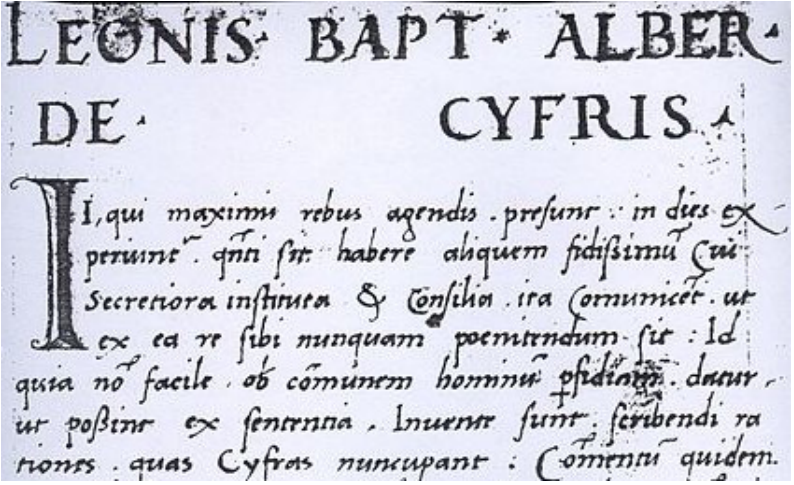

De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

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

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Monday, 19 April 2021 - 16:00

Online webinar on the Zoom platform
http://tiny.cc/crypto_webinar

Roberto La Scala
Università di Bari

Cifrari ed equazioni alle differenze

Abstract: Molti cifrari a flusso o a blocchi di interesse applicativo quali Trivium, Keeloq, sistemi di LFSR con combinatore (E0 di Bluetooth)... possono essere modellizzati come sistemi di equazioni esplicite alle differenze su campi finiti. Tali sistemi infatti determinano l'evoluzione nel tempo dei registri interni di questi "cifrari alle differenze". L'utilizzo della teoria formale delle equazioni alle differenze permette lo studio di alcune proprietà fondamentali di questi cifrari, quali ad esempio la loro invertibilità, e la corretta definizione di attacchi algebrici ai fini della stima della loro sicurezza. Tale modellizzazione e la corrispondente crittanalisi permette quindi lo sviluppo di nuovi cifrari.

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

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