Nomenclators

Early code/cipher combination, popular form 1400s-1800s.

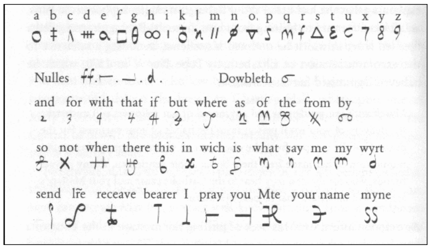
Philip of Spain (1589, see Kahn):

LO = Spain
POM = King of Spain
64 = confederation
overlined two-digit groups = null

+ substitution cipher with homophones

Nomenclator Example

Nomenclator used by Mary, Queen of Scots
in 1586 in the plot against Elizabeth I



a b c d e f g h i k l m n o p q r s t u x y z

Nulles ff. — . — . d .   Dowbleth σ

and for with that if but where as of the from by

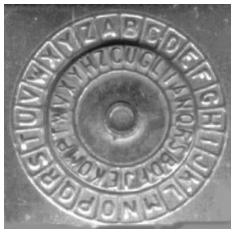
so not when there this in wich is what say me my wyrt

send lre receave bearer I pray you Mte your name myne

Taken from Simon Singh. The Code Book.

Alberti's Cipher Disk

Invented by Leon Battista Alberti in 1460s.



Correspondents agree on index letter on inner disk.
Key: corresponding letter on outer disk.
Key can change during encryption

Cipher Disk Examples

Let’s choose “k” as the index letter.

↓

Examples:

pOIDDEXEMDL
bQVPAPAEUMKEOHEWEU
vJUHaNYQTiQWBsGYRR

Since the key can change, this cipher is no longer monoalphabetic, but polyalphabetic.

Are there other ways to use the cipher disk?

Johannes Trithemius

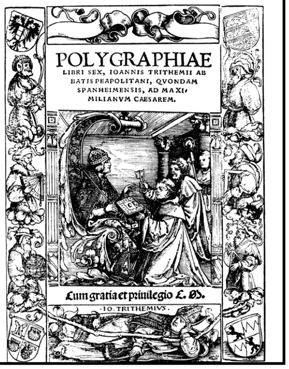
1462-1516, Germany

Polygraphiae, 1518
First printed book on cryptography.

- Ave Maria Cipher
- Polyalphabetic substitution
- Progressive key

Steganographia, 1606

- hidden writing



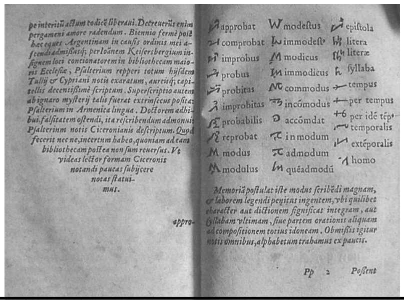
POLYGRAPHIAE
LIBRI SEX, IOANNIS TRITHEMII AB
BATIS PEAPOLITANI, QVONDAM
SPANHEIMENSIS, AD MAXI-
MILIANVM CAESAREM.

Cum gratia et privilegio C. M.

IO. TRITHEMIVS.

Polygraphiae I

The *Polygraphiae* contains many pages of code.



pe interitū actum codicē liberaui. Decreuerūt enim pergameni amore radendum. Biennio fermè poſt hæc eques Argentinam in cauſis ordinis mei aſcendi admiſſusq; per Ioānem Keiſersbergium inſignem loci concionatorem in bibliothecam maioris Eccleſiæ, Pſalterium repperi totum hijſdem Tullij & Cypriani notis exaratum, aureisq; capitellis decentiſſimè ſcriptum. Superſcriptio autem ab ignaro myſterij talis fuerat extrinſecus poſita: Pſalterium in Armenica lingua. Doctorem adhibui, falſitatem oſtendi, ita reſcribendum admonui: Pſalterinm notis Ciceronianis deſcriptum. Quod fecerit nec ne, incertnm habeo, quoniam ad eam bibliothecam poſtea non ſum reuerſus. Vt videas lector formam Ciceronis notandi paucas ſubijcere notas ſtatuimus.

appro-

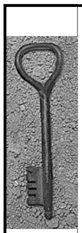
approbat
comprobat
improbus
probus
probitas
improbitas
probabilis
reprobat
modus
modulus

modeſtus
immodeſtè
modicus
immodicus
commodus
incōmodus
accōmdat
in modum
admodum
quēadmodū

epiſtola
litera
literæ
ſyllaba
tempus
per tempus
per idē tēp•
temporalis
extēporalis
homo

Memoriā poſtulat iſte modus ſcribēdi magnam, & laborem legendi penitus ingentem, vbi quilibet character aut dictionem ſignificat integram, aut ſyllabam vltimam, ſiue partem orationis aliquam ad compoſitionem totius idoneam. Obmiſſis igitur notis omnibus, alphabetum trahamus ex paucis.

Pp 2 Poſſent

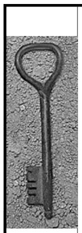


Polygraphiae II

Ave Maria Cipher

a	deus	a	clemens
b	creator	b	clementissimus
c	conditor	c	pius
d	opisex	d	pijssimus
e	dominus	e	magnus
f	dominator	f	excelsus
g	consolator	g	maximus
h	arbiter	h	optimus

1st page of Ave Maria Cipher, taken from the first book of the Polygraphiae



Steganographia

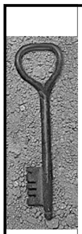
Begun in 1499; published posthumously in 1606

```
Parmesiel Oshurmi Delmuson Thafloin
          s u m          t a l i

Peano Charustrea Melany Lyamunto
     c a u t e       l a u t
```

Placed on Index Librorum Prohibitorum in 1609

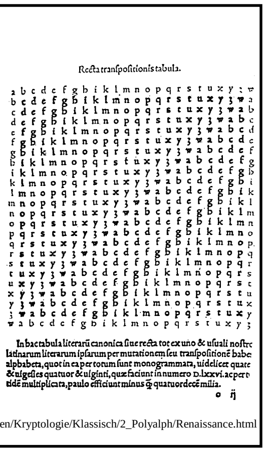
“full of peril and superstition (M. A. Del Rio)



Polygraphiae III

Tabula recta, from the 6th book of the Polygraphiae.

•Polyalphabetic substitution
•Progressive key



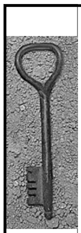
Recta tranſpoſitionis tabula.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e
g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f
h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g
i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i
l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k
m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l
n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m
o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n
p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o
q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
r	s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
s	t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
t	u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
u	x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
x	y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
y	ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
ʒ	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y
w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ

In hac tabula literarũ canonica ſiue recta tot ex uno & uſuali noſtre
latinarum literarum ipſarum per mutationem ſeu tranſpoſitionẽ habe
alphabeta, quot in ea per totum ſunt monogrammata, uidelicet quate
& uigeſies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac per
tidẽ multiplicata, paulo efficiunt minus ꝙ quatuordecẽ milia.

o ij

http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/2_Polyalph/Renaissance.html



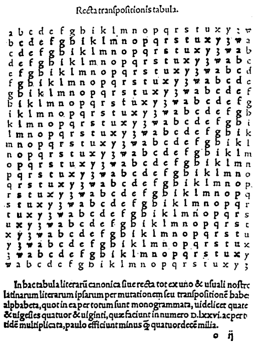
Polygraphiae IV

Examples (starting with first alphabet)

- hunc caveto virum
- Johannes
- SUGKCSUOAKATXO

More Examples

- TNOEZR
- BDF



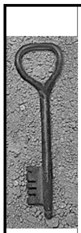
Recta tranſpoſitionis tabula.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e
g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f
h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g
i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i
l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k
m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l
n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m
o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n
p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o
q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y
w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z

In hac tabula literarũ canonica ſiue recta tot ex uno & uſuali noſtre
latinarum literarum ipſarum per mutationem ſeu tranſpoſitionē habe
alphabeta, quot in ea per totum ſunt monogrammata, uidelicet quate
& uigeſies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac per t
tidē multiplicata, paulo efficiunt minus q̃ quatuordecē milia.

o ij

http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/2_Polyalph/Renaissance.html



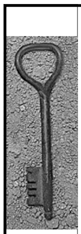
Giovan Batista Belaso

La cifra del. Sig. Giovan Batista Belaso, 1553

Idea: combine polyalphabeticity with keyword; that is, select cipher alphabet according to keyword

key	`viavia viaviav iaviav`
plaintext	`giovan batista belaso`
ciphertext	`bqoqin witdatv jegisj`

Only used standard alphabets (abcd...xyz)



Giovan Batista Belaso

La cifra del. Sig. Giovan Batista Belaso, 1553

key	`viavia viaviav iaviav`
plaintext	`giovan batista belaso`
ciphertext	`bqoqin witdatv jegisj`

Examples

plaintext: message, key: help
ciphertext: ZINGLXXTZWLVL, key: help

Giovanni Battista Porta I

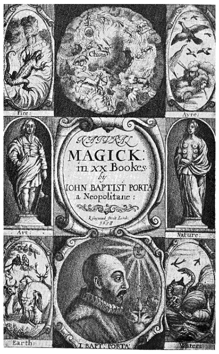
1535-1615, Naples

Founded the first scientific society, Academia Secretorum Naturae

Magia naturalis, 1558

Book 16
Of Invisible Writing

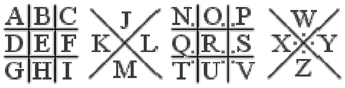
- invisible inks
- hiding messages



Giovanni Battista Porta II

De Furtivis Literarum Notis, 1563

- criticizes traditional ciphers (Rosicrucian cipher)
- Substitution/Transposition
- Digraphic Substitution
- symbol substitution
- Mixed polyalphabetic cipher



Freemason’s cipher (similar to Rosicrucian cipher)

De Furtivis I

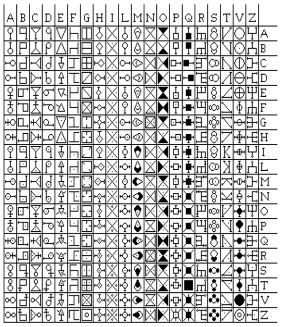
Classification of ciphers according to method:

- Transposition
- Substitution by symbol
- Substitution by value

Suggests deliberate mistakes in plaintext to confuse cryptanalyst.

Suggests probable word analysis

De Furtivis II


A B C D E F G H I L M N O P Q R S T V Z
A B C D E F G H I L M N O P Q R S T V Z

Earliest known Digraphic Substitution

Symbol substitution

De Furtivis III

Mixed polyalphabetic cipher

Combining Alberti's mixed alphabet with Trithemius/Belaso's tabula recta

First ideas for cryptanalysis of mixed polyalphabetic ciphers

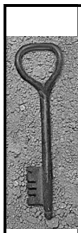
De Furtivis IV

Cryptanalysis of mixed polyalphabetic cipher

What happens to "def", "stu" in a progressive polyalphabetic cipher?

Observation on a polyalphabetic cipher with literal key:

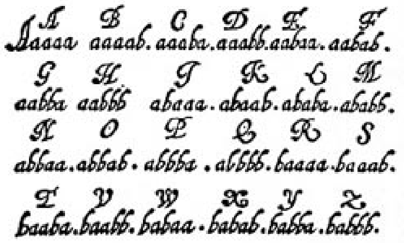
> "Since there are 51 letters between the first MMM and the same three letters repeated in the thirteenth word, I conclude that the key has been given three times and decide correctly that it has 17 letters."



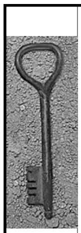
Bacon’s Biliteral cipher I

1561-1626, England

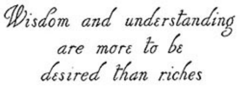
First idea: encode letters in binary (1623)



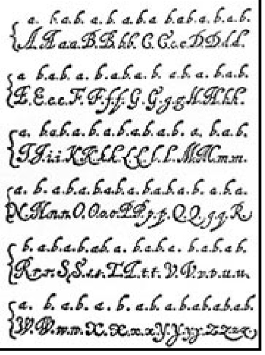
A	B	C	D	E	F
aaaaa	aaaab	aaaba	aaabb	aabaa	aabab
G	H	I	K	L	M
aabba	aabbb	abaaa	abaab	ababa	ababb
N	O	P	Q	R	S
abbaa	abbab	abbba	abbbb	baaaa	baaab
T	V	W	X	Y	Z
baaba	baabb	babaa	babab	babba	babbb



Bacon’s Biliteral cipher II

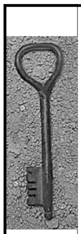


Wisdom and understanding
are more to be
desired than riches



Second idea: use two different typefaces to encode a/b decision.

Example:
To be *o*r not to be *th*a*t* *i*s *th*e *q*uestion.



Girolamo Cardano

De Subtilitate, 1550; De Rerum Varietate, 1556

Autokeys:

```
key     SIC SICE SICERGOEL
plain   sic ergo elementic
cipher  NTF ZCLT ZVHRYVIPE
```

Problems?

Also invented the Cardano grille