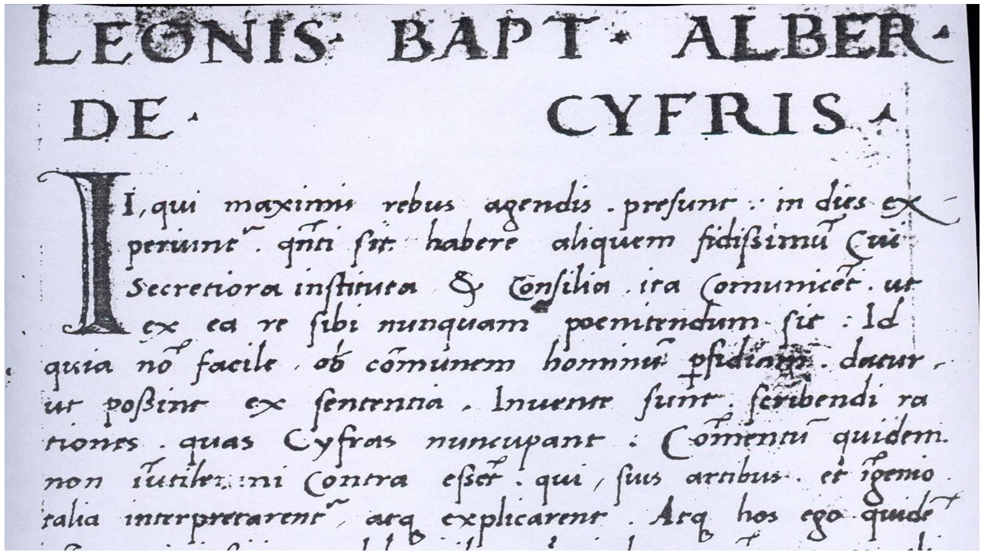
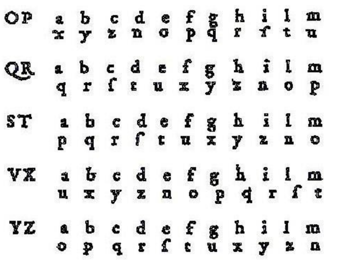


LEONIS BAPT. ALBER.
DE CYFRIS.

I, qui maximis rebus agendis presunt: in dies ex
periunt quanti sit habere aliquem fidissimu cui
Secretiora instituta & Consilia ita comunicet. ut
ex ea re sibi nunquam poenitendum sit: Id
quia no facile ob comunem hominu pfidiam datur,
ut possint ex sententia. Inuenti sunt scribendi ra
tiones quas Cyfras nuncupant: Comentu quidem
non inutile: ni contra esset. qui suis artibus et ingenio
talia interpretarentur atq explicarent. Atq hos ego quide



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

Mercoledì 6 Aprile 2022 – ore 16:00

Seminario Online via Zoom

Seminario congiunto UMI - Gruppo Crittografia e Codici e Iniziativa De Componendis Cifris - Gruppo MathCifris

Marzio Mula

Università di Trento

Random sampling of supersingular elliptic curves

Abstract: Many isogeny-based cryptographic protocols make use of supersingular elliptic curves over finite fields of large characteristic. The classic method for uniformly sampling such curves combines the reduction of suitable CM curves and random walks.

This strategy, though, has a major drawback which makes it unsuitable for cryptographic applications: the endomorphism ring of the output curve can be efficiently computed.

In this talk, we explain how the classic method works and why it reveals "too much" information about the output curve. We also investigate possible alternatives based on the Hasse invariant and division polynomials.

Link al seminario su Zoom

ID riunione: 818 1880 1871
Passcode: 786242

Referente	Associazione De Componendis Cifris	UMI
Norberto Gavioli	seminari@decifris.it segreteria@decifris.it matematica@decifris.it	seminariumi-cc@googlegroups.com