DE CYFRIS. I qui maximi rebus agendis presunt in dies ex peruint ann su habere aliquem sidissimu cui secretiora instituta & Considio ita comunicet ut ex ea re sibi nunquam poemitendum sir ild quia no facile ob comunem homnus osidiani daeur ur possint ex sentenna Inuente sunt seribendi ra trones quas Cyfras nuncupant: Comentu quidem.

De Cifris Augustae Taurinorum









Friday, 22 November 2019 – at 15.00 Aula 2, Università di Torino Dipartimento di Matematica, Via Carlo Alberto 10

Stefano Barbero Politecnico di Torino

An overview on cryptanalysis of ARX ciphers

Abstract: We present some features of block ciphers based on the three operations: addition mod 2n, rotation and XOR (ARX ciphers) and the main cryptanalitic attacks obtained by developing the methods underlying differential cryptanalysis. We focus on the recent tecnique of rotational-XOR differential cryptanalysis giving some ideas of this attack

and its application to SPECK 32/64.

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