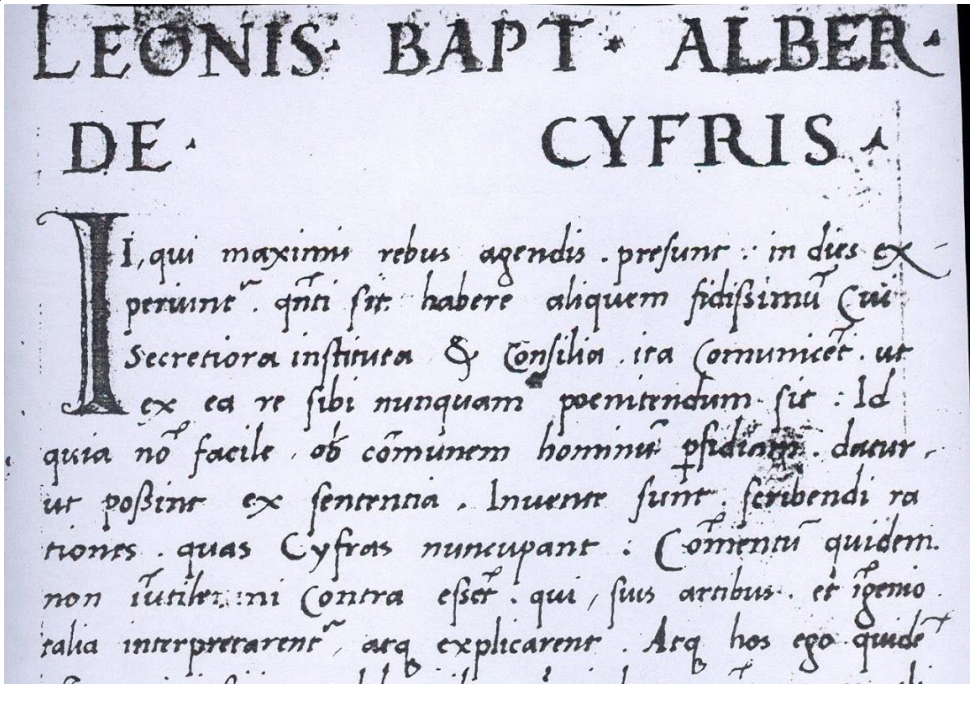
LEONIS BAPT. ALBER-
DE CYFRIS

Il qui maximis rebus agendis presunt: in dies ex-
periunt quanti sit habere aliquem fidissimu cui
Secretiora instituta & Consilia ita Comunicet. ut
ex ea re sibi nunquam poeniteudum sit: Id
quia no facile ob comunem hominu pfidiam. datur
ut possint ex sententia. Inuenta sunt scribendi ra
tiones. quas Cyfras nuncupant: Comentu quidem.
non iutilem. ni Contra esset. qui, suis artibus. et igemo
talia interpretarent, atq explicarent. Atq hos ego quide

De Cifris Schola Latina

DIPARTIMENTO DI INFORMATICA
SAPIENZA UNIVERSITÀ DI ROMA
disim

DE CIFRIS

ROMA TRE UNIVERSITÀ DEGLI STUDI
DMF

Wednesday 26th February 2020 – at 3:00 p.m.
Roma Tre University
Room 311, Department of Mathematics and Physics

ROBERTO CIVINO

Università de l'Aquila

Differential attacks using alternative operations

Abstract: *Block ciphers and their security are the main subjects of this seminar, where it is described the impact of differential cryptanalysis, a powerful statistical attack against block ciphers, when operations different from the one used to perform the key addition are considered on the message space. It is proven that when an alternative difference operation is carefully designed, a cipher that is proved secure against classical differential cryptanalysis can instead be attacked using this alternative difference.*

Contact person: Marco Pedicini

Address: Room 311, Building C, Roma Tre University
Largo San Leonardo Murialdo 1, Roma

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it