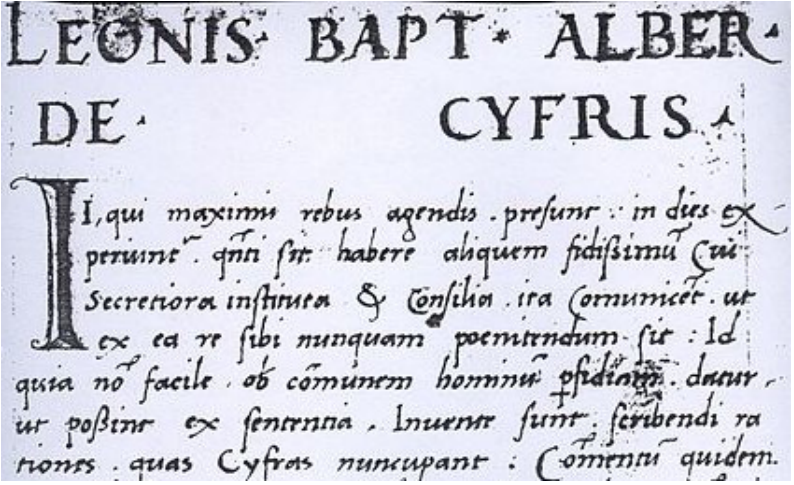

De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

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

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Friday, 26 March 2021 - 14:30

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

Francesco Stocco
Telsy

A theoretical approach to Shor's Algorithm and Quantum Bits

Abstract: In 1994, Peter W. Shor showed how to factor integers and to solve discrete logarithms in polynomial time, assuming a suitable quantum computer were available. In this seminar we will give a quick overview of the mathematical formalism behind quantum bits, providing the audience with the basic knowledge in quantum computing needed to approach Shor's algorithm for period finding. Given two coprime positive integers N and a, the algorithm computes the period of the function f(x)=ax mod N. The mathematical interpretation of the algorithm, in the framework of Hidden Subgroup Problem (HSP), will be the main subject of the talk. Furthermore, we will briefly show a couple of strategies to break RSA's protocol applying period finding.

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