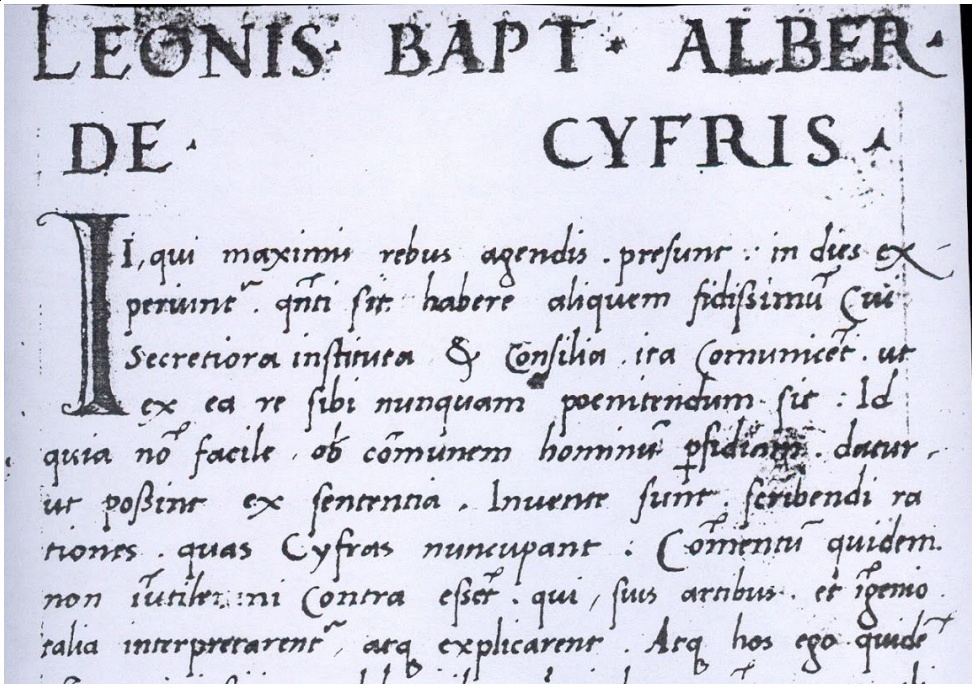
LEONIS BAPT. ALBER
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex
periuntur . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita communicet . ut
ex ea re sibi nunquam poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentũ quidem
non iutile . ni Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

MathCifris

OP	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	f	t	u
QR	a	b	c	d	e	f	g	h	i	l	m
	q	r	f	t	u	x	y	z	n	o	p
ST	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	f	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	f	t
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	f	t	u	x	y	z	n

Thursday 10th December 2020 – at 10:00 a.m.
Online Seminar via Zoom

Francesco Sica

Nazarbayev University, Kazakhstan

Fattorizzazione con indizi

Abstract: Voglio esporre un primo lavoro su relazioni fra le fattorizzazioni di numeri interi vicini e il conseguente impatto sulla crittografia a chiave pubblica.

In particolare, il risultato che presenterò stabilisce che per fattorizzare deterministicamente $N=pq$, un prodotto di due primi, in tempo $O(N^{\frac{1}{3}+\varepsilon})$ con $\varepsilon > 0$ piccolo a piacere, basta conoscere le fattorizzazioni dei $O(N^{\frac{1}{3}+\varepsilon})$ interi ad esso più vicini.

I metodi che uso sono analitici, il che costituisce un approccio nuovo per studiare il problema della fattorizzazione di interi.

Iscrizione all'evento online *da effettuare entro il 9 dicembre* tramite il seguente link:

click here

Gli iscritti riceveranno l'ID Zoom un'ora prima dell'inizio dell'evento.

Contact person: Norberto Gavioli

CONTATTI
Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it