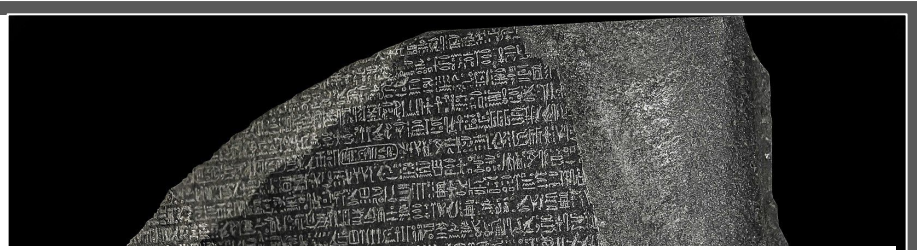
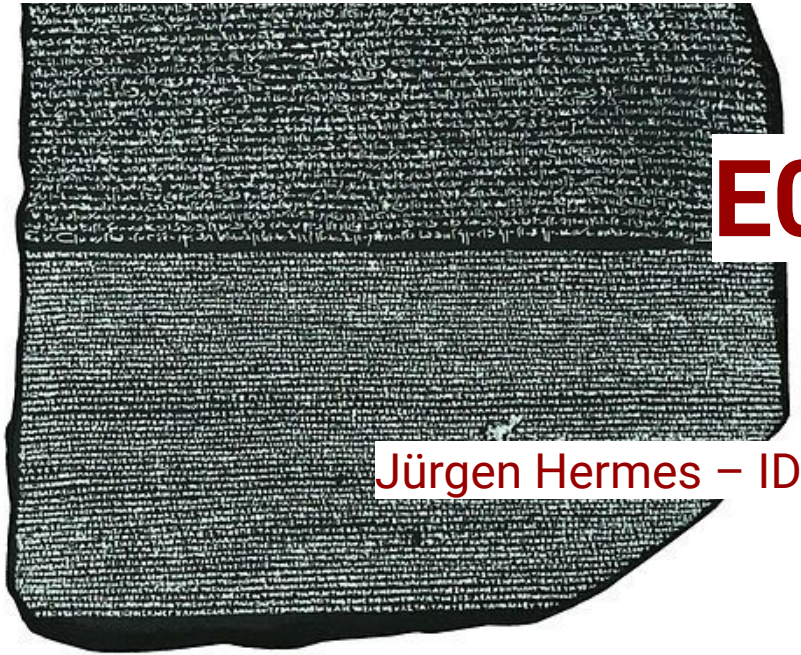


Anatomie der Schriftsprachen



E05

Jürgen Hermes – IDH – WiSe 2022/2023

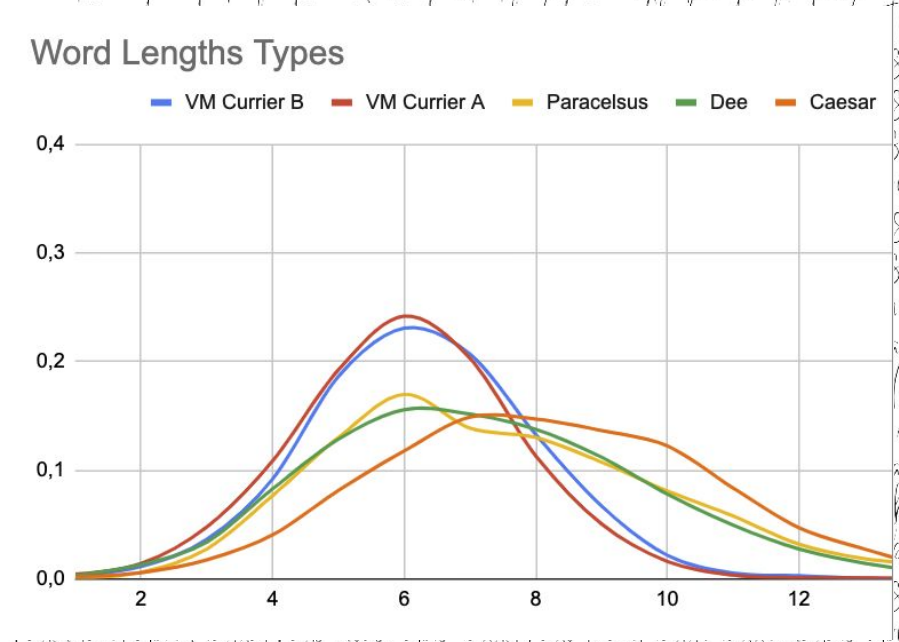
Polygraphia III – The Cipher that pretends to be an artificial language

Jürgen Hermes – University of Cologne

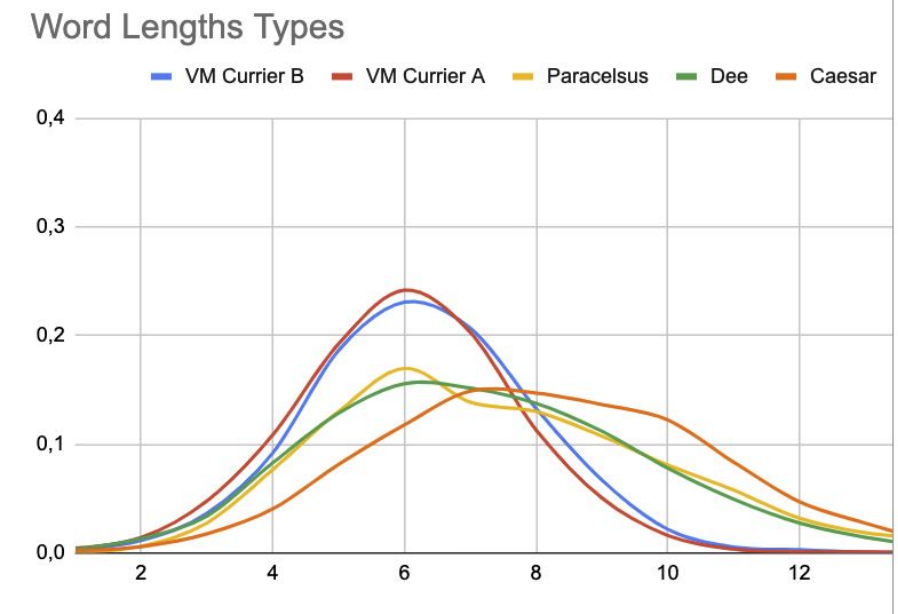
Structure

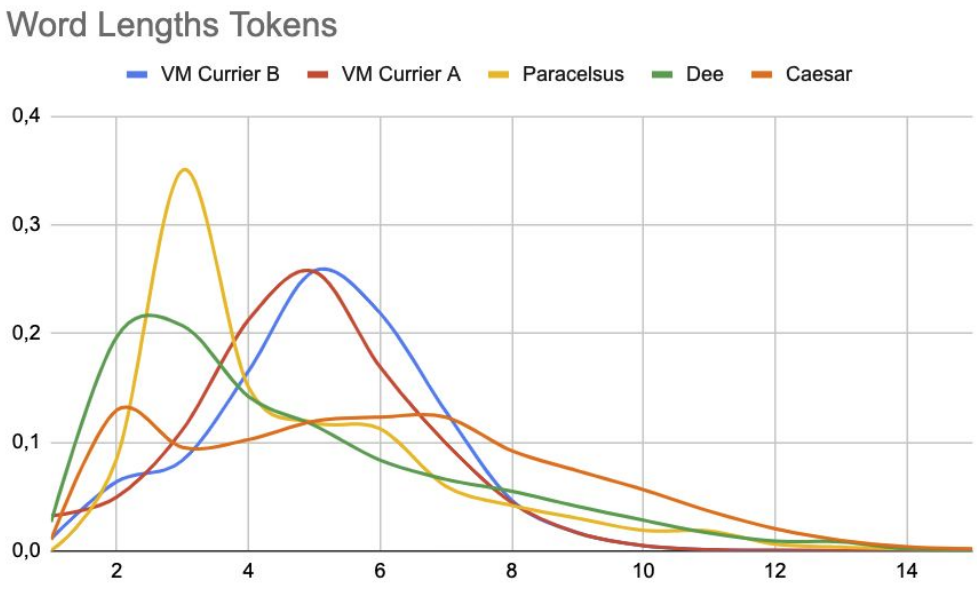
- The properties of Voynichese (and the problems arising from it)
- The hypothesis of Friedman (and the problems arising from it)
- The ciphers of Trithemius – Polygraphiae I and III
- Experiments and results
- What I (do not) claim

The Odd Properties of Voynichese: Word Length



The Odd Properties of Voynichese: Word Length





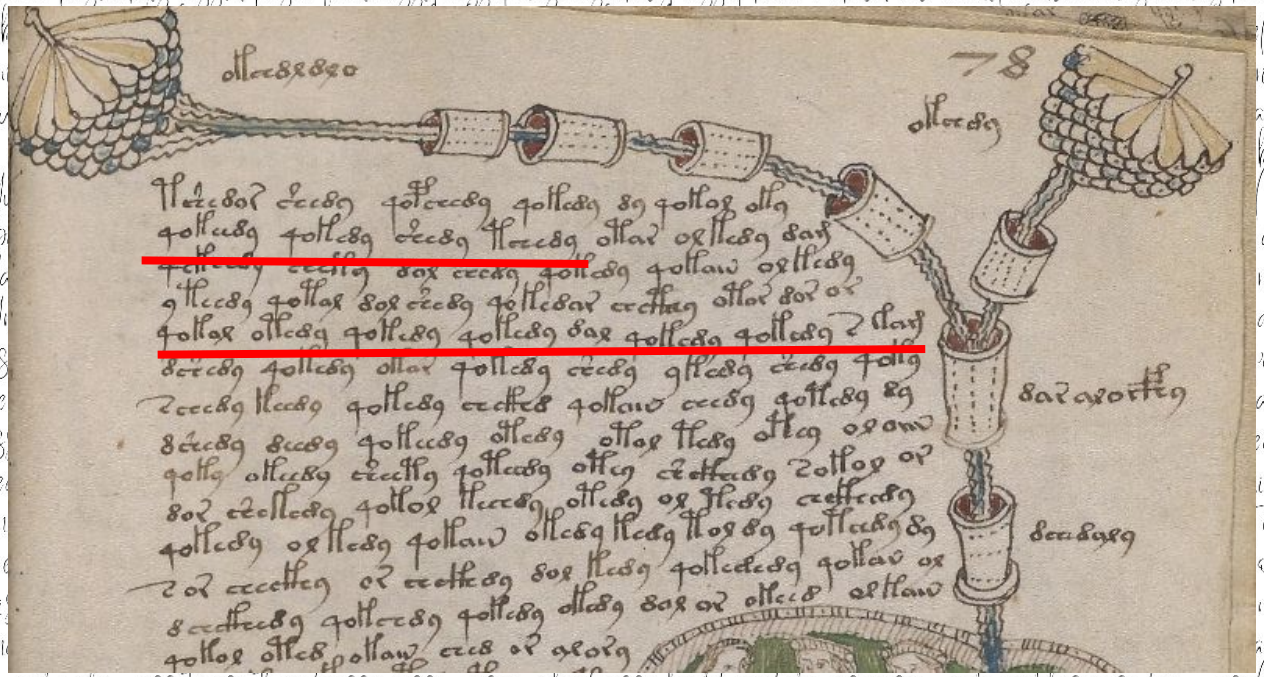
The Odd Properties of Voynichese: Entropy

$$h_2 = \sum_{I=1}^{n} p(I,J) * b(I,J) = -\sum_{I=1}^{n}\sum_{J=1}^{n} p(x_I) * p(y_J|x_I) * log_2(p(y_J|x_I))$$

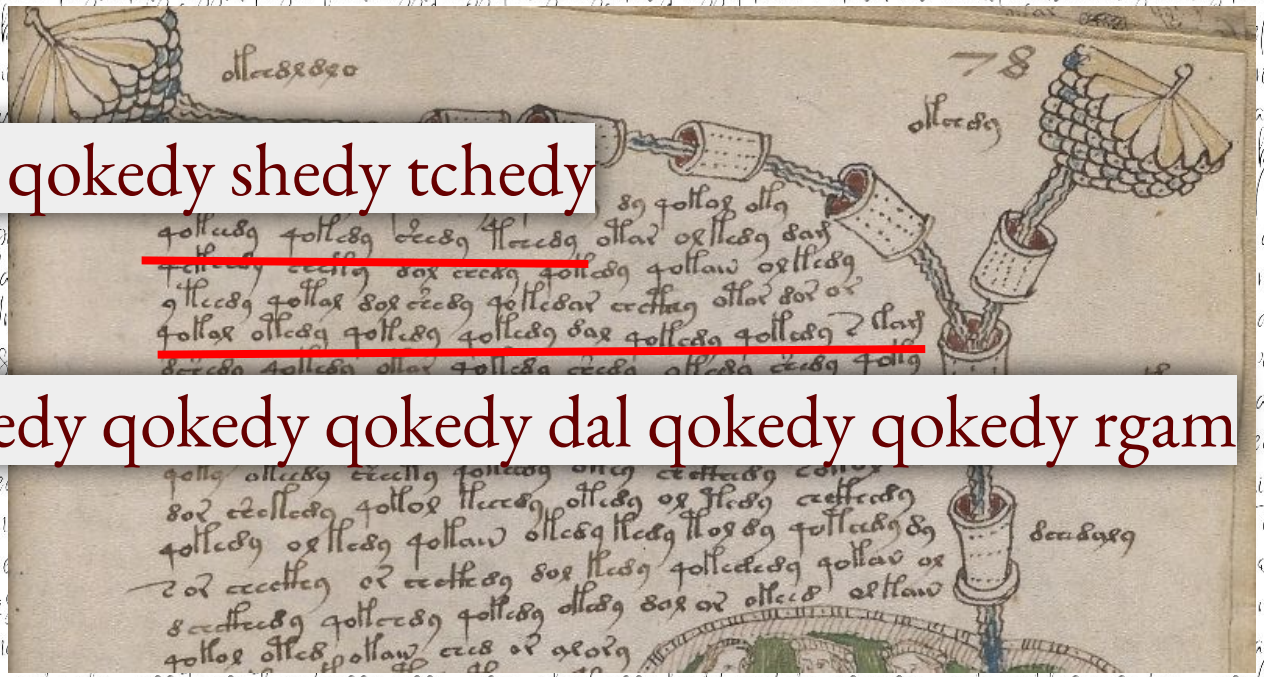
The Odd Properties of Voynichese: Entropy

$$h_2 = \sum_{I=1}^{n} p(I,J) * b(I,J) = -\sum_{I=1}^{n}\sum_{J=1}^{n} p(x_I) * p(y_J|x_I) * log_2(p(y_J|x_I))$$

The Odd Properties of Voynichese: Repetitiveness



The Odd Properties of Voynichese: Repetitiveness



qokeedy qokedy shedy tchedy

qokal otedy qokedy qokedy dal qokedy qokedy rgam

The Anagram Friedman left us (1959)

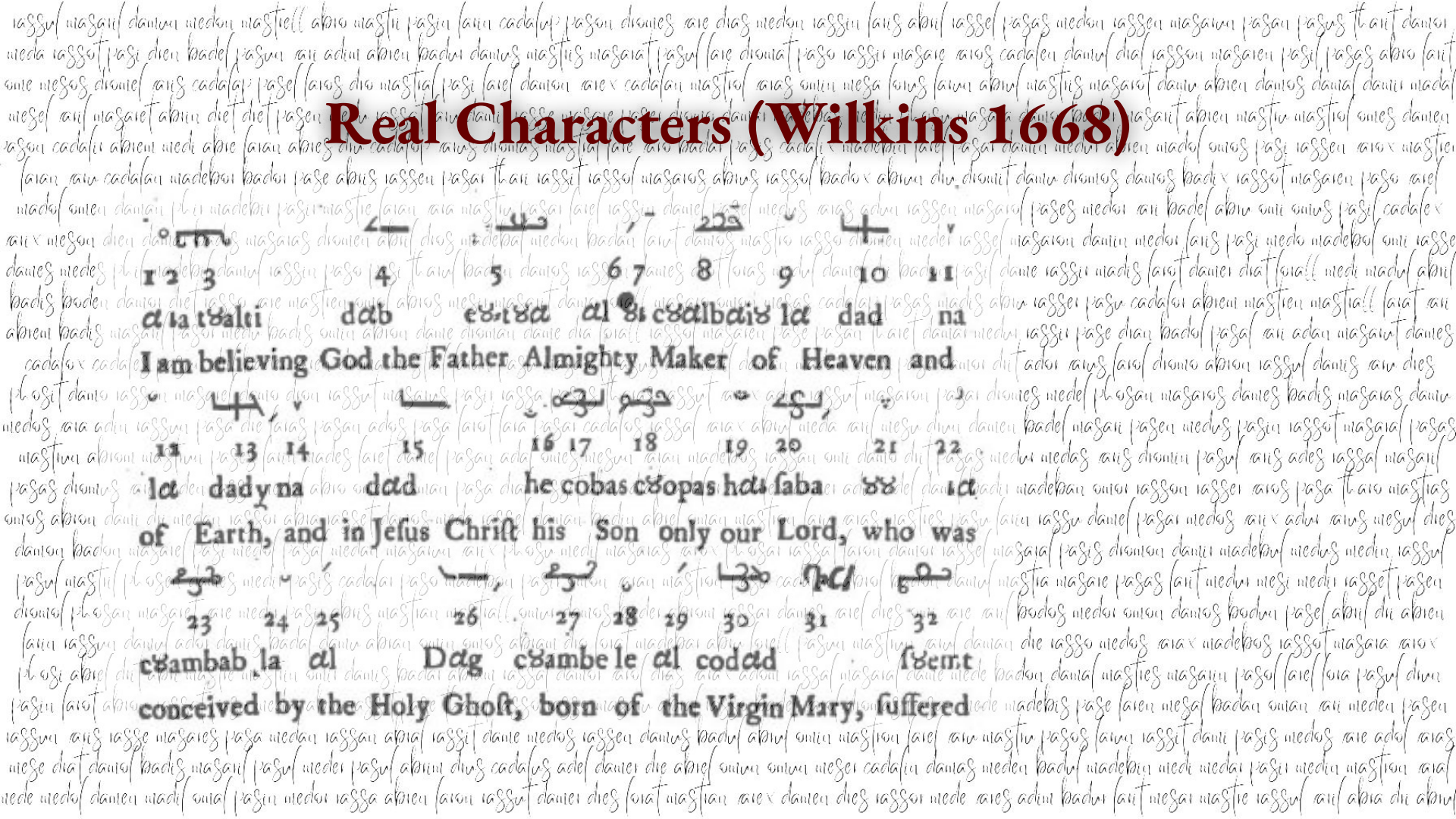
"I put no trust in anagrammatic acrostic cyphers, for they are of little real value — a waste — and may prove nothing — finis."

The Anagram Friedman left us (1959)

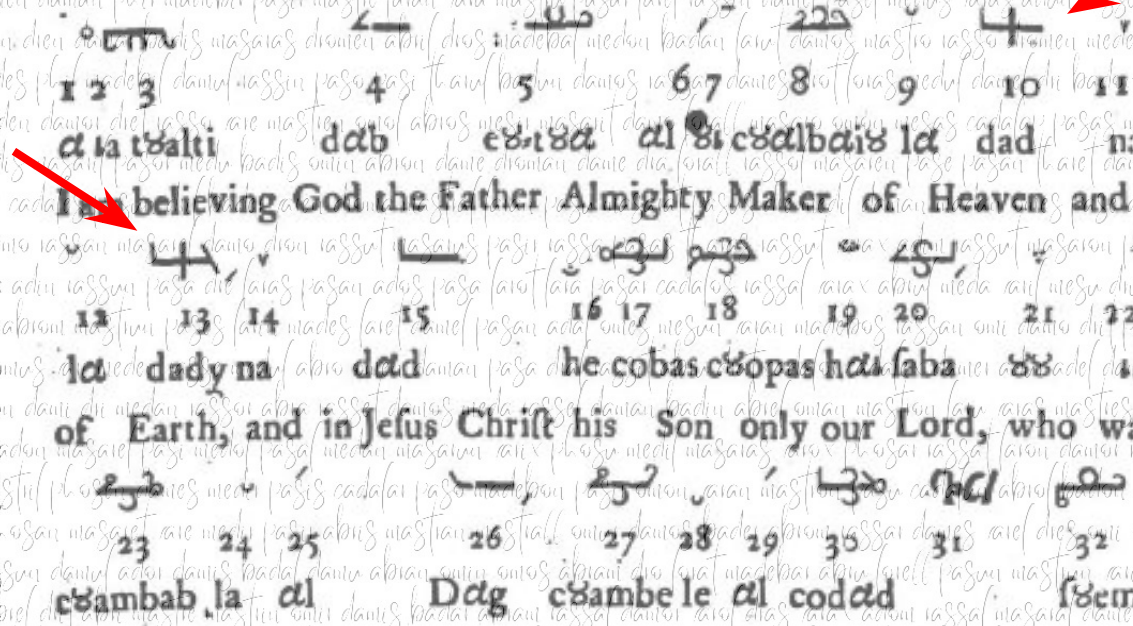
"I put no trust in anagrammatic acrostic cyphers, for they are of little real value — a waste — and may prove nothing — finis."

"The Voynich Manuscript was an early attempt to construct an artificial or universal language of the A-Priori type.—Friedman."

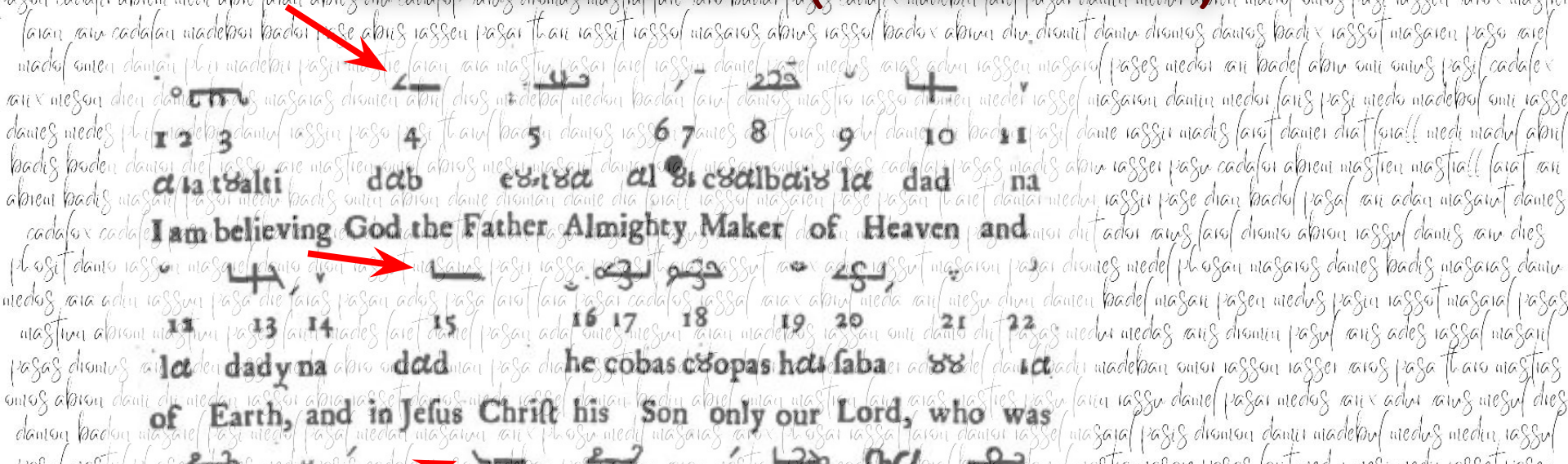
Real Characters (Wilkins 1668)



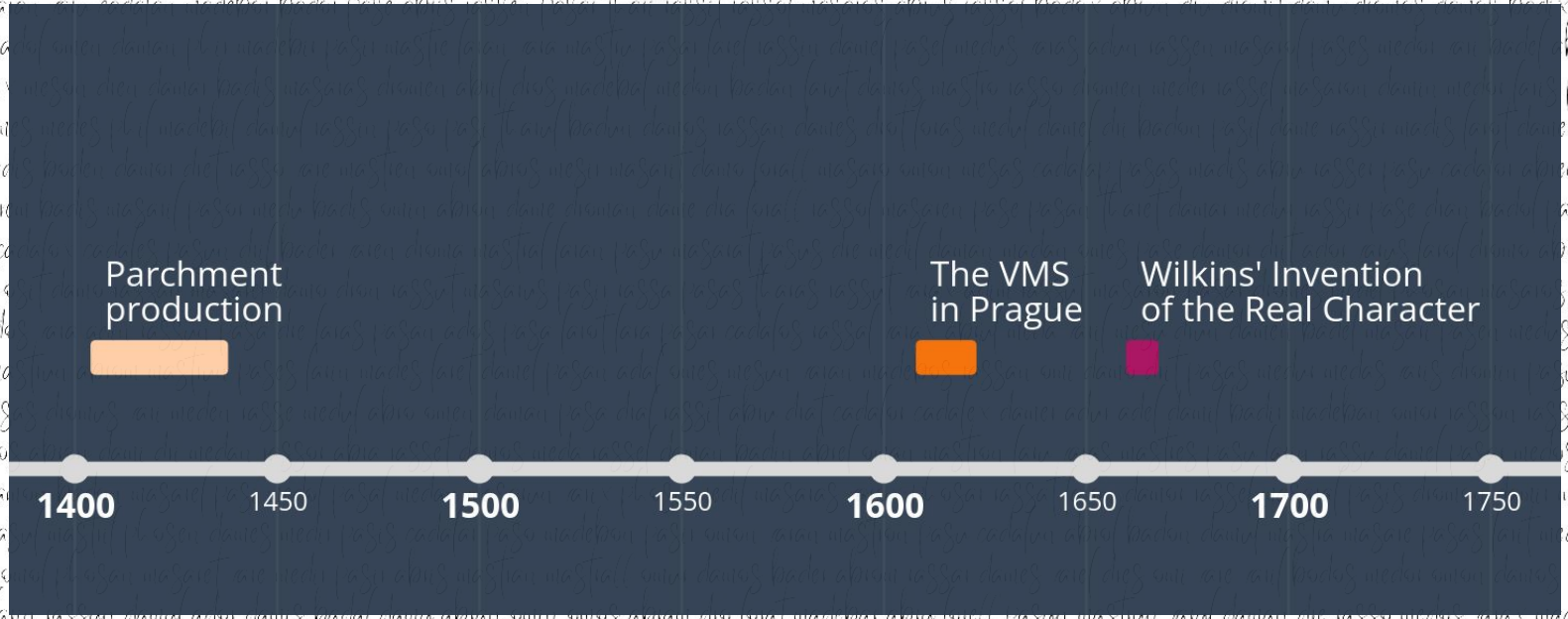
Real Characters (Wilkins 1668)



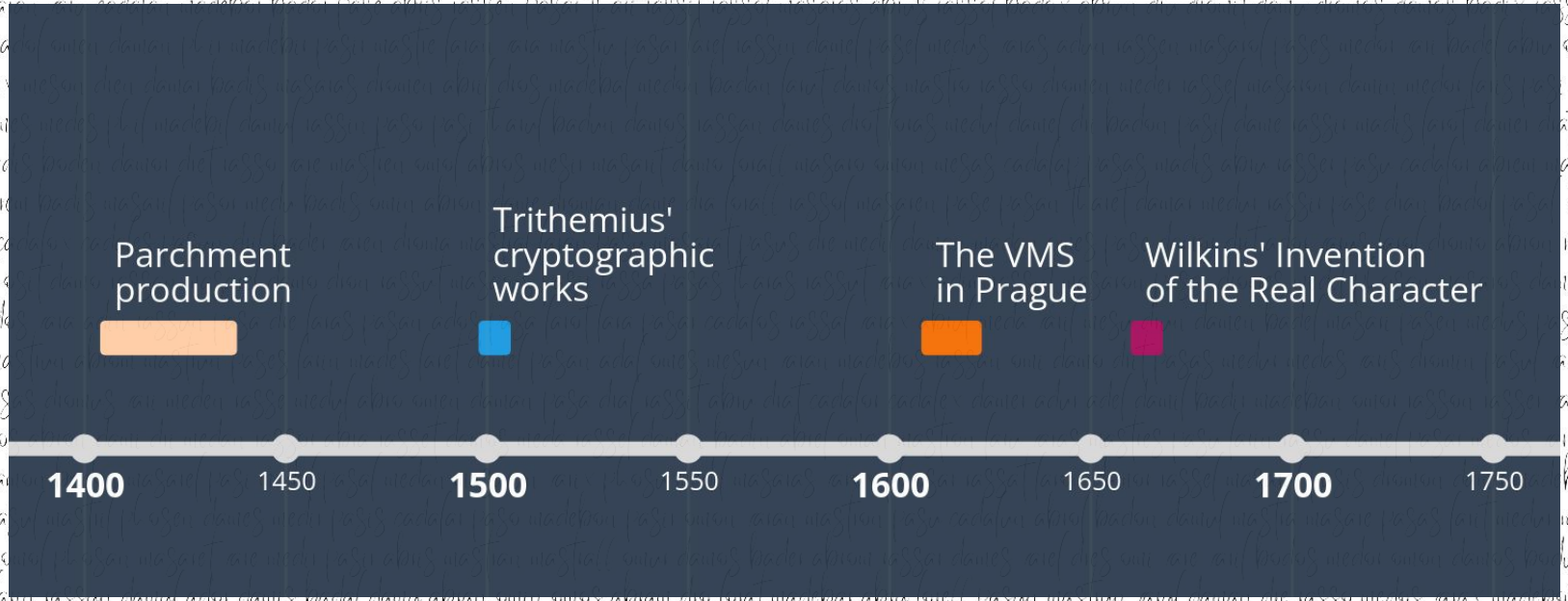
Real Characters (Wilkins 1668)



The problematic timeline

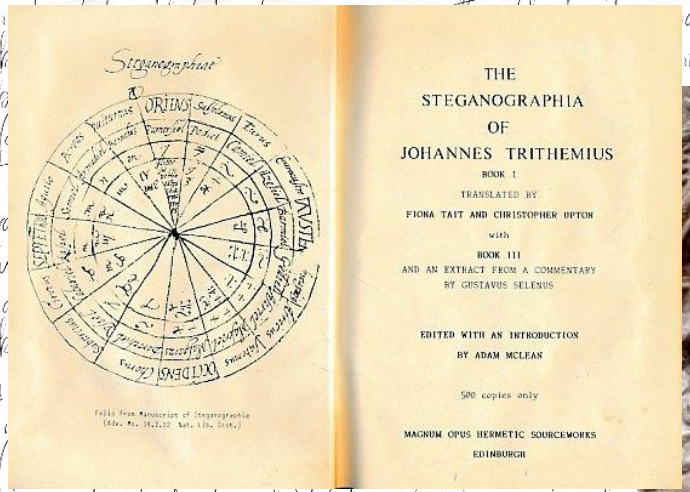


The problematic timeline

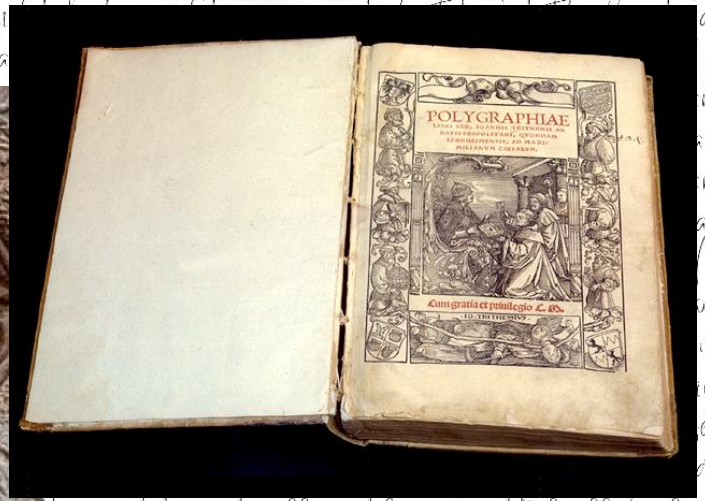


Johannes Trithemius (1462 - 1516)

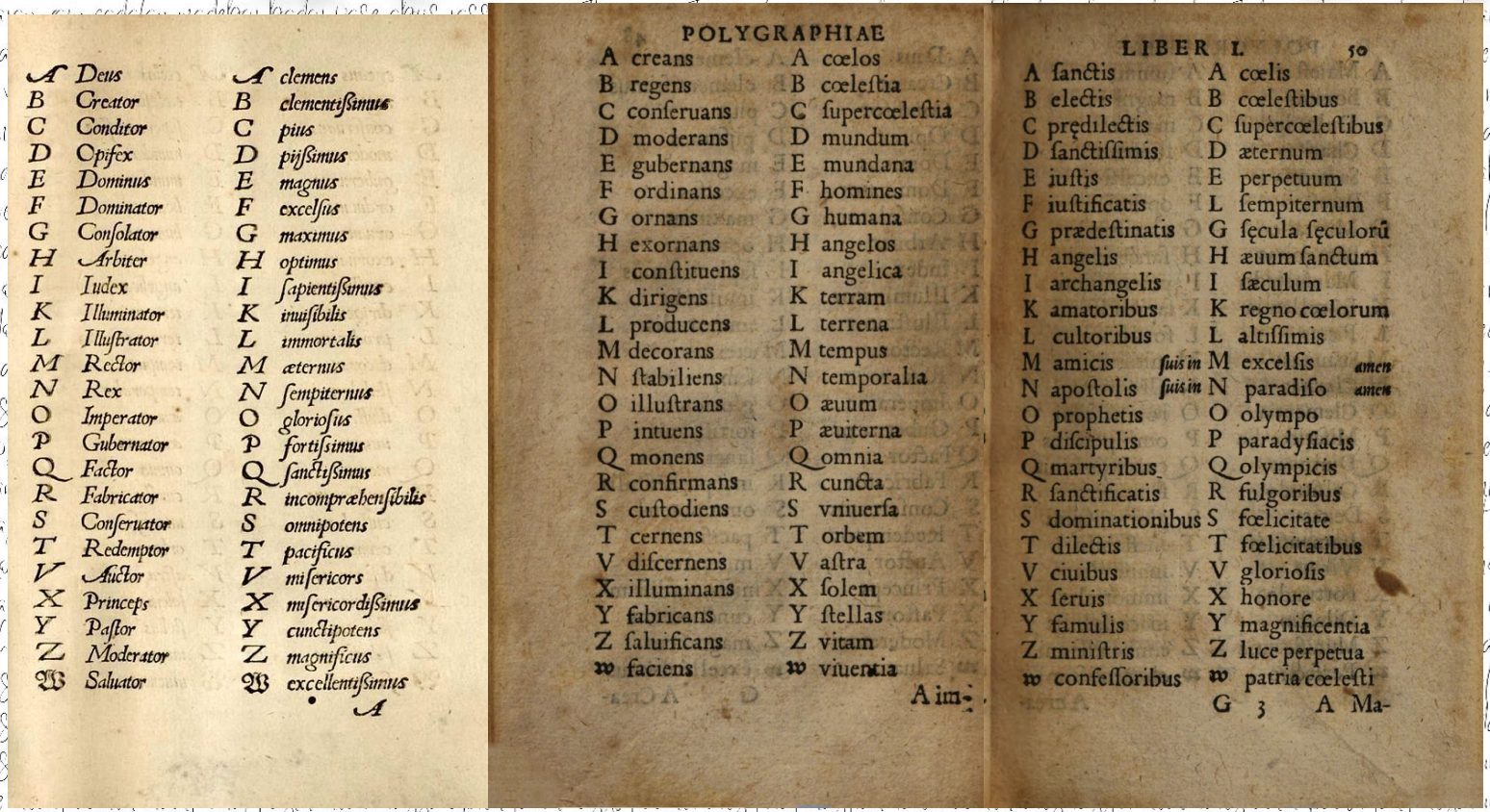
Steganographia (1499/1500)



Polygraphia (1506)



Polygraphia I: Ave Maria (Hale Mary) Cipher



A	Deus	A	clemens
B	Creator	B	elementiſſimus
C	Conditor	C	pius
D	Opifex	D	piiſſimus
E	Dominus	E	magnus
F	Dominator	F	excelſius
G	Conſolator	G	maximus
H	Arbiter	H	optimus
I	Iudex	I	ſapientiſſimus
K	Illuminator	K	inuiſibilis
L	Illuſtrator	L	immortalis
M	Rector	M	æternus
N	Rex	N	ſempiternus
O	Imperator	O	glorioſius
P	Gubernator	P	fortiſſimus
Q	Factor	Q	ſanctiſſimus
R	Fabricator	R	incompræhenſibilis
S	Conſeruator	S	omnipotens
T	Redemptor	T	pacificus
V	Auctor	V	miſericors
X	Princeps	X	miſericordiſſimus
Y	Paſtor	Y	cunctipotens
Z	Moderator	Z	magnificus
W	Saluator	W	excellentiſſimus

A

POLYGRAPHIAE

A	creans	A	cœlos
B	regens	B	cœleſtia
C	conſeruans	C	ſupercœleſtia
D	moderans	D	mundum
E	gubernans	E	mundana
F	ordinans	F	homines
G	ornans	G	humana
H	exornans	H	angelos
I	conſtituens	I	angelica
K	dirigens	K	terram
L	producens	L	terrena
M	decorans	M	tempus
N	ſtabiliens	N	temporalia
O	illuſtrans	O	æuum
P	intuens	P	æuiterna
Q	monens	Q	omnia
R	confirmans	R	cuncta
S	cuſtodiens	S	vniuerſa
T	cernens	T	orbem
V	diſcernens	V	aſtra
X	illuminans	X	ſolem
Y	fabricans	Y	ſtellas
Z	ſaluificans	Z	vitam
w	faciens	w	viuentia

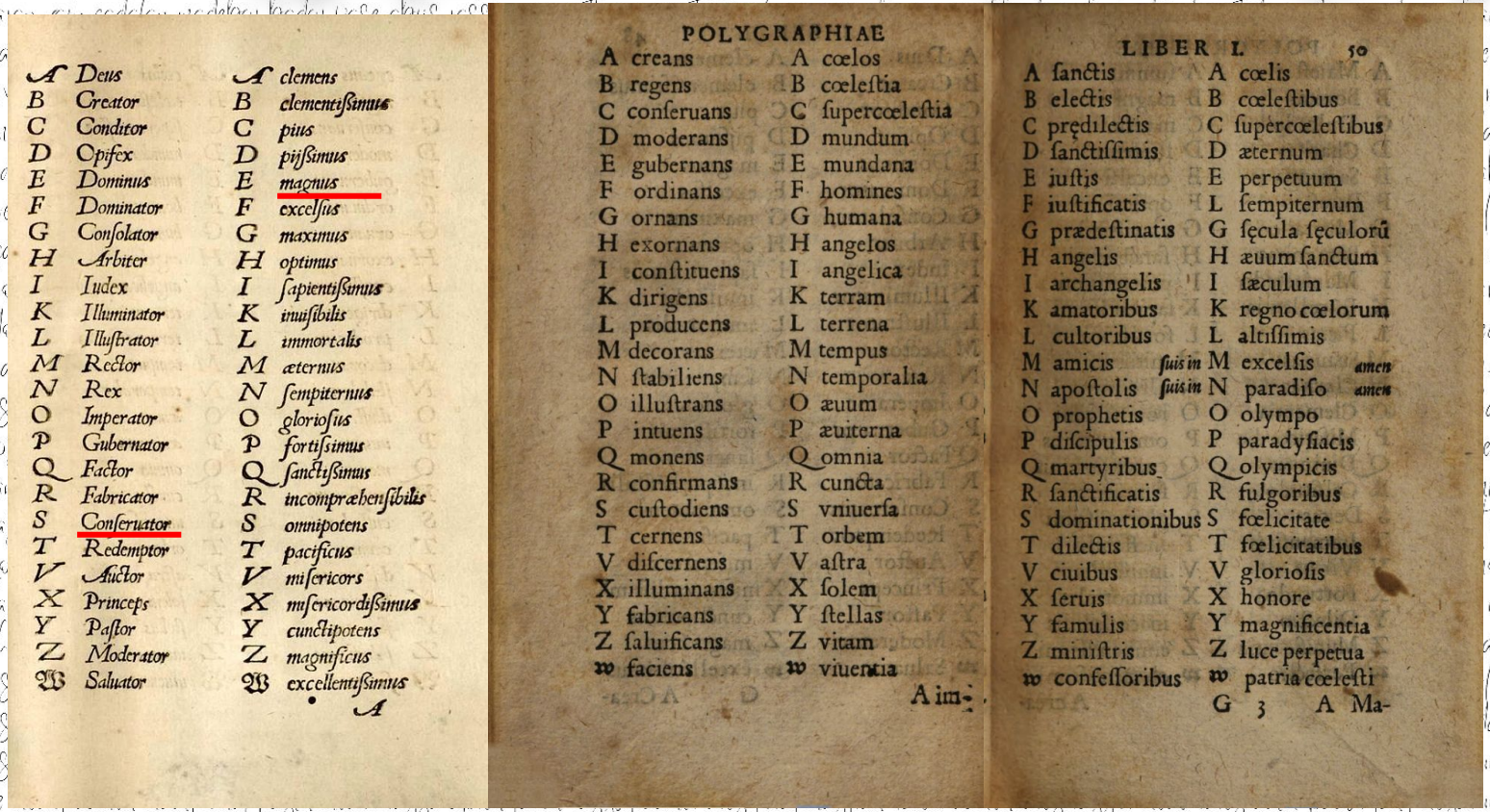
A im-

LIBER I. 50

A	ſanctis		A	cœlis
B	electis		B	cœleſtibus
C	prędilectis		C	ſupercœleſtibus
D	ſanctiſſimis		D	æternum
E	iuſtis		E	perpetuum
F	iuſtificatis		L	ſempiternum
G	prædeſtinatis		G	ſęcula ſęculorũ
H	angelis		H	æuum ſanctum
I	archangelis		I	ſæculum
K	amatoribus		K	regno cœlorum
L	cultoribus		L	altiſſimis
M	amicis	*ſuis in*	M	excelſis *amen*
N	apoſtolis	*ſuis in*	N	paradiſo *amen*
O	prophetis		O	olympo
P	diſcipulis		P	paradyſiacis
Q	martyribus		Q	olympicis
R	ſanctificatis		R	fulgoribus
S	dominationibus		S	fœlicitate
T	dilectis		T	fœlicitatibus
V	ciuibus		V	glorioſis
X	ſeruis		X	honore
Y	famulis		Y	magnificentia
Z	miniſtris		Z	luce perpetua
w	confeſſoribus		w	patria cœleſti

G 3 A Ma-

Polygraphia I: Ave Maria (Hale Mary) Cipher



A	Deus	A	clemens
B	Creator	B	elementiſſimus
C	Conditor	C	pius
D	Opifex	D	piiſſimus
E	Dominus	E	magnus
F	Dominator	F	excelſius
G	Conſolator	G	maximus
H	Arbiter	H	optimus
I	Iudex	I	ſapientiſſimus
K	Illuminator	K	inuiſibilis
L	Illuſtrator	L	immortalis
M	Rector	M	æternus
N	Rex	N	ſempiternus
O	Imperator	O	glorioſius
P	Gubernator	P	fortiſſimus
Q	Factor	Q	ſanctiſſimus
R	Fabricator	R	incompræhenſibilis
S	Conſeruator	S	omnipotens
T	Redemptor	T	pacificus
V	Auctor	V	miſericors
X	Princeps	X	miſericordiſſimus
Y	Paſtor	Y	cunctipotens
Z	Moderator	Z	magnificus
W	Saluator	W	excellentiſſimus

A

POLYGRAPHIAE

A	creans	A cœlos
B	regens	B cœleſtia
C	conſeruans	C ſupercœleſtia
D	moderans	D mundum
E	gubernans	E mundana
F	ordinans	F homines
G	ornans	G humana
H	exornans	H angelos
I	conſtituens	I angelica
K	dirigens	K terram
L	producens	L terrena
M	decorans	M tempus
N	ſtabiliens	N temporalia
O	illuſtrans	O æuum
P	intuens	P æuiterna
Q	monens	Q omnia
R	confirmans	R cuncta
S	cuſtodiens	S vniuerſa
T	cernens	T orbem
V	diſcernens	V aſtra
X	illuminans	X ſolem
Y	fabricans	Y ſtellas
Z	ſaluificans	Z vitam
w	faciens	w viuentia

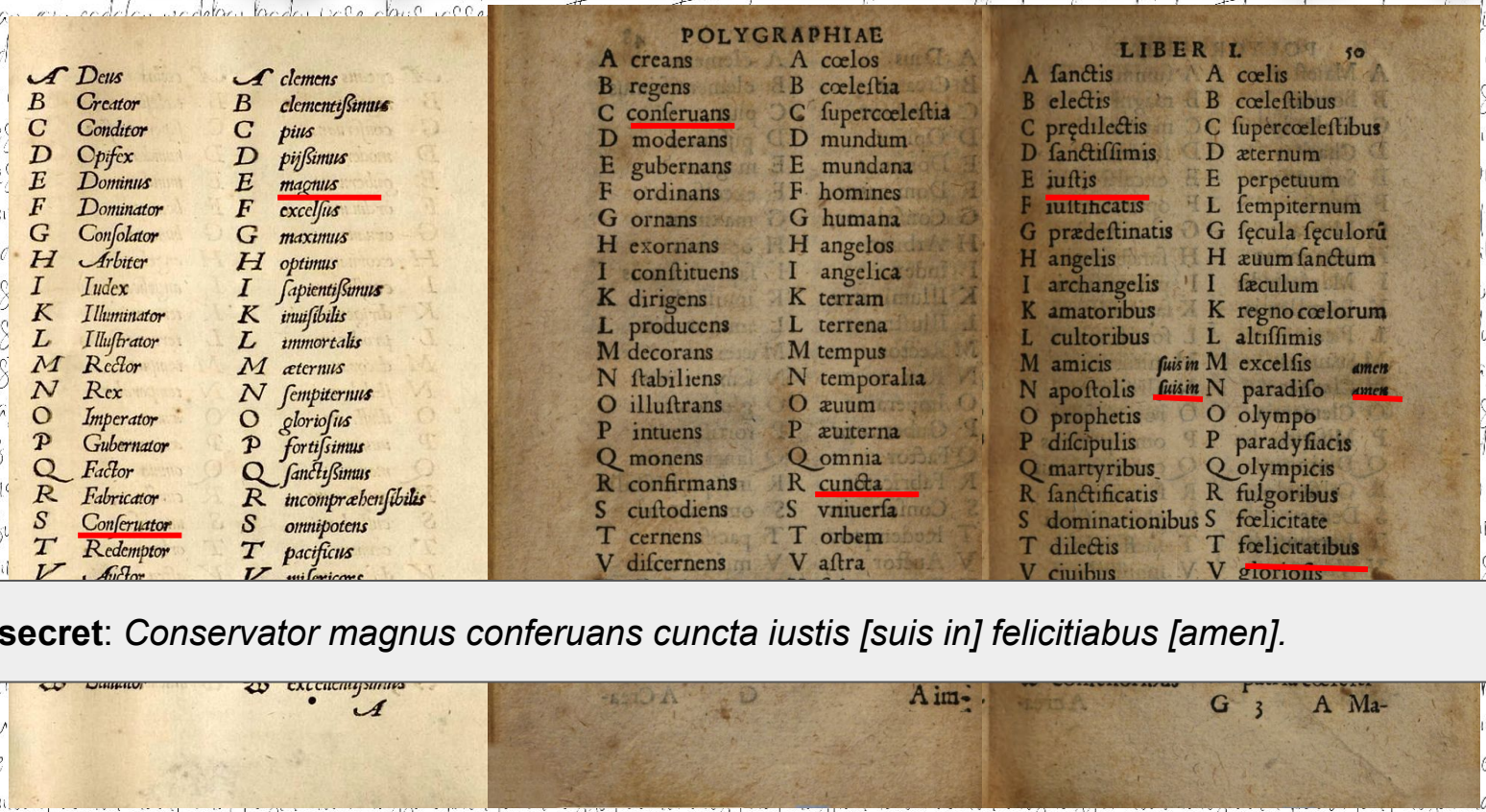
A im-

LIBER I. 50

A	ſanctis		A	cœlis
B	electis		B	cœleſtibus
C	prędilectis		C	ſupercœleſtibus
D	ſanctiſſimis		D	æternum
E	iuſtis		E	perpetuum
F	iuſtificatis		L	ſempiternum
G	prædeſtinatis		G	ſęcula ſęculorũ
H	angelis		H	æuum ſanctum
I	archangelis		I	ſæculum
K	amatoribus		K	regno cœlorum
L	cultoribus		L	altiſſimis
M	amicis	*ſuis in*	M	excelſis *amen*
N	apoſtolis	*ſuis in*	N	paradiſo *amen*
O	prophetis		O	olympo
P	diſcipulis		P	paradyſiacis
Q	martyribus		Q	olympicis
R	ſanctificatis		R	fulgoribus
S	dominationibus		S	fœlicitate
T	dilectis		T	fœlicitatibus
V	ciuibus		V	glorioſis
X	ſeruis		X	honore
Y	famulis		Y	magnificentia
Z	miniſtris		Z	luce perpetua
w	confeſſoribus		w	patria cœleſti

G 3 A Ma-

Polygraphia I: Ave Maria (Hale Mary) Cipher



A	Deus	A	clemens
B	Creator	B	clementiſſimus
C	Conditor	C	pius
D	Opifex	D	piiſſimus
E	Dominus	E	magnus
F	Dominator	F	excelſus
G	Conſolator	G	maximus
H	Arbiter	H	optimus
I	Iudex	I	ſapientiſſimus
K	Illuminator	K	inuiſibilis
L	Illuſtrator	L	immortalis
M	Rector	M	æternus
N	Rex	N	ſempiternus
O	Imperator	O	glorioſus
P	Gubernator	P	fortiſſimus
Q	Factor	Q	ſanctiſſimus
R	Fabricator	R	incompræhenſibilis
S	Conſeruator	S	omnipotens
T	Redemptor	T	pacificus

POLYGRAPHIAE

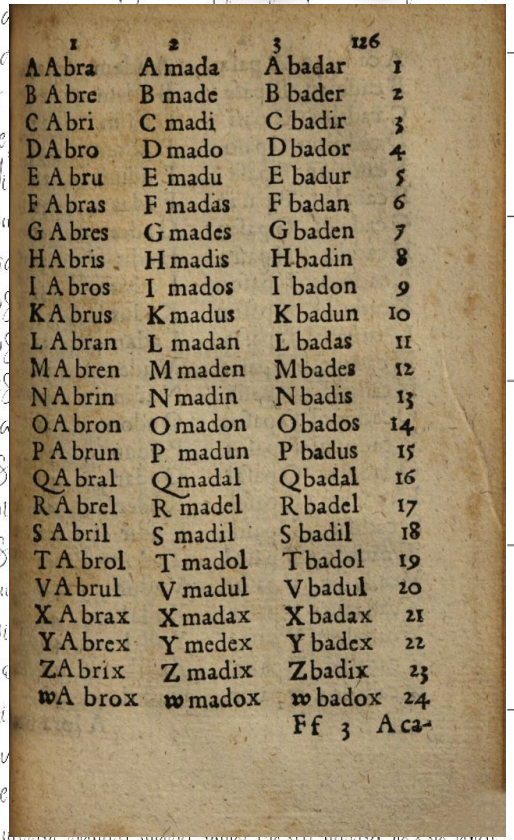
A	creans	A	cœlos
B	regens	B	cœleſtia
C	conſeruans	C	ſupercœleſtia
D	moderans	D	mundum
E	gubernans	E	mundana
F	ordinans	F	homines
G	ornans	G	humana
H	exornans	H	angelos
I	conſtituens	I	angelica
K	dirigens	K	terram
L	producens	L	terrena
M	decorans	M	tempus
N	ſtabiliens	N	temporalia
O	illuſtrans	O	æuum
P	intuens	P	æuiterna
Q	monens	Q	omnia
R	confirmans	R	cuncta
S	cuſtodiens	S	vniuerſa
T	cernens	T	orbem
V	diſcernens	V	aſtra

LIBER L 50

A	ſanctis		A	cœlis	
B	electis		B	cœleſtibus	
C	prędilectis		C	ſupercœleſtibus	
D	ſanctiſſimis		D	æternum	
E	iuſtis		E	perpetuum	
F	iuſtificatis		L	ſempiternum	
G	prædeſtinatis		G	ſęcula ſęculorũ	
H	angelis		H	æuum ſanctum	
I	archangelis		I	ſæculum	
K	amatoribus		K	regno cœlorum	
L	cultoribus		L	altiſſimis	
M	amicis	*ſuis in*	M	excelſis	*amen*
N	apoſtolis	*ſuis in*	N	paradiſo	*amen*
O	prophetis		O	olympo	
P	diſcipulis		P	paradyſiacis	
Q	martyribus		Q	olympicis	
R	ſanctificatis		R	fulgoribus	
S	dominationibus		S	fœlicitate	
T	dilectis		T	fœlicitatibus	
V	ciuibus		V	gloriosis	

secret: *Conservator magnus conferuans cuncta iustis [suis in] felicitiabus [amen].*

Polygraphia III: The Artificial Language Mimic



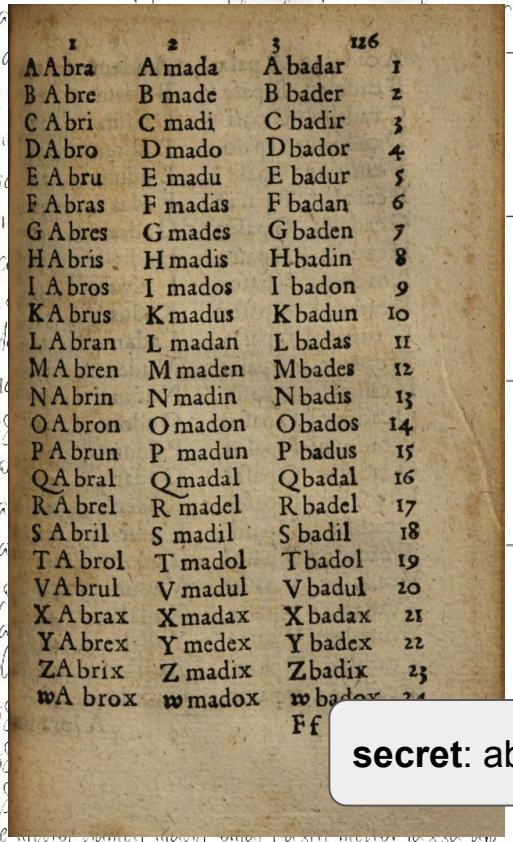
1 2 3 126

A Abra	A mada	A badar	1
B Abre	B made	B bader	2
C Abri	C madi	C badir	3
D Abro	D mado	D bador	4
E Abru	E madu	E badur	5
F Abras	F madas	F badan	6
G Abres	G mades	G baden	7
H Abris	H madis	H badin	8
I Abros	I mados	I badon	9
K Abrus	K madus	K badun	10
L Abran	L madan	L badas	11
M Abren	M maden	M bades	12
N Abrin	N madin	N badis	13
O Abron	O madon	O bados	14
P Abrun	P madun	P badus	15
Q Abral	Q madal	Q badal	16
R Abrel	R madel	R badel	17
S Abril	S madil	S badil	18
T Abrol	T madol	T badol	19
V Abrul	V madul	V badul	20
X Abrax	X madax	X badax	21
Y Abrex	Y medex	Y badex	22
Z Abrix	Z madix	Z badix	23
w A brox	w madox	w badox	24

Ff 3 A ca-

	P.III-1	P.III-2	P.III-3	P.III-4	P.III-5	P.III-6	P.III-7
a	abra	mada	badar	cadalan	pasa	adam	lora
b	abre	made	bader	cadalen	pase	adem	lore
c	abri	madi	badir	cadalin	pasi	adim	lori
d	abro	mado	bador	cadalon	paso	adom	loro
e	abru	madu	badur	cadalun	pasu	adum	loru
f	abras	madas	badas	cadalas	pasan	adas	loraff
g	abres	mades	bades	cadales	pasen	ades	loreff
h	abris	madis	badis	cadalis	pasin	adis	loriff
i	abros	mados	bados	cadalos	pason	ados	loroff
k	abrus	madus	badus	cadalus	pasun	adus	loruff
l	abran	madan	badan	cadalap	pasas	adan	loras
m	abren	maden	baden	cadalep	pases	aden	lores
n	abrin	madin	badin	cadalip	pasis	adin	loris
o	abron	madon	badon	cadalop	pasos	adon	loros
p	abrun	madun	badun	cadalup	pasus	adun	lorus
q	abral	madal	badal	cadalar	pasal	adar	loran
r	abrel	madel	badel	cadaler	pasel	ader	loren
s	abril	madil	badil	cadalir	pasil	adir	lorin
t	abrol	madol	badol	cadalor	pasol	ador	loron
v	abrul	madul	badul	cadalur	pasul	adur	lorun
x	abram	madax	badax	cadalax	pasar	adal	lorat
y	abrem	madex	badex	cadalex	paser	adel	loret
z	abrim	madix	badix	cadalix	pasir	adil	lorit
w	abrom	madox	badox	cadalox	pasor	adol	lorot

Polygraphia III: The Artificial Language Mimic



1 2 3 126

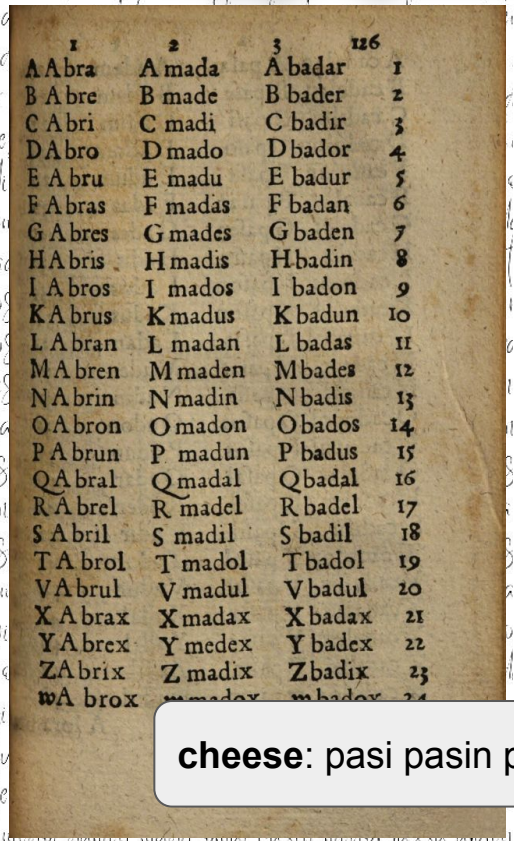
A Abra	A mada	A badar	1
B Abre	B made	B bader	2
C Abri	C madi	C badir	3
D Abro	D mado	D bador	4
E Abru	E madu	E badur	5
F Abras	F madas	F badan	6
G Abres	G mades	G baden	7
H Abris	H madis	H badin	8
I Abros	I mados	I badon	9
K Abrus	K madus	K badun	10
L Abran	L madan	L badas	11
M Abren	M maden	M bades	12
N Abrin	N madin	N badis	13
O Abron	O madon	O bados	14
P Abrun	P madun	P badus	15
Q Abral	Q madal	Q badal	16
R Abrel	R madel	R badel	17
S Abril	S madil	S badil	18
T Abrol	T madol	T badol	19
V Abrul	V madul	V badul	20
X Abrax	X madax	X badax	21
Y Abrex	Y medex	Y badex	22
Z Abrix	Z madix	Z badix	23
w A brox	w madox	w bado[illegible]	24

Ff

	P.III-1	P.III-2	P.III-3	P.III-4	P.III-5	P.III-6	P.III-7
a	abra	mada	badar	cadalan	pasa	adam	lora
b	abre	made	bader	cadalen	pase	adem	lore
c	abri	madi	badir	cadalin	pasi	adim	lori
d	abro	mado	bador	cadalon	paso	adom	loro
e	abru	madu	badur	cadalun	pasu	adum	loru
f	abras	madas	badas	cadalas	pasan	adas	loraff
g	abres	mades	bades	cadales	pasen	ades	loreff
h	abris	madis	badis	cadalis	pasin	adis	loriff
i	abros	mados	bados	cadalos	pason	ados	loroff
k	abrus	madus	badus	cadalus	pasun	adus	loruff
l	abran	madan	badan	cadalap	pasas	adan	loras
m	abren	maden	baden	cadalep	pases	aden	lores
n	abrin	madin	badin	cadalip	pasis	adin	loris
o	abron	madon	badon	cadalop	pasos	adon	loros
p	abrun	madun	badun	cadalup	pasus	adun	lorus
q	abral	madal	badal	cadalar	pasal	adar	loran
r	abrel	madel	badel	cadaler	pasel	ader	loren
s	abril	madil	badil	cadalir	pasil	adir	lorin
t	abrol	madol	badol	cadalor	pasol	ador	loron
v	abrul	madul	badul	cadalur	pasul	adur	lorun
					[illegible]sar	adal	lorat
					[illegible]ser	adel	loret
					[illegible]asir	adil	lorit
w	abrom	madox	badox	cadalox	pasor	adol	lorot

secret: abril madu badir cadeler pasu ador

Polygraphia III: The Artificial Language Mimic



1	2	3	126
A Abra	A mada	A badar	1
B Abre	B made	B bader	2
C Abri	C madi	C badir	3
D Abro	D mado	D bador	4
E Abru	E madu	E badur	5
F Abras	F madas	F badan	6
G Abres	G mades	G baden	7
H Abris	H madis	H badin	8
I Abros	I mados	I badon	9
K Abrus	K madus	K badun	10
L Abran	L madan	L badas	11
M Abren	M maden	M bades	12
N Abrin	N madin	N badis	13
O Abron	O madon	O bados	14
P Abrun	P madun	P badus	15
Q Abral	Q madal	Q badal	16
R Abrel	R madel	R badel	17
S Abril	S madil	S badil	18
T Abrol	T madol	T badol	19
V Abrul	V madul	V badul	20
X Abrax	X madax	X badax	21
Y Abrex	Y medex	Y badex	22
Z Abrix	Z madix	Z badix	23
wA brox			

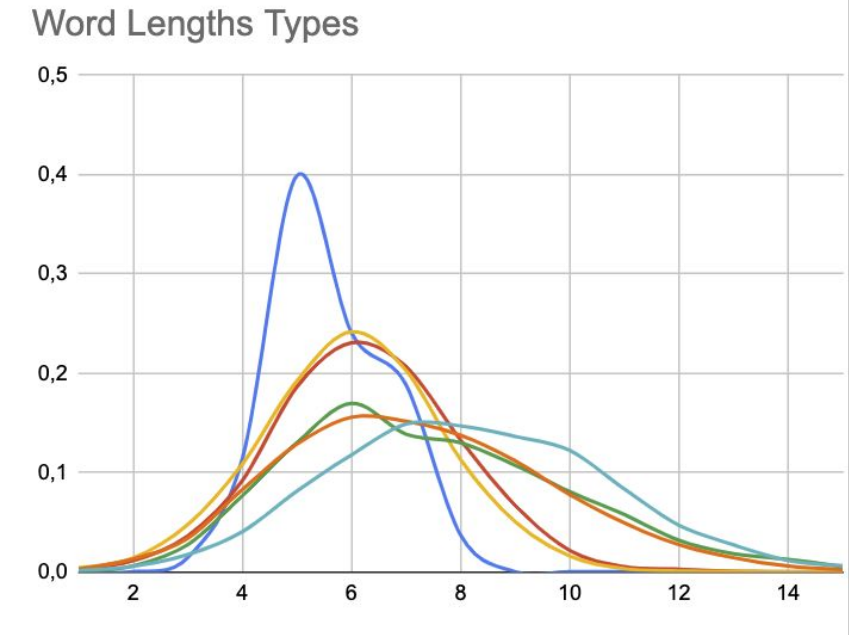
cheese: pasi pasin pasu pasu pasil pasu

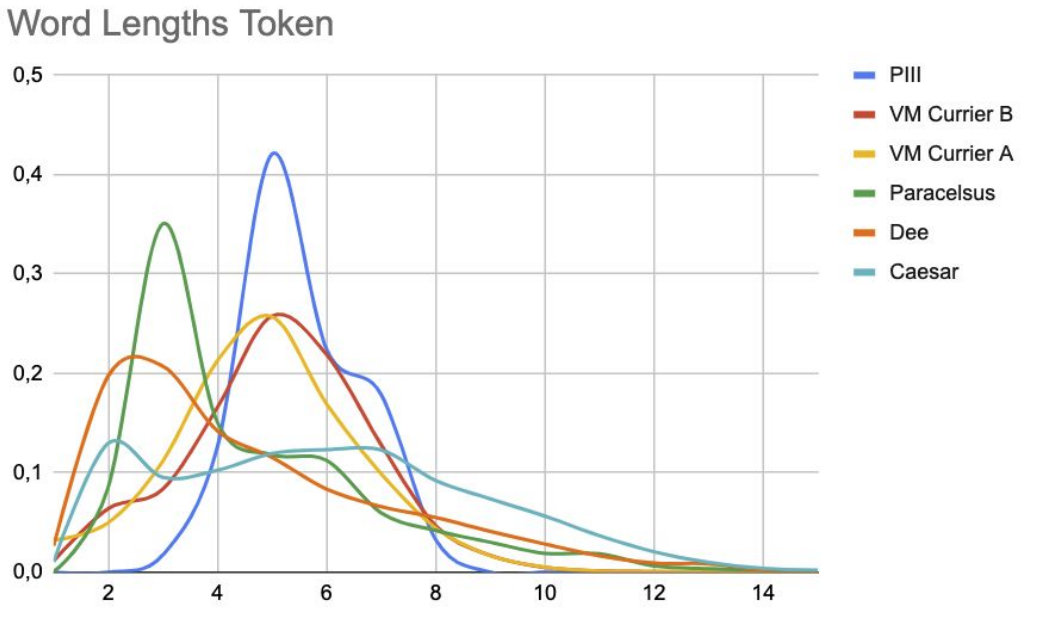
	P.III-1	P.III-2	P.III-3	P.III-4	P.III-5	P.III-6	P.III-7
a	abra	mada	badar	cadalan	pasa	adam	lora
b	abre	made	bader	cadalen	pase	adem	lore
c	abri	madi	badir	cadalin	pasi	adim	lori
d	abro	mado	bador	cadalon	paso	adom	loro
e	abru	madu	badur	cadalun	pasu	adum	loru
f	abras	madas	badas	cadalas	pasan	adas	loraff
g	abres	mades	bades	cadales	pasen	ades	loreff
h	abris	madis	badis	cadalis	pasin	adis	loriff
i	abros	mados	bados	cadalos	pason	ados	loroff
k	abrus	madus	badus	cadalus	pasun	adus	loruff
l	abran	madan	badan	cadalap	pasas	adan	loras
m	abren	maden	baden	cadalep	pases	aden	lores
n	abrin	madin	badin	cadalip	pasis	adin	loris
o	abron	madon	badon	cadalop	pasos	adon	loros
p	abrun	madun	badun	cadalup	pasus	adun	lorus
q	abral	madal	badal	cadalar	pasal	adar	loran
r	abrel	madel	badel	cadaler	pasel	ader	loren
s	abril	madil	badil	cadalir	pasil	adir	lorin
t	abrol	madol	badol	cadalor	pasol	ador	loron
v	abrul	madul	badul	cadalur	pasul	adur	lorun
				cadalax	pasar	adal	lorat
				cadalex	paser	adel	loret
				cadalix	pasir	adil	lorit
w	abrom	madox	badox	cadalox	pasor	adol	lorot

Experiments

- **Hypothesis:** The application of a cipher that works according to the principle of Polygraphia III produces a text with similar properties to a text in Voynichese.
- **Generate** texts by simulating encryptions with the PIII cipher.
- **Compare** the statistical properties of this texts to the properties of (medieval / early modern) texts of different languages
  - English: Dee – Elements
  - German: Paracelus – Paragranum
  - Italian: Dante – Divina Comedia
  - Voynichese

Results: Word Length Distributions





Results: Entropy Values

	Dee	Dante	Paracelsus	VMS A	VMS B	P.III big	P.III small
h_{words}	9.27	9.66	8.93	9.88	9.89	10.74	6.52
h_0	5.36	4.59	4.95	4.46	4.46	4.52	4.00
h_1	4.10	3.93	4.04	3.85	3.88	4.00	3.57
h_2	3.29	3.11	3.14	2.17	2.01	2.90	1.90
$h_1 - h_2$	0.81	0.82	0.90	1.68	1.87	1.10	1.67

Word entropy and the three character-based entropies: h_0 is h_{max}, h_1 is the entropy of single, h_2 of joint characters. The last column gives the difference between h_1 and h_2 (see Stallings 1998)

Results: Entropy Values

	Dee	Dante	Paracelsus	VMS A	VMS B	P.III big	P.III small
h_{words}	9.27	9.66	8.93	9.88	9.89	10.74	6.52
h_0	5.36	4.59	4.95	4.46	4.46	4.52	4.00
h_1	4.10	3.93	4.04	3.85	3.88	4.00	3.57
h_2	3.29	3.11	3.14	2.17	2.01	2.90	1.90
$h_1 - h_2$	0.81	0.82	0.90	1.68	1.87	1.10	1.67

Word entropy and the three character-based entropies: h_0 is h_{max}, h_1 is the entropy of single, h_2 of joint characters. The last column gives the difference between h_1 and h_2 (see Stallings 1998)

Results: Minimal Pairs and Repetitions

	Dee	Dante	Paracelsus	VMS A	VMS B	P.III big	P.III small
Minimal pairs	5.53	2.61	6.40	35.32	30.25	11.12	222.23
Minimal triplets	0.08	0.10	0	2.26	1.70	0.06	47.21
Word repeated	0.98	0	2.56	9.59	8.46	1.36	25.65

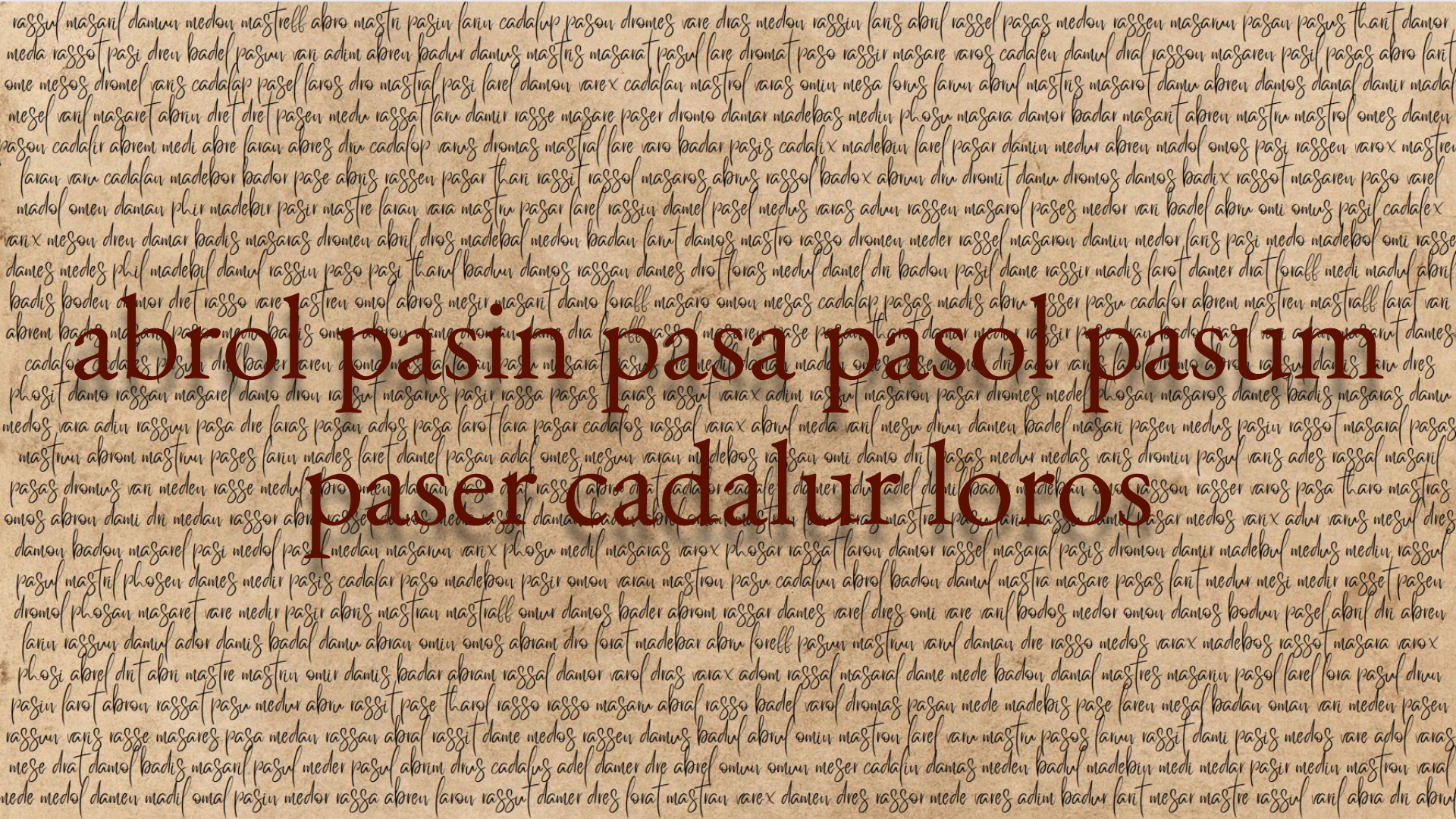
Proportions of minimal pairs resp. minimal triplets resp. word repetitions in all pairs resp. triplets of the texts.

What I don't claim (This one is for you, Reviewer 2)

- Trithemius is the author the VMS.
- The VMS is encoded in Latin.
- The VMS is definitely an encoded text.
- It is likely that the VMS was encoded with a codebook.
- I have made the best attempt yet to generate a text with the properties of the VMS.

But...

- Still a key question: "How could a text with the crude characteristics of the Voynich Manuscript have been created?"
- Previous attempts to explain a natural language or a known cipher as the basis for the generation were (imo) not convincing.
- Described methods for generating a meaningless text are (imo) comprehensible, but they ... only produce a meaningless text.
- Knowing that there were encryption methods in late medieval times that could produce a text with properties similar to a Voynichese text at least keeps alive the hope for a hidden information in the favorite manuscript of all of us.


abrol pasin pasa pasol pasum
paser cadalur loros

Literatur zur Nachbereitung / Vorbereitung

- Falls Sie das Paper zum Vortrag lesen wollen, finden Sie in ILIAS **Jürgen Hermes (2016)**: **Polygraphia III – The cipher that pretends to be an artificial language**. (Veröffentlichung steht noch aus, deswegen bitte noch nicht weitergeben)
- Erstellen Sie ein möglichst großes Korpus für Ihre Sprache und berechenen und visualisieren Sie einige Basiskennwerte. Genauere Anweisungen finden Sie in ILIAS.
- Für die Bearbeitung der Aufgabe haben Sie bis zum 8.1.2023 Zeit. Sie können dafür u.a. die nächste Unterrichtsstunde nutzen, die als Online-Sprechstunde stattfinden wird.