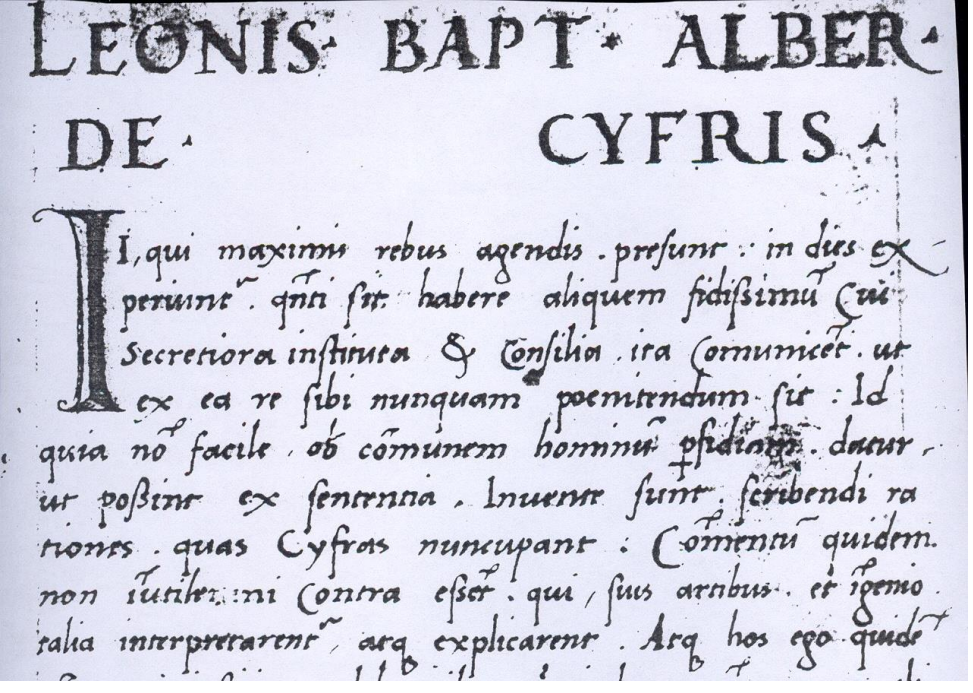
LEONIS BAPT. ALBER
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex
periuntur . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita Comunicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia nõ facile , ob cõmunem hominũ ꝓfidiam . datur ,
ut possint ex sententia . Inuenti sunt . scribendi ra
tiones . quas Cyfras nuncupant : Comentũ quidem
non iutilissimi Contra esset . qui , suis armis . et igno
ralia interpretarent , atq explicarent . Atq hos ego quide

De Cifris Mediolanensibus

Tuesday 12th October 2021 – at 15:00

Online Seminar via Zoom

Enrico Zimuel

Principal Software Engineer - Elastic

Introduzione alle problematiche nell'implementazione dei sistemi crittografici

Abstract: In questo presentazione verranno introdotte le principali problematiche legate all'implementazione degli algoritmi crittografici. Tra gli argomenti che verranno presentati: wiping state, swap file, key derivation, data integrity, randomness, side-channel attack, etc. Inoltre verranno presentate alcune delle librerie open source più utilizzate, con alcuni esempi in NaCl e libsodium.

Iscrizione all'evento online *da effettuare entro l'11 ottobre* tramite il seguente link:

click here

Gli iscritti potranno accedere all'evento attraverso il seguente link Zoom
https://us02web.zoom.us/j/9021141143?pwd=ZWZrZElsVmxibWFSaGNGbHFrczBndz09

Contact person: Andrea Visconti, Università degli Studi di Milano, Dip.to di Informatica

CONTATTI
Iniziativa Nazionale De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it