Nomenclators

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

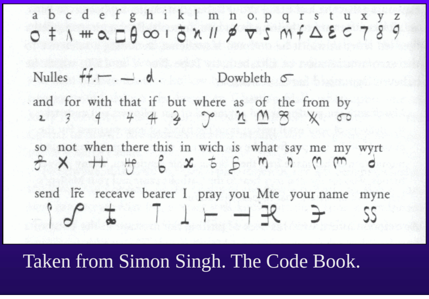
Philip of Spain (1589, see Kahn):

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

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

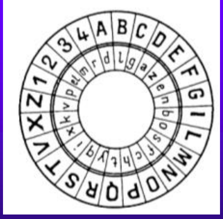
so not when there this in wich is what say me my wyrt

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.



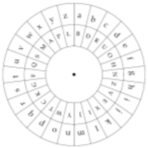
A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
g l k l n r t v z & x y s o m q i h f d b a c e p

outer disk (fixed)
plaintext

inner disk (moving)
ciphertext

Agree on *index letter* on inner disk.
Key: letter corresponding to index letter on outer disk.
Key can change during encryption

Cipher Disk Examples



Let’s choose “K” as index letter.

↓

Examples:

rRVTZOK
aKVtTRCK
HKmZMEP

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

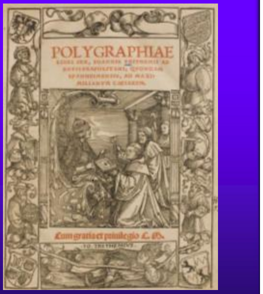
Are there other ways to use the cipher disk?

Johannes Trithemius

1462-1516, Germany

Polygraphiae, 1518
First printed book on cryptography.

- Ave Maria Cipher
- Polyalphabetic substitution
- Progressive key



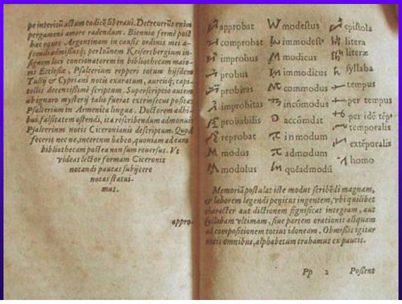
http://diglib.hab.de/drucke/12-3-rhet-2f/start.htm

Steganographia, 1606

- hidden writing

Polygraphiae I

The *Polygraphiae* contains many pages of code.



pe interitū aſtum todiceē liberaui. Decreuerūt enim pergameni amore radendum. Biennio fermè poſt hec equet Argentinam in cauſis ordinis mei aſcendi admiſſusq; per Ioānem Keiſersbergium inſignem loci contionatorem in bibliothecam maioris Eccleſie, Pſalterium repperi totum hÿſdem Tullÿ & Cypriani notis exaratum, aureisq; capitellis decentiſſimè ſcriptum. Superſcriptio autem ab ignaro myſterÿ talis fuerat extrinſecus poſita: Pſalterium in Armenica lingua. Doctorem adhibui, falſitatem oſtendi, ita reſcribendum admonui: Pſalterium notis Ciceronianis deſcriptum. Quod fecerit nec ne, incertum habeo, quoniam ad eam bibliothecam poſtea non ſum reuerſus. Vt videas lector formam Ciceronis notandi paucas ſubÿcere notas ſtatuimus.

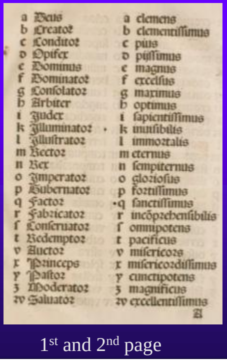
appro-

approbat	modeſtus	epiſtola
comprobat	immodeſt⁹	litera
improbus	modicus	literæ
probus	immodicus	ſyllaba
probitas	commodus	tempus
improbitas	incómodus	per tempus
probabilis	accōmdat	per idē tēp⁹
reprobat	inmodum	temporalis
modus	admodum	extēporalis
modulus	quēadmodū	homo

Memoriā poſtulat iſte modus ſcribēdi magnam, & laborem legendi peritus 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.

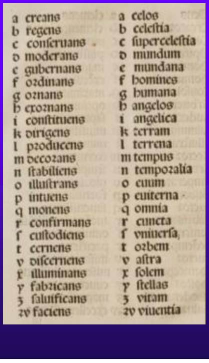
Pp 2 Poſſent

Polygraphiae II: Ave Maria



a	Deus	a	clemens
b	Creatoꝛ	b	clementiſſimus
c	Conditoꝛ	c	pius
d	Opifex	d	piiſſimus
e	Dominus	e	magnus
f	Dominatoꝛ	f	excelſus
g	Conſolatoꝛ	g	maximus
h	Arbiter	h	optimus
i	Iudex	i	ſapientiſſimus
k	Illuminatoꝛ	k	inuiſibilis
l	Illuſtratoꝛ	l	immoꝛtalis
m	Rectoꝛ	m	eternus
n	Rex	n	ſempiternus
o	Imperatoꝛ	o	gloꝛioſus
p	Gubernatoꝛ	p	foꝛtiſſimus
q	Factoꝛ	q	ſanctiſſimus
r	Fabꝛicatoꝛ	r	incōpꝛehenſibilis
ſ	Conſeruatoꝛ	ſ	omnipotens
t	Redemptoꝛ	t	pacificus
v	Auctoꝛ	v	miſericoꝛs
x	Princeps	x	miſericoꝛdiſſimus
y	Paſtoꝛ	y	cunctipotens
z	Moderatoꝛ	z	magnificus
w	Saluatoꝛ	w	excellentiſſimus

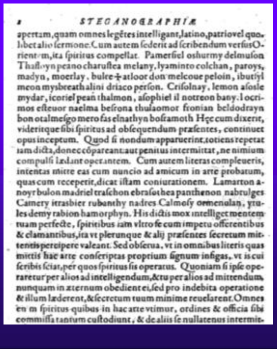
A



a	creans	a	celos
b	regens	b	celeſtia
c	conſeruans	c	ſupercęleſtia
d	moderans	d	mundum
e	gubernans	e	mundana
f	oꝛdinans	f	homines
g	oꝛnans	g	humana
h	exoꝛnans	h	angelos
i	conſtituens	i	angelica
k	dirigens	k	terram
l	pꝛoducens	l	terrena
m	decoꝛans	m	tempus
n	ſtabiliens	n	tempoꝛalia
o	illuſtrans	o	euum
p	intuens	p	euiterna
q	monens	q	omnia
r	confirmans	r	cuncta
ſ	cuſtodiens	ſ	vniuerſa
t	cernens	t	oꝛbem
v	diſcernens	v	aſtra
x	illuminans	x	ſolem
y	fabꝛicans	y	ſtellas
z	ſalutificans	z	vitam
w	faciens	w	viuentia

1st and 2nd page

Steganographia



STEGANOGRAPHIÆ

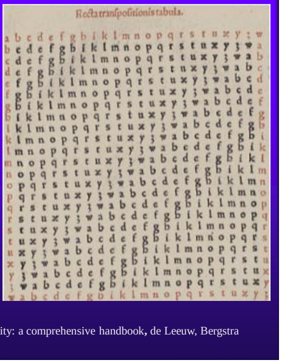
apertam, quam omnes legētes intelligant, latino, patrio vel quolibet alio ſermone. Cum autem ſederit ad ſcribendum verſus Orientem, ita ſpiritus compellat. Pamerſiel oshurmy delmuſon Thafloyn peano charuſtea melany, lyaminto colchan, paroys, madyn, moerlay, bulre + atloor don melcoue peloin, ibutſyl meon mysbreathalini driaco perſon. Criſolnay, lemon aſosle mydar, icoriel peañ thalmon, aſophiel il notreon bany. Iocrimos eſteuor naelma beſrona thuſaomor fronian beldodrayn bon otalmeſgo mero fas elnathyn boſramoth. Hęc cum dixerit, videritque ſibi ſpiritus ad obſequendum præſentes, continuet opus inceptum. Quod ſi nondum apparuerint, totiens repetat iam dicta, donec cōpareant: aut penitus intermittat, ne nimium compulſi lædant operantem. Cum autem literas compleueris, intentas mitte eas cum nuncio ad amicum in arte probatum, quas cum receperit, dicat iſtam coniurationem. Lamarton anoyr bulon madriel traſchon ebraſothea panthenon nabrulges Camery itrasbier rubanthy nadres Calmoſy ormenulan, ytules demy rabion hamorphyn. His dictis mox intelliget mentem tuam perfecte, ſpiritibus iam vltro ſe cum impetu offerentibus & clamantibus, ita vt plerunque & alij præſentes ſecretum mittentis percipere valeant. Sed obſerua, vt in omnibus literis quas mittis hac arte conſcriptas proprium ſignum inſigas, vt is cui ſcribis ſciat, per quos ſpiritus ſis operatus. Quoniam ſi ipſe operaretur per alios ad intelligendum, & tu per alios ad mittendum, nunquam in æternum obedient ei, ſed pro indebita operatione & illum læderent, & ſecretum tuum minime reuelarent. Omnes enim ſpiritus quibus in hac arte vtimur, ordines & officia ſibi commiſſa tantum cuſtodiunt, & de aliis ſe nullatenus intermit-

http://books.google.com/books?id=bQdCAAAAcAAJ&dq=Trithemius%20Steganographia&pg=PR6#v=onepage&q&f=false

Polygraphiae III

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

- Polyalphabetic substitution
- Progressive key



Recta tranſpoſitionis tabula.

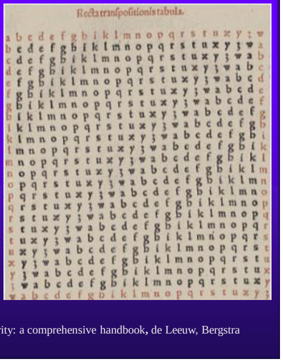
a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e
g	h	i	k	l	m	n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

The history of information security: a comprehensive handbook, de Leeuw, Bergstra

Polygraphiae IV

Examples (starting with first alphabet)

- Johannes
- SUGKESUOWSUN



Recta transpoſitionis tabula.

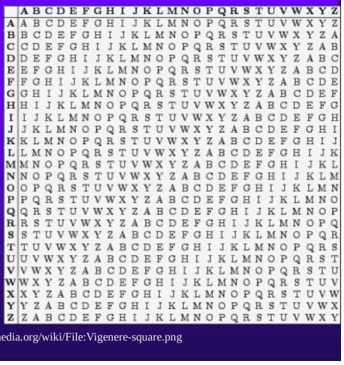
a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	ʒ	w	a	b	c	d	e
g	h	i	k	l	m	n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

The history of information security: a comprehensive handbook, de Leeuw, Bergstra

Modern Tabula Recta

More Examples (not from beginning)

- XNNN
- NUGUV



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

http://commons.wikimedia.org/wiki/File:Vigenere-square.png

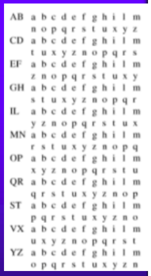
Giovan Batista Belaso

La cifra del. Sig. Giovan Batista Belaso, 1553

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

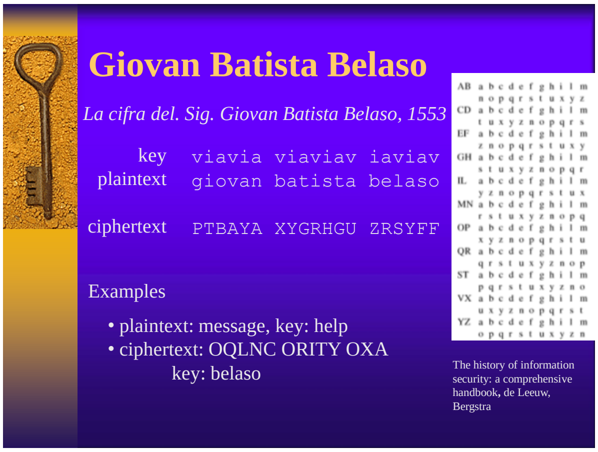
```
      key   viavia viaviav iaviav
plaintext   giovan batista belaso

ciphertext  PTBAYA XYGRHGU ZRSYFF
```

Decrypt: OQLNC ORITY OXA (belaso)



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

The history of information security: a comprehensive handbook, de Leeuw, Bergstra



Giovan Batista Belaso

La cifra del. Sig. Giovan Batista Belaso, 1553

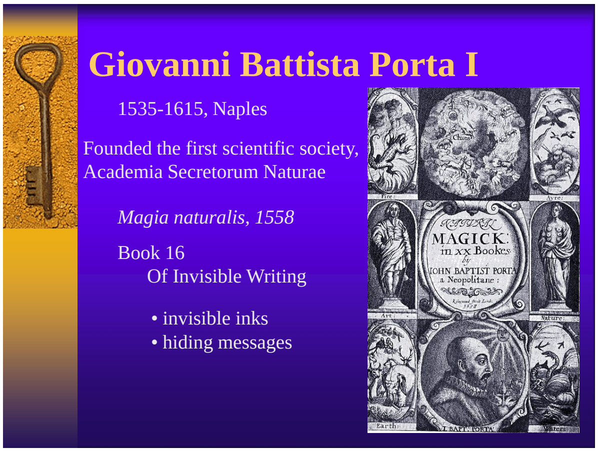
```
       key   viavia viaviav iaviav
 plaintext   giovan batista belaso

ciphertext   PTBAYA XYGRHGU ZRSYFF
```

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

Examples

- plaintext: message, key: help
- ciphertext: OQLNC ORITY OXA
  key: belaso

The history of information security: a comprehensive handbook, de Leeuw, Bergstra



Giovanni Battista Porta I

1535-1615, Naples

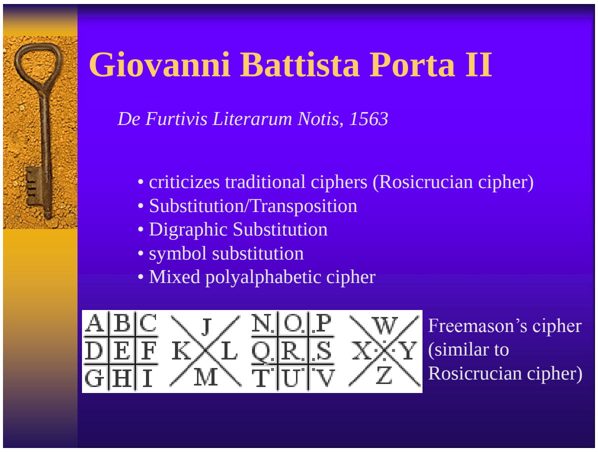
Founded the first scientific society, Academia Secretorum Naturae

Magia naturalis, 1558

Book 16
Of Invisible Writing

- invisible inks
- hiding messages

Chaos
Fire
Ayre
NATURAL MAGICK in xx Bookes by JOHN BAPTIST PORTA a Neopolitane
Art
Nature
Earth
I. BAPT. PORTA
Waters

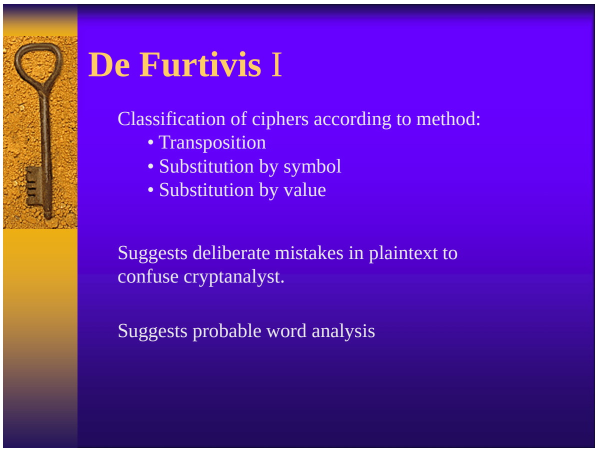


Giovanni Battista Porta II

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)



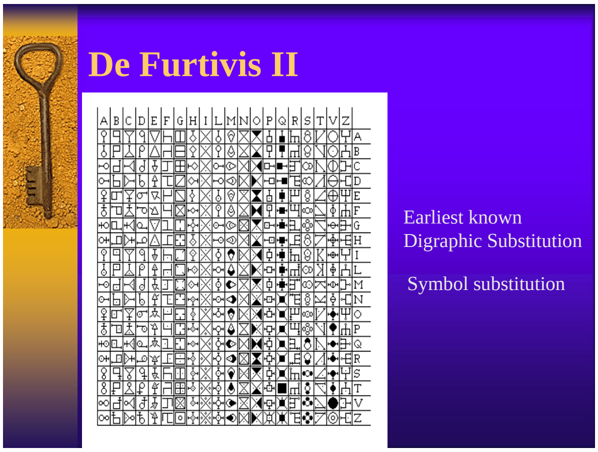
De Furtivis I

Classification of ciphers according to method:

- Transposition
- Substitution by symbol
- Substitution by value

Suggests deliberate mistakes in plaintext to confuse cryptanalyst.

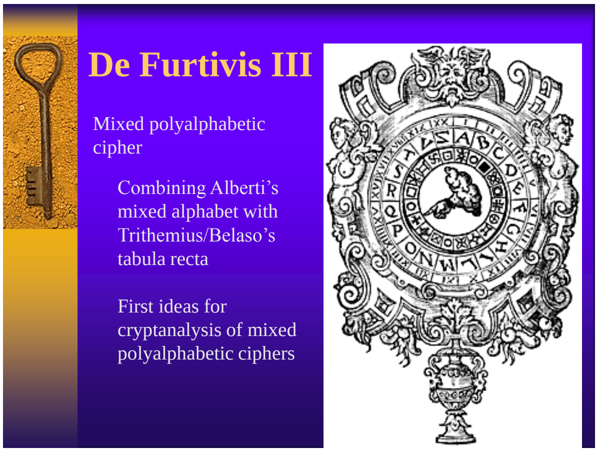
Suggests probable word analysis



De Furtivis II

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 “fed”, “pon” in a progressive polyalphabetic cipher?

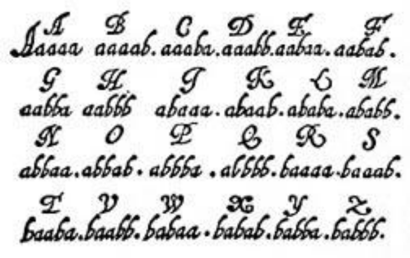
Observation on a polyalphabetic cipher with literal key:

> “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

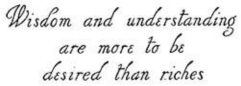
Francis Bacon (1561-1626), England

First idea: encode letters in binary (1623)

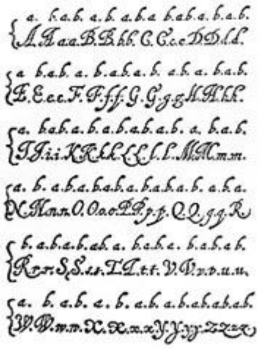


A	B	C	D	E	F
aaaaa	aaaab.	aaaba.	aaabb.	aabaa.	aabab.
G	H	I	K	L	M
aabba	aabbb	abaaa.	abaab.	ababa.	ababb.
N	O	P	Q	R	S
abbaa.	abbab.	abbba.	abbbb.	baaaa.	baaab.
T	V	W	X	Y	Z
baaba.	baabb.	babaa.	babab.	babba.	babbb.

Bacon’s Biliteral cipher II

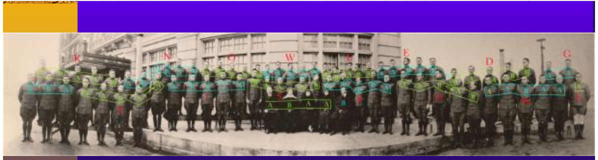


Wisdom and understanding are more to be desired than riches



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

Example:
To be *or* not to be *that* is *the* *q*uestion.



Girolamo Cardano

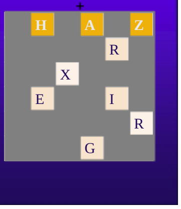
De Subtilitate, 1550; De Rerum Varietate, 1556

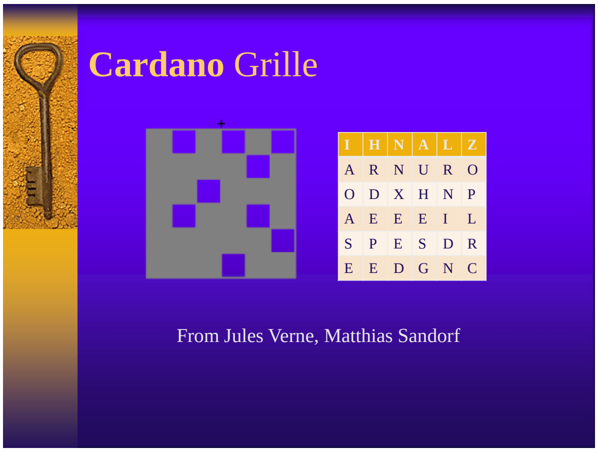
Autokeys:

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

Problems?

Also invented the Cardano grille





Cardano Grille

I	H	N	A	L	Z
A	R	N	U	R	O
O	D	X	H	N	P
A	E	E	E	I	L
S	P	E	S	D	R
E	E	D	G	N	C

From Jules Verne, Matthias Sandorf