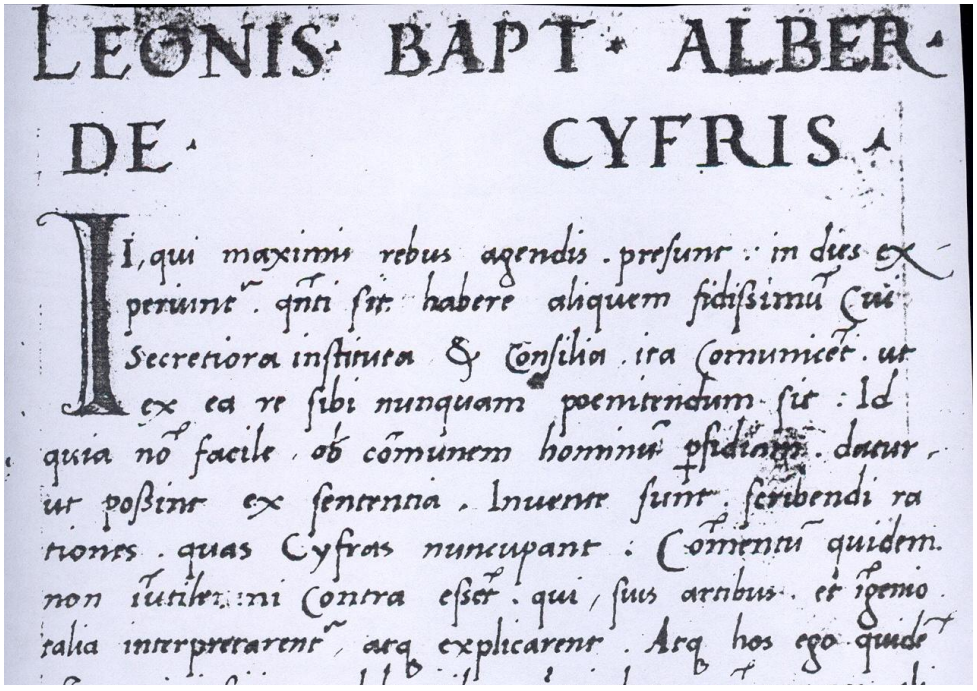
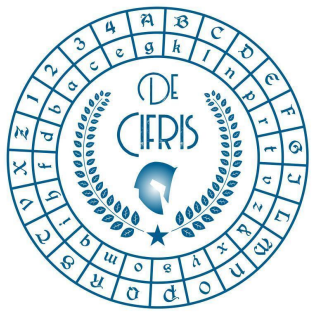
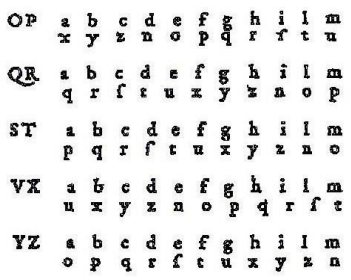

LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periunt q̃ti sit habere aliquem fidissimu cui
Secretiora instituta & Consilia ita communicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia nõ facile , ob cõmunem hominũ pfidiam . datur ,
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutilem Contra esset . qui , suis artibus . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

MathCifris

UMI




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 8th April 2021 – at 3:00 p.m.

Online Seminar via Zoom

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

Emmanuela Orsini

COSIC, KU Leuven, Belgium

Post-quantum secure oblivious transfer

Abstract: Oblivious Transfer (OT) is a fundamental primitive in modern cryptography, that has been proved to be complete for both two-party and multiparty computation. It has been used as a building block in many cryptographic protocols and has a number of interesting applications. In this talk, we start by introducing OT, giving some basic definitions, notion of security and showing some recent applications. Then, we will consider few OT constructions based on cryptographic assumptions that are supposed to be secure against post-quantum attacks. We conclude with a discussion on their efficiency and security.

Iscrizione all'evento online *da effettuare entro il 7 aprile* 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
matematica@decifris.it