenaes, 450 BCE; and others).

However, Bacon's introduction of the use of bit space to define complexity and character space (or capacity) laid out the basis for binary mathematics a full hundred years before Leibniz 1703 'Explanation of Binary Arithmetic'. Bacon's system was complete to the point that he provided accurate binary summations for his bi-literal substitution system. It appears that Bacon's only fault in his reconing of this system is that he used 'a' and 'b' rather than '1' and '0' and presented the system as a means to calculating an enciphered message length rather than presenting it as a system of arithmetic.

Substitution Ciphers in Operation

Now that we have established the basic working of substitution ciphers, and provided a historical context for their study, we will review a selection of substitution ciphers taken directly from primary sources. The examples shown here are taken, for the most part, from works dedicated to cryptography, to ensure that created our sampling is not polluted with material of questionable origin or utility. There are certain images where I have chosen to use a modern reproduction for clarity but citation is provided so that you may, if you were so inclined, go directly back to the primary source material. Sound you choose to investigate these sources in further detail then I humbly offer this advice: “Brush up on your latin first”.

The simplest form which a substitution cipher may take is that of ‘direct substitution’ (Kahn, 1996). A direct substitution cipher is one in which one element is replaced for

another, one for one. This can take numerous forms, for example: letter for letter (a = t), symbol for letter (a = □), character/number/symbol for di or tri-graph (th = R, ing = 5), word/phrase/pattern for letters or sets of letters (a = zig), etc. In *Polygraphia*, Trithemius commits the overwhelming majority, more than 450 pages of the 520 pages of content, of his manual to documenting many hundreds of variations on this theme.

Some of these, as shown below in figure 3, are fairly straight forward. In this case we see the application of a rotational pattern to achieve the desired encryption or decryption operation. This, as in most cases, relies on a ‘pre-shared key. Trithemius discusses several ways to communicate this information within the cipher and the options really are endless. Examples include simply pre-arranging the key, using the first capitalized letter of the enciphered text, including the key in some other prearranged location or format, etc.

Using this ‘Recta Transpositionis Tablua’ we can encode the message ATLANTIA with the key ‘O’ by moving down the O column until we encounter the letter A, which corresponds to the letter L (which is found by moving horizontally along the row). Using the example ATLANTIA = LEULZETL. While these cipher methods are simple to use, and will provide a degree of confidentiality against the casual observer, they do suffer from two major flaws. These flaws relate to the most essential features of what constitutes a ‘good’ secret language. First, direct letter substitution ciphers are obvious in that they ‘are’ trying to avoid disclosing information. A casual observer may not be able to tell what the contents of the message are but they know that you don’t want to share, that is to say: they are not clandestine. Secondly, the ciphers are subject to the most rudimentary form of attacks, namely frequency analysis.

Figures 4 and 5 are also taken from Polygraphia and provide examples of how whole word substitution systems may be employed in a one to one substitution..

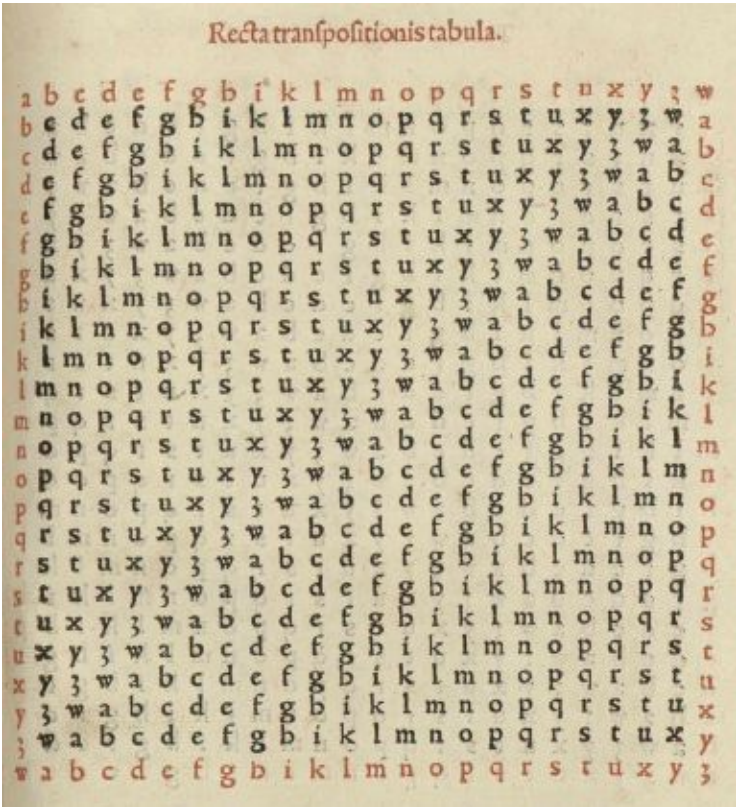


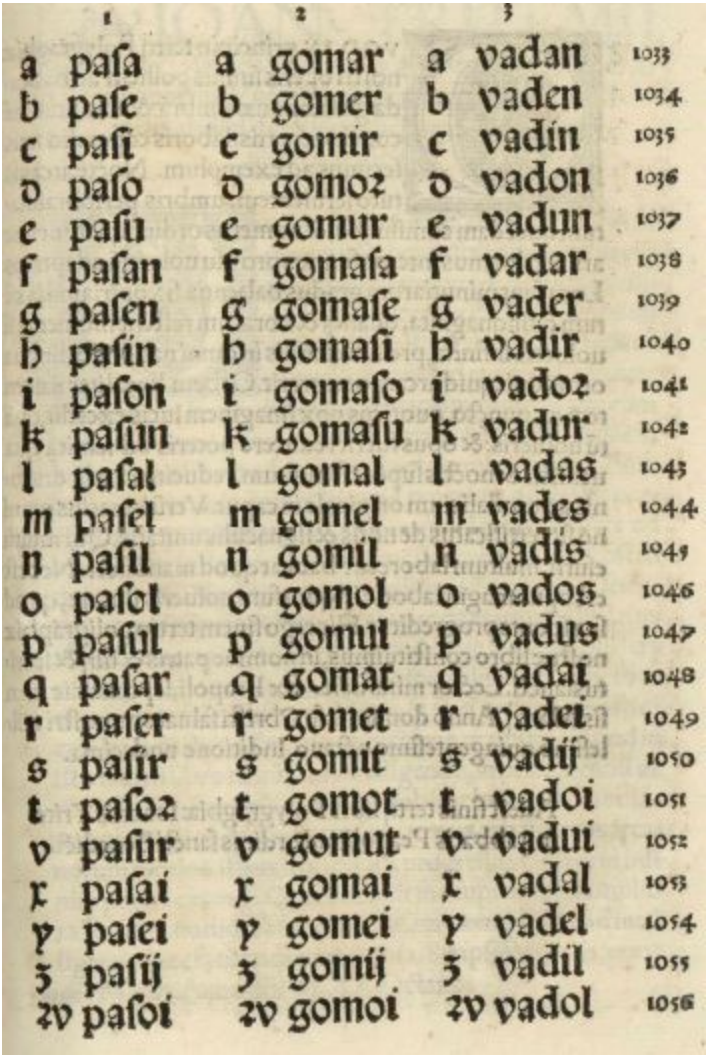
Figure 3. (Trithemius, 1518)


a Deus
b Creator
c Conditor
d Opifex
e Dominus
f Dominator
g Conſolator
h Arbiter
i Judex
k Illuminator
l Illuſtrator
m Rector
n Rex
o Imperator
p Gubernator
q Factor
r Fabricator
ſ Conſeruator
t Redemptor
v Auctor
x Princeps
y Paſtor
z Moderator
zv Saluator

a clemens
b clementiſſimus
c pius
d piiſſimus
e magnus
f excelſus
g maximus
h optimus
i ſapientiſſimus
k inuiſibilis
l immortalis
m eternus
n ſempiternus
o glorioſus
p fortiſſimus
q ſanctiſſimus
r incõprehenſibilis
ſ omnipotens
t pacificus
v miſericors
x miſericordiſſimus
y cunctipotens
z magnificus
zv excellentiſſimus

A

Figure 4. (Trithemius, 1518)



1	2	3	
a pasa	a gomar	a vadan	1033
b pase	b gomer	b vaden	1034
c pasi	c gomir	c vadin	1035
d paso	d gomoz	d vadon	1036
e pasu	e gomur	e vadun	1037
f pasan	f gomasa	f vadar	1038
g pasen	g gomase	g vader	1039
h pasin	h gomasi	h vadir	1040
i pason	i gomaso	i vadoz	1041
k pasun	k gomasu	k vadur	1042
l pasal	l gomal	l vadas	1043
m pasel	m gomel	m vades	1044
n pasil	n gomil	n vadis	1045
o pasol	o gomol	o vados	1046
p pasul	p gomul	p vadus	1047
q pasar	q gomat	q vadai	1048
r paser	r gomet	r vadei	1049
s pasir	s gomit	s vadij	1050
t pasoz	t gomot	t vadoi	1051
v pasur	v gomut	v vadui	1052
x pasai	x gomai	x vadal	1053
y pasei	y gomei	y vadel	1054
z pasij	z gomij	z vadil	1055
zv pasoi	zv gomoi	zv vadol	1056

Figure 5. (Trithemius, 1518)

One of, if not the, most famous ciphers documented of the middle ages is that uses by Mary Queen of Scots during the Babbington Rebelion of 1583 (Smith, 1943). The history behind this particular cipher is both well documented and terrifically fascinating. It is a topic on which many books have been written, and rightfully so.

This cipher captures the imagination for a constellation of reasons, not least of which is its historical significance. The cipher symbols are esoteric and yet familiar. The use of intermixed letter and word substitutions was not entirely novel but together with intermixed nulls and syntaticall markers such as for the dowbleth (double letters, the ‘tt’ in letters - for example) we see a system of substitution which was making use of a wide variety of techniques. The cipher’s key may be seen in figure 6.

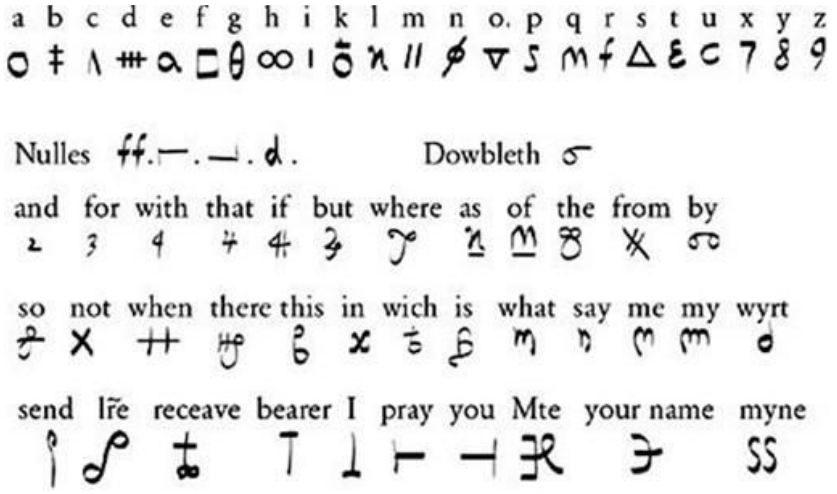

a b c d e f g h i k l m n o. p q r s t u x y z
Nulles
Dowbleth
and for with that if but where as of the from by
so not when there this in wich is what say me my wyrt
send lr̃e receave bearer I pray you Mte your name myne

Figure 6

Giovanni Battista Della Porta published two books which were committed to the science of cryptography. *De Furtivia Literarum Notis* in 1561 and *De Occultus Literarum Notic* in 1593. Both of which were sufficiently popular to warrant several printings. While the work stood on its own, Porta's highly accurate frequency analysis tables made him something of a celebrity among mathematicians and cryptographers of his day, as pointed out by Fletcher Pratt in Secret & Urgent. His work was also exhaustive its documentation of extant cryptographic systems (Kahn, 1996).

A complete description of the ciphers documented by Porta would be far beyond the scope of this minor introduction to medieval cryptography so I have elected to investigate one of these ciphers, which builds logically on those we have already discussed. An appendix is provided with selection of various encryption methods take from the source material, with short descriptions, for your review.

LITERÆ SCRIPTI

LITERÆ CLAVIS

AB	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	s	t	v	x	y	z
CD	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	s	t	v	x	y
EF	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	s	t	v	x
GH	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	v
IL	a	b	c	d	e	f	g	h	i	l	m
	v	x	y	z	n	o	p	q	r	s	t
MN	a	b	c	d	e	f	g	h	i	l	m
	t	v	x	y	z	n	o	p	q	r	s
OP	a	b	c	d	e	f	g	h	i	l	m
	s	t	v	x	y	z	n	o	p	q	r
QR	a	b	c	d	e	f	g	h	i	l	m
	r	s	t	v	x	y	z	n	o	p	q
ST	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	v	x	y	z	n	o	p
VX	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	v	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	v	x	y	z	n

In

Figure 7 (Porta, 1593)

In figure 7 we see a scheme where the key, '*literae clavis'*, is used to define which substitution alphabets are to be utilized in the coding process. This method can be used for both mono and polyalphabetic substitutions. For example: Using a key of **M** can encode the message "Atlantia" as "TARTFAQT. As you can see, we simply using the single key to select the substitution set to use, as in previously discussed ciphers. However, if we define a complex key, such as 'SEA' then we introduce the potential of polyalphabetic substitution that is almost guaranteed for messages of any substantial length. The key, which identifies which encoding system to use is repeated along the length of the entire message. Continuing the previous example:

A T L A N T I A ← Plain text
S E A S E A **S E** ← Key
Q I Y Q C Q N Y ← Encoded message.

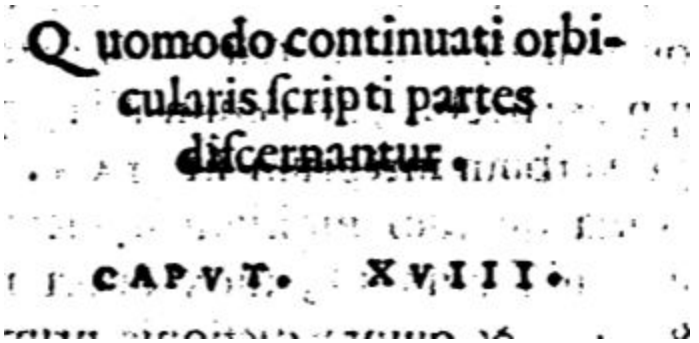
Notice that Q is used for the first two instance of the letter A but not the last, which is encoded to Y. However, the letter Q is also used for the second instance of T, while the first is encoded to I. Decoding the message is accomplished through the same process but in reverse.

Q I Y Q C Q N Y ← Encoded message.
S E A S E A **S E** ← Key
A T L A N T I A ← Plain text

Conclusion

Thank you for your interest in historic cryptography. In this short introduction to substitution ciphers we have shown there basic operation and the mathematical concepts which underpin the processes of encryption and decryption, a brief history of, published, western cryptography was presented, and finally a cross section of substitution ciphers was reviewed to show how period ciphers, taken directly from primary sources may be utilized.

Appendix



Q uomodo continuati orbicularis ſcripti partes diſcernantur.

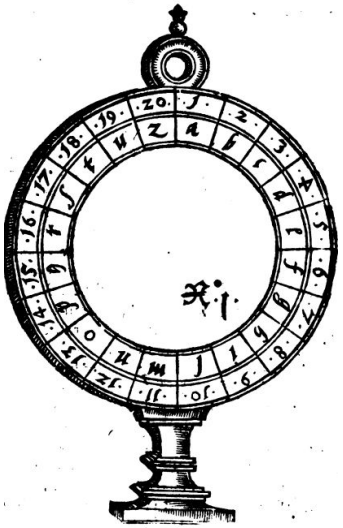
CAPVT. XVIII.

(Porta, 1593) “Bi-literal” cipher example

ordines.

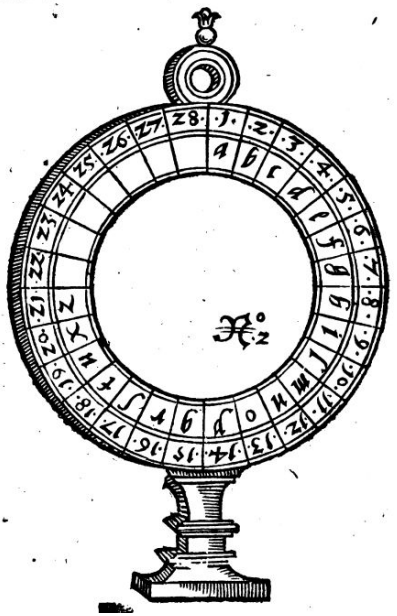
numeri ordinum	1	2	3	4
1	a	f	m	r
2	b	g	n	s
3	c	h	o	t
4	d	i	p	u
5	e	l	q	z

(Porta, 1593) page 42

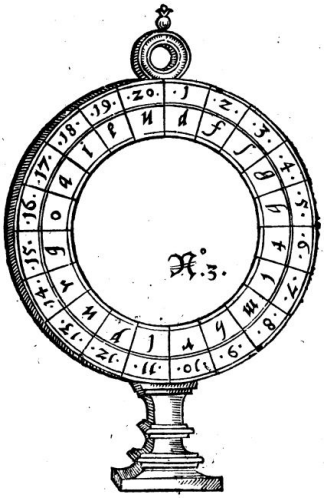


CAPVT VIII.
Quaratione ad ſcribendum inſtrumento vti poſſumus.

Page 91



Page 98



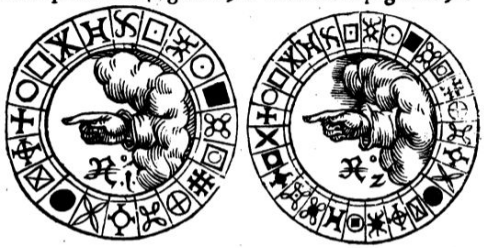
CAPVT. XI.
Eodem Rotæ artificio quomodo aliter literis per tabulam expanſis vti poſſimus.

Page 102

NOTA.

Quoniam harum figurarum formæ Typographo non fuerunt in tempore reddite, inter excudendum omiſſæ fuerant. Sed ne quid huic operi deeſſet, huc ſunt repoſitæ.

Prima pertinet ad paginam 92. Secunda ad paginam 98.



Tertia ad paginam 103.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z	a
	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z	a	b
	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z	a	b	c
	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z	a	b	c	d
	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z	a	b	c	d	e
	g	h	i	l	m	n	o	p	q	r	s	t	u	z	a	b	c	d	e	f
	h	i	l	m	n	o	p	q	r	s	t	u	z	a	b	c	d	e	f	g
	i	l	m	n	o	p	q	r	s	t	u	z	a	b	c	d	e	f	g	h
	l	m	n	o	p	q	r	s	t	u	z	a	b	c	d	e	f	g	h	i
	m	n	o	p	q	r	s	t	u	z	a	b	c	d	e	f	g	h	i	l
	n	o	p	q	r	s	t	u	z	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	u	z	a	b	c	d	e	f	g	h	i	l	m	n
	p	q	r	s	t	u	z	a	b	c	d	e	f	g	h	i	l	m	n	o
	q	r	s	t	u	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p
	r	s	t	u	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q
	s	t	u	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r
	t	u	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s
	u	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t
	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	v

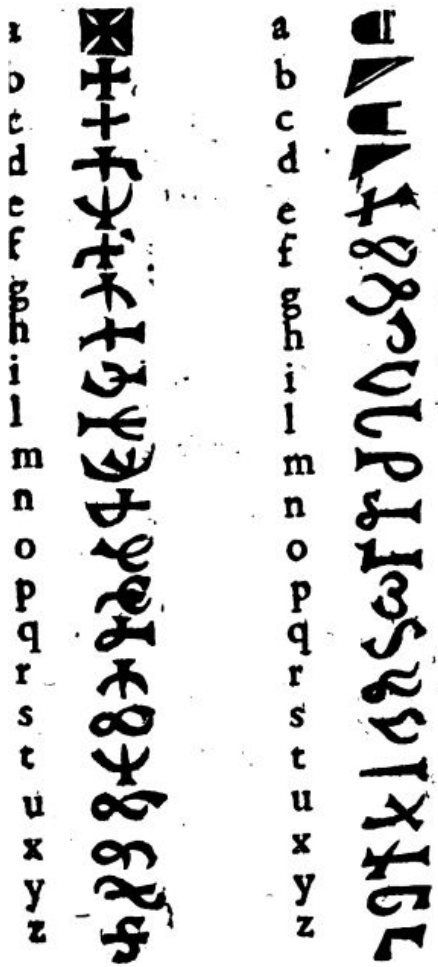
(Porta, 1593) Page 105

(Porta, 1593) Page 107, introduction of digraphs

(Porta, 1593) Page 116, character sub

60 different substitution alphabets are described.

Variatæ tabellæ per numerum literarum.



a Recepi
b Aſpexi
c Percepi
d Habui
e Nactus ſum
f Cognoui
g Concepi
h Perſpexi
i Intellexi
l Sumpſi
m Aſſumpſi
n Percurri
o Suſcepi
p Reſumpſi
q Proſpexi
r Vidi
s Accepi
t Perlegi
u Legi
x Reſpexi
y Conſpexi
z Noui

a literam

4	5	6
a literam	a dulcis	a et
b epiſtolas	b honorate	b atq; etiam
c ſyngraphas	c amate	c perinde ac
d paginam	d ſuauis	d &
e paginas	e lepide	e idemq;
f literulas	f humane	f ac etiam
g ſchædulam	g probe	g ac
h ſchædulas	h ſpectate	h atq;
i epiſtoliũ TVAM TVAS TVAM	i dilecte	i æque ac
l tabellam	l magnanime	l atq;
m ſcriptum	m iucunde	m que
n ſcriptum	n magnifice	n q;
o chyrographum	o ornate	o que
p chartas	p honeſte	p q;
q chartulam	q exculte	q q.
r chartam	r docte	r q.
s epiſtolam	s prudens	s &
t literas	t prouide	t atq;
u tabellulas	u ſincere	u & ſimul
x chartulas	x manſuete	x ſimul ac
y tabellas	y ingenioſe	y ac ſimul
z ſyngraphas	z optime	z ſimulet

a Illu-

31		32	33
a : :		a aliud	a remanens eſt
b .		b nouum negotiũ	b remanet
c ,		c quicquam nouũ	c reliquum eſt
d ;		d aliqua res	d relinquitur
e :.		e aliquid	e reſtat
f ..		f quæpiam	f reſidet
g ·:		g quicquam	g reſiduum eſt
h :		h aliud negotium	h reſidens eſt
i ..		i alia res	i ſupereſt
l ?		l nonnihil	l eſt præterea
m)	SI	m noua res	m vacat
n :: .		n quæ res	n eſt inſuper
o ,		o aliquid noui	o adiungitur
p ;		p quid	p ſuperat
q .		q quicquid	q adhuc extat
r :.		r aliquid nouum	r neceſſarium eſt
s .:		s quidpiam noui	s deſit præterea
t :		t agendum aliud	t deeſt etiam
u ..		u quidpiam	u ſuper extat
x ?		x negotiũ aliquod	x etiamnum deeſt
y ·		y aliquod negotiũ	y excedit
z)		z aliud officium	z ſuperadditur

a maiuſculis incipiendum

a iu-

52	53	54
a 1	a Iannuarij	a 1539
b 2	b Februarij	b 1540
c 3	c Martij	c 1541
d 4	d Aprilis	d 1542
e 5	e Iunij	e 1543
f 6	f Maij	f 1544
g 7	g Iulij	g 1560
h 8	h Auguſti	h 1546
i 9	i Septembris	i 1547
l 10	l Octobris	l 1568
m 11	m Nouembris	m 1549
n 12	n Decembris	n 1550
o 13	o Sextilis	o 1551
p 14	p Quintilis	p 1552
q 15	q Ianuar.	q 1553
r 16	r Februar.	r 1554
s 17	s Mart.	s 1555
t 18	t April.	t 1556
u 19	u Mai.	u 1557
x 20	x Iun.	x 1558
y 21	y Iul.	y 1559
z 22	z Aug.	z 1545

55

(Porta, 1593) Page 140, words replaced with symbols.

Primary Sources

Digital copies of all primary sources are available on request

Alberti (1467), *De Ciphera*

Bellaso (1553), *La Cifra del Sig*

Cardano (1554), *Subtilitas de Subtilitate rerum* (1554)

Porta (1563 edition), *De Furtivers Literarum Notis*

Porta (1598 edition), *De Occultis Literarum Notis*

Silvestri (1526), *Opus Novum*

Trithemius (1518 edition), *Polygraphia*

Secondary References

Commercially available but several are rare or VERY expensive. Contact the author of this paper if you are interested in reviewing any of the following.

Beutelspacher, A., & Fisher, J. C. (1994). Cryptology: An introduction to the art and science of enciphering, encrypting, concealing, hiding, and safeguarding described without any arcane skullduggery but not without cunning waggery for the delectation and instruction of the general public. Washington, DC: Mathematical Association of America.
(Beutelspacher & Fisher, 1994)

D'Agapeyeff, A. (2006). Codes and ciphers. S.I: Hesperides Press.
(D'Agapeyeff, 2006)

Ellison, K. (2017). A cultural history of modern English cryptography manuals. Abingdon, Oxon: Routledge, Taylor & Francis Group.

Gaines, H. F. (1956). Cryptanalysis; a study of ciphers and their solution. New York: Dover Publications.
(Gaines, 1956)

Kahn, D. (1996). The codebreakers: The story of secret writing. New York: Scribner.
(Kahn, 1996)

Smith, L. D. (1955). Cryptography: The science of secret writing. New York: Dover Publications.
(Smith, 1955)

Singh, S. (1999). The code book: The science of secrecy from ancient Egypt to quantum cryptography.
(Singh, 1999)