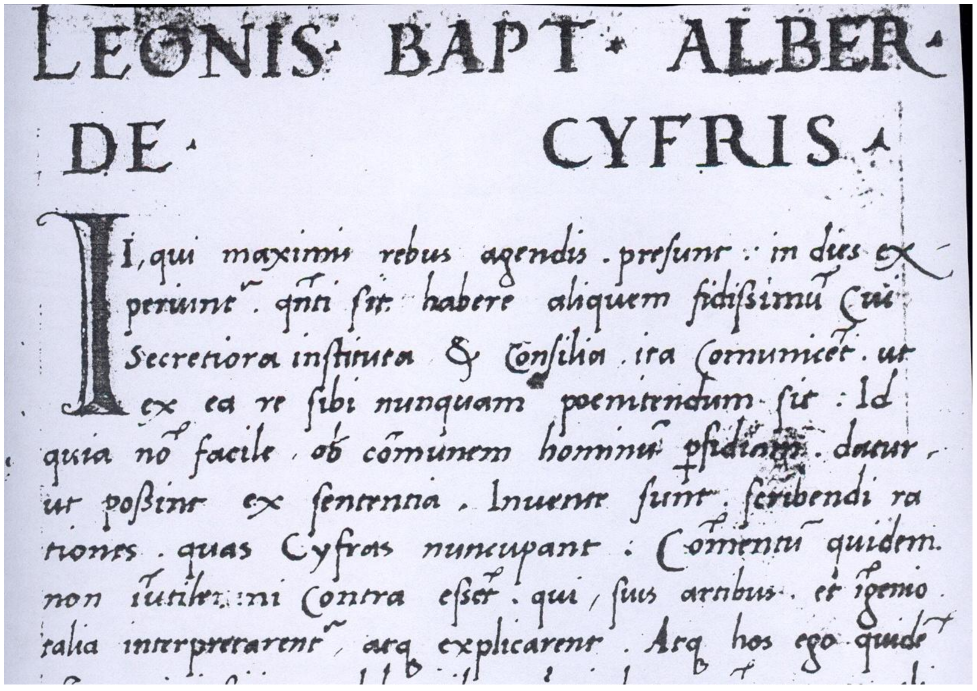

LEONIS· BAPT· ALBER·
DE· CYFRIS·
I, qui maximis rebus agendis . preſunt : in dies ex
periunt . quanti ſit habere aliquem fidiſsimu cui
Secretiora inſtituta & Conſilia . ita comunicet . ut
ex ea re ſibi nunquam poenitendum ſit : Id
quia no facile . ob comunem hominu perfidiam . datur .
ut poſsint ex ſententia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

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Monday 7th June 2021 – at 10:00 a.m.
Online Seminar via Zoom

Marco Calderini

University of Bergen

Permutation groups and security of block ciphers

Abstract: In 1975, Coppersmith and Grossman considered a set of functions that can be used to define a block cipher and, by studying the permutation group generated by those, they opened the way to a new branch of research focused on group-theoretical properties which can reveal weaknesses of the cipher itself.

In this talk, we will explain the relationship between permutation groups and security of block ciphers. We will present some results that characterize the properties of the components of a block cipher, and of the corresponding permutation group, which guarantee security against known algebraic attacks.

Iscrizione all'evento online *da effettuare entro il 6 giugno* tramite il seguente link:

click here

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

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

segreteria@decifris.it
seminari@decifris.it