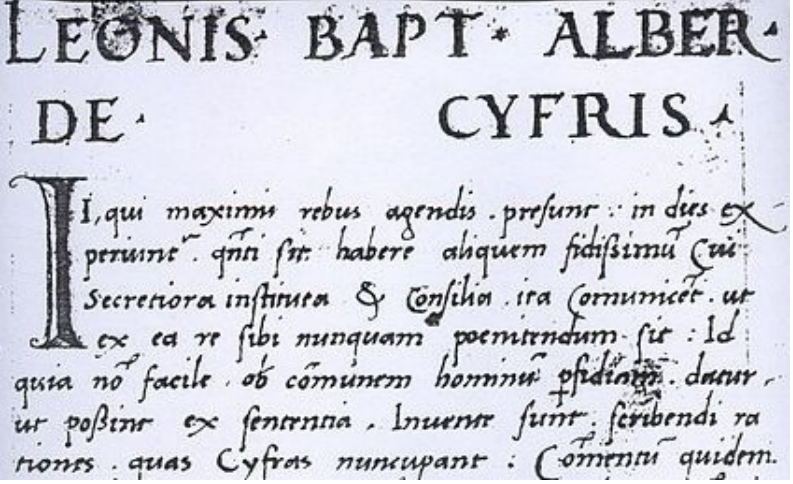

De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

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

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Friday, 17 July 2020 – at 14.30
Streaming availbale at http://tiny.cc/crypto_webinar

Giordano Santilli
University of Trento

An investigation on Integer Factorization applied to Public Key Cryptography

Abstract: Among the difficult number-theoretic problems, the Integer Factorization Problem (IFP) is one of the most famous: given a composite integer number, recovering its factors is commonly believed to be hard. Many asymmetric algorithms such as RSA found their mathematical security on IFP.
In this talk I will present two different approaches to attempt to solve IFP presented in my Ph.D. thesis: the first one is a joint work with prof. Massimiliano Sala on the remainders of a fixed integer for successive moduli, which can be seen as a second-degree interpolating polynomial of three initial monotonic consecutive remainders. This result leads to the creation of a formula that computes all the remainders, however I will show that the problem of finding a root for this formula is equivalent to IFP.
The second part of the talk will be devoted to describing a possible generalization of the GNFS protocol: starting from two simple quadratic extensions of the rational numbers it is possible to define the biquadratic extension of degree 4 that contains both. We will prove that the first-degree prime ideals in the smaller extensions may be used to generate the same kind of ideals in the larger one and, adding some additional hypotheses, we will show that also the converse is true. Using this fact, it is possible to speed up the search for smooth principal ideals in the biquadratic extension in terms of its factorization in the smaller quadratic extensions. This second part comes from a joint work with prof. Massimiliano Sala and Ph.D. Daniele Taufer.

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