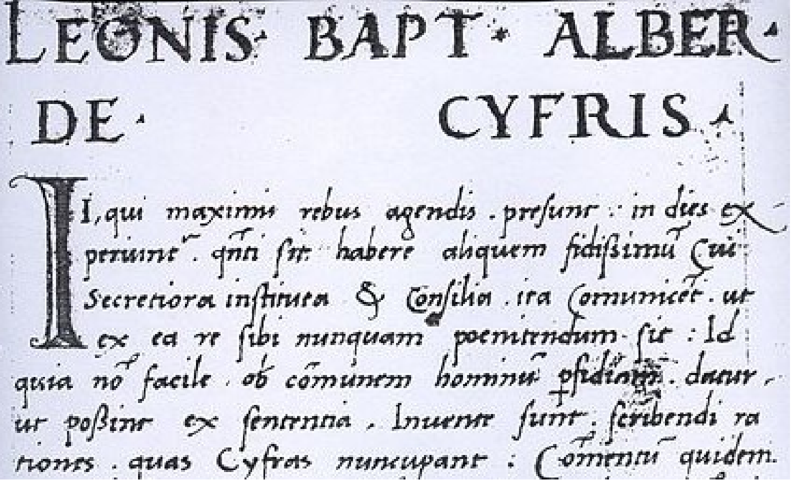

LEONIS BAPT· ALBER·
DE· CYFRIS·
II, qui maximis rebus agendis. præſunt: in dies ex
periunt. quãti ſit habere aliquem fidiſsimũ cui
Secretiora inſtituta & Conſilia. ita cõmunicet. ut
ex ea re ſibi nunquam pœnitendum ſit: Id
quia nõ facile. ob cõmunem hominũ perfidiam. datur,
ut poſsint ex ſententia. Inuentæ ſunt. ſcribendi ra
tiones. quas Cyfras nuncupant: Cõmentũ quidem.

De Cifris Augustae Taurinorum

quadrans FOUNDATION

Telsy

POLITECNICO DI TORINO
Dipartimento di Scienze Matematiche G.L. Lagrange

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Thursday, 21 May 2020 – at 14.30
Streaming availbale at http://tiny.cc/crypto_webinar

Michela Ceria
University of Milan

Why you should not even think to use Ore algebras in Cryptography

(Joint work with T.Mora and A. Visconti)

Abstract: Burger and Heinle, in 2014 , specialized the generalized Stickel's Diffie-Hellman protocols to the special setting of multivariate Ore extensions. In this talk, we discuss an extension to the setting of iterated Ore extensions with power substitutions and we propose a cryptanalysis, based on Buchberger reduction and left/right divisibility.

For Information: danilo.bazzanella@polito.it, fabio.fiori@food-chain.it, guglielmo.morgari@telsy.it, nadir.murru@polito.it, lea.terracini@unito.it.

CONTATTI
Associazione De Componendis Cifris
direttore@decifris.it, segreteria@decifris.it