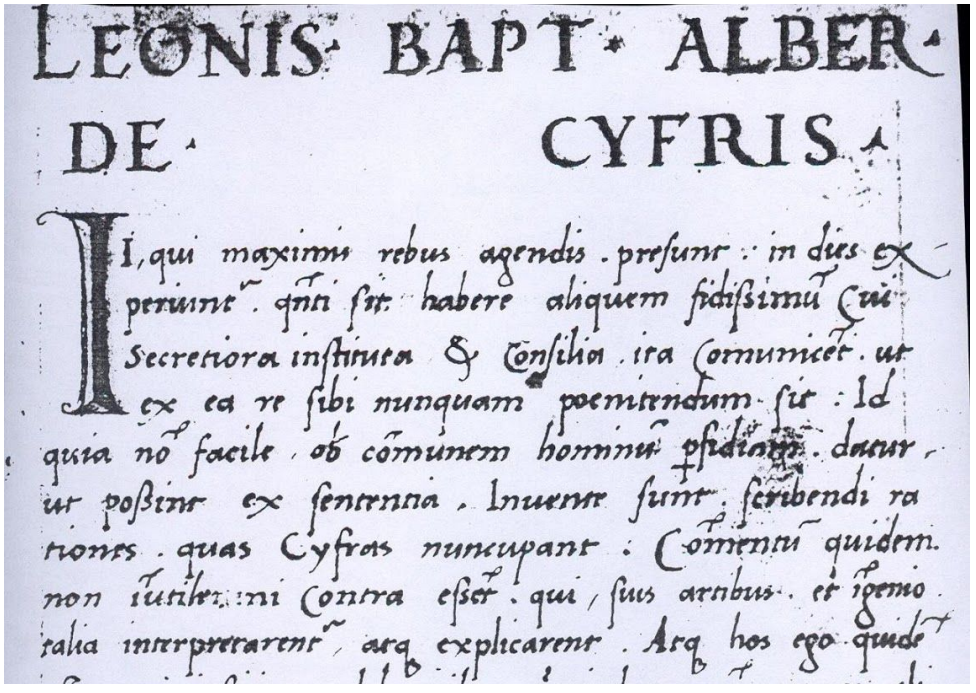
LEONIS BAPT ALBER
DE CYFRIS
Il, qui maximis rebus agendis . presunt : in dies ex
periuntur . quti sit habere aliquem fidissimu cui
Secretiora instituta & consilia ita comunicet . ut
ex ea re sibi nunquam poenitendum sit : Id
quia no facile . ob comunem hominu pfidiam . datur
ut possint ex sententia . Inuenta sunt . scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutile : ni Contra esset . qui , suis artibus . et igno
ralia interpretarent , atq explicarent . Atq hos ego quide

De Cifris

Schola Latina

DIPARTIMENTO DI INFORMATICA

SAPIENZA UNIVERSITÀ DI ROMA

disim

DE CIFRIS

ROMA TRE UNIVERSITÀ DEGLI STUDI

DME

Monday 27th January 2020 – at 2:00 p.m.
Roma Tre University
Department of Mathematics and Physics

ANDREA VISCONTI

Università di Milano

SSL/TLS cryptographic protocols and their weaknesses

Abstract: SSL/TLS are cryptographic protocols widely used over the Internet. In order to protect sensitive data, SSL and TLS provide authentication, integrity and confidentiality between clients, servers and applications. In the last 20 years, these protocols have undergone significant changes to cope with the ongoing attacks published in the literature. In this talk, we will (a) introduce SSL/TLS protocols, (b) explain the attacks known in the literature and finally (c) present the countermeasures adopted.

Contact person: Marco Pedicini

Address: Room M3, Building "Polo Aule", Roma Tre University
Lungotevere Dante 376, Roma

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it