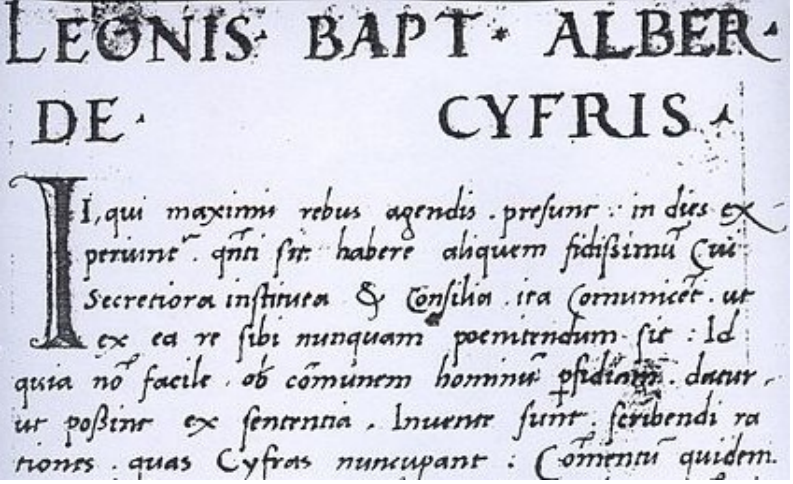
LEONIS BAPT. ALBER
DE CYFRIS

De Cifris Augustae Taurinorum

Wednesday, 25 September 2019 – at 14.30
Aula S, Università di Torino
Dipartimento di Matematica, Via Carlo Alberto 10

Andrea Visconti
Università di Milano

Key derivation function: an essential (and usually transparent) component of real-world applications

Abstract: A key-derivation function (KDF) is a component of cryptographic systems used to provide passwords or more generally to obtain secret cryptographic keying material. Several applications use KDFs to derive one or more cryptographically strong secret keys, stretching keys into longer ones or getting keys of a required format. These functions are usually transparent to the users, who enjoy the benefits without being aware of how they are accomplished. In this talk will be (a) introduced the main ideas underlying the KDFs, (b) described a number of real-world applications in which KDFs are involved and (c) presented the current state of the art.

For Information: 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