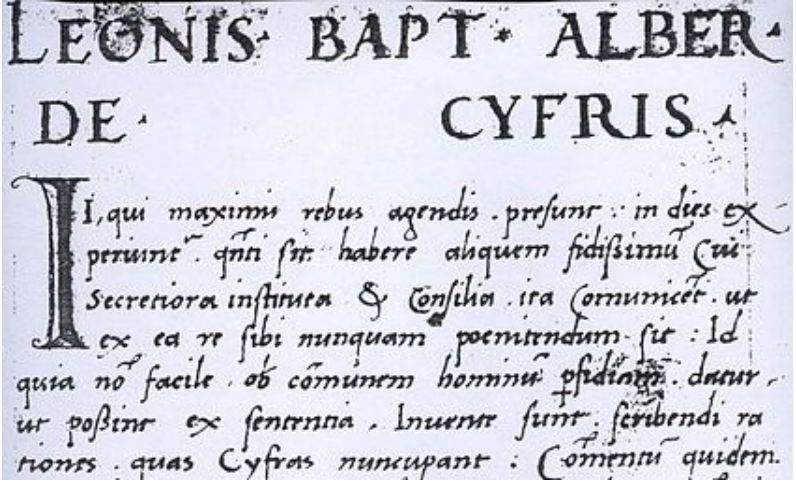

De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

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

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Tuesday 20 September 2022 - 14:30

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

Veronica Cristiano
Telsy SpA

Cryptographic aspects in WireGuard, a modern VPN protocol

Abstract: A Virtual Private Network (VPN) protocol establishes a secure "tunnel" between two parties on the Internet, providing a private encrypted channel while using public networks. Several VPN protocols have been developed and are widely used, such as IPsec and OpenVPN. In this talk, we present WireGuard, a state-of-the-art VPN protocol that achieves better performances and improved ease of use. After an introduction to VPNs and the network settings, we are going to explore WireGuard's Authentication Key Exchange protocol, based on the Noise framework, and discuss the cryptographic properties achieved.

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