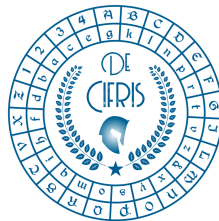


LEONIS BAPT ALBER
DE CYFRIS

I, qui maximis rebus agendis. presunt. in dies ex
perunt. qnti sit. habere aliquem fidissimū Cui
Secretiora instruta & Consilia. ita Cornunicet. ut
ex ea re sibi nunquam poenitendum sit. Id
quia nō facile. ob cōmunem hominū pfidiam. datur
ut possint ex sententia. Inuenti sunt. scribendi ra
tiones. quas Cyfras nuncupant. Cōmentū quidem.

De Cifris Augustae Taurinorum



POLITECNICO
DI TORINO

Dipartimento
di Scienze Matematiche
G.L. Lagrange



DIPARTIMENTO
DI MATEMATICA
GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Friday, 5 February 2021 - ore 14:30

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

Carlo Sanna
Politecnico di Torino

Introduction to Multivariate Cryptography

Abstract: Multivariate Cryptography is a Public-Key Cryptography that builds its trapdoors on the problem of solving multivariate polynomial systems over a finite field. Currently, two signature schemes in the NIST Post-Quantum Cryptography Standardization Process are based on Multivariate Cryptography: Rainbow (Round 3 Finalist) and GeMSS (Alternate Candidate). This introductory talk shows: the motivation behind Multivariate Cryptography; the basic principles and design of a Multivariate Public Key Cryptosystem; the possible attacks; the Unbalanced Oil and Vinegar scheme; and the Hidden Field Equations scheme.

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