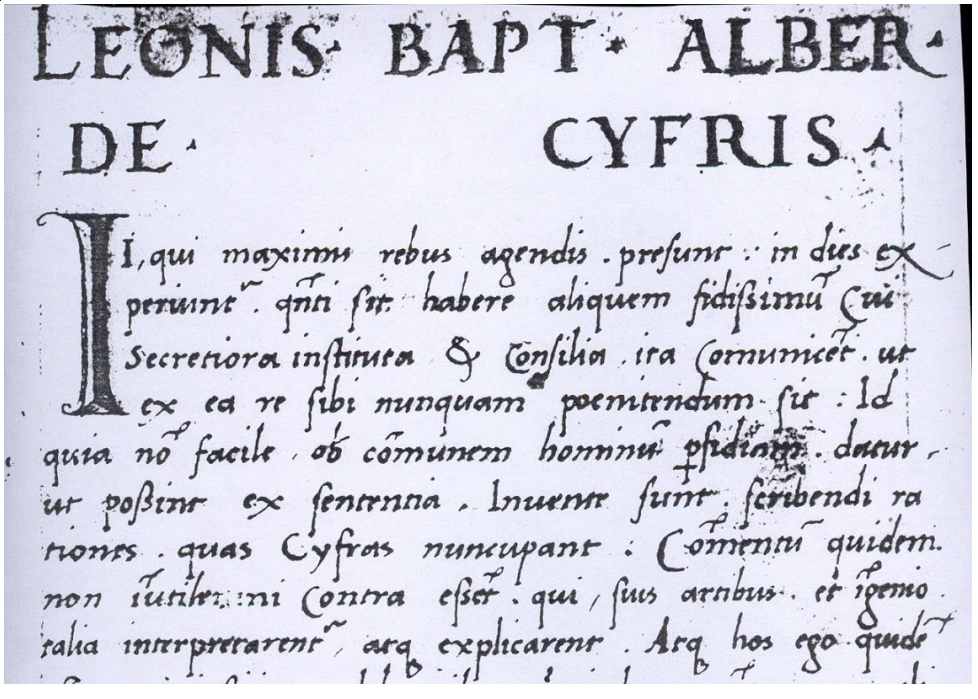
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periunt . 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 , 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 25th January 2021 – at 11:00 a.m.
Online Seminar via Zoom

Daniele Venturi
Università di Roma - La Sapienza

Immunizing Cryptographic Primitives against Complete Subversion

Abstract: In this talk I will review recent work on immunizing cryptographic primitives whose implementation might have been subverted in a surreptitious manner. This topic recently gained momentum in the cryptographic community due to the revelations by Edward Snowden about the NSA tweaking the Dual EC PRG standard with the purpose of mass surveillance.

Iscrizione all'evento online *da effettuare entro il 24 gennaio* 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