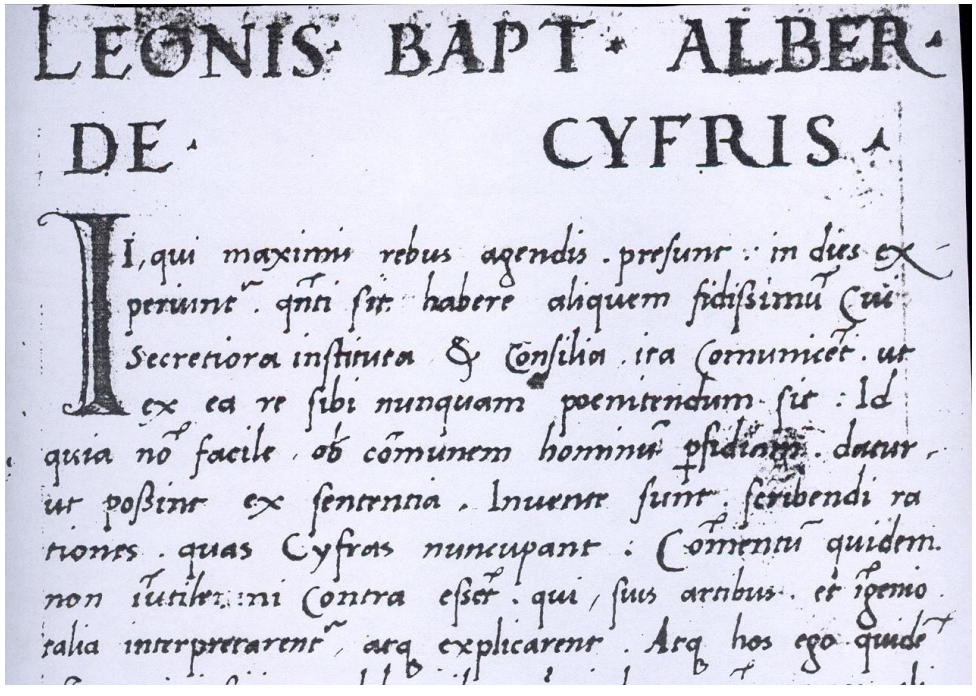
LEONIS BAPT ALBER
DE CYFRIS
II, qui maximis rebus agendis . presunt : in dies ex
perirent . quis sit habere aliquem fidissimu Cui
secretiora instituta & Consilia ita Comunicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia no facile . ob cōmunem hominū ofidiam . dicur
ut possint ex sententia . Inuenit sunt . scribendi ra
tiones . quas Cyfras nuncupant . Comentu quidem
non iutilem . ni Contra esset . qui , suis artibus . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Schola Latina

Wednesday 13th April 2022 – at 15.00
Conference

Marco Cesati

Università di Roma Tor Vergata

A new idea for RSA backdoors

Abstract: We present a new method to inject backdoors in RSA and other cryptographic primitives based on the Integer Factorization problem for balanced semi-primes. The method relies on mathematical congruences among the factors of the semi-primes modulo a large prime number, which acts as a "designer key" or "escrow key". In particular, two different backdoors are proposed, one targeting a single semi-prime and the other one a pair of vulnerable semi-primes.

Dipartimento di Matematica e Fisica - Università Roma Tre
Aula 311 - Edificio C - Largo San Leonardo Murialdo 1
https://bit.ly/3wViuZK

Contact person: Marco Pedicini

CONTATTI

Iniziativa De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it