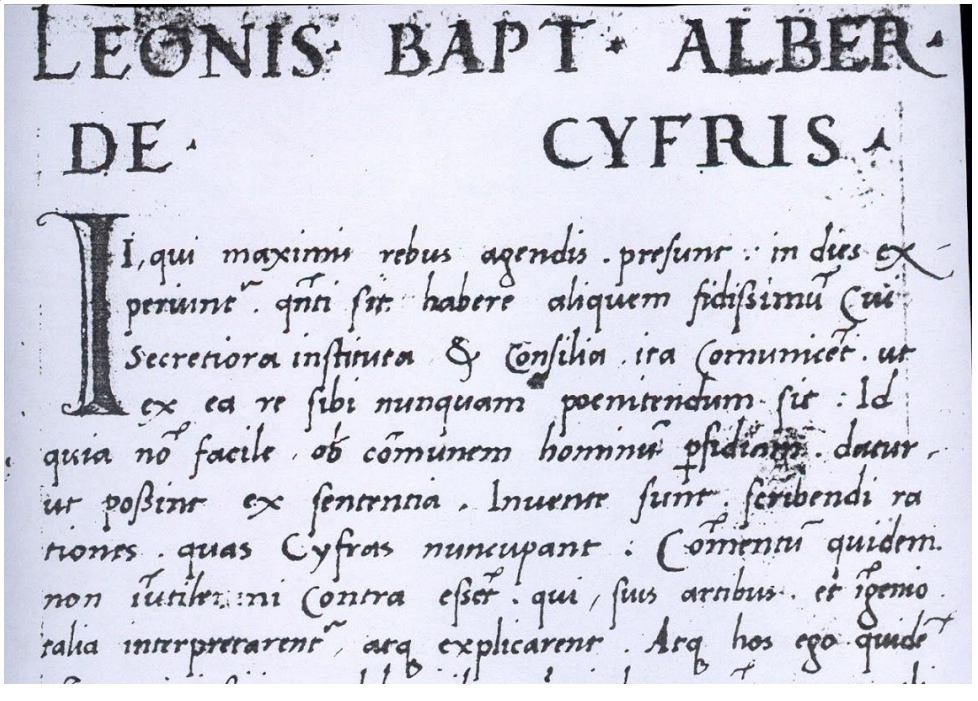
LEONIS BAPT. ALBER-
DE CYFRIS.

II, qui maximis rebus agendis . presunt : in dies ex-
periunt . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita communicet . ut
ex ea re sibi nunquam poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ ꝓfidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutilissimi Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Schola Latina

DIPARTIMENTO DI INFORMATICA
SAPIENZA UNIVERSITÀ DI ROMA
disim

DE CIFRIS

ROMA TRE UNIVERSITÀ DEGLI STUDI
DMF

Thursday 21st November 2019 – at 11:00 a.m.
Department of Mathematics and Physics
Room 211, Roma Tre University

LORENZO GRASSI

IAIK, University of Technology of Graz

SYMMETRIC CRYPTOGRAPHY: DESIGN & CRYPTANALYSIS

Abstract: Block ciphers are certainly among the most important cryptographic primitives. Their design and analysis are well advanced, and with today's knowledge designing a secure block cipher is a problem that is largely considered solved.

Since it is not possible to prove mathematically the security of a symmetric scheme, the security of symmetric cipher is always against specific attacks. In this presentation, we focus on "differential cryptanalysis", probably one of the most powerful attack in symmetric cryptography. It was introduced by Biham and Shamir in the late 1980s in order to break full DES. After a brief introduction using SPN toy ciphers, we analyze how the "Wide Trail Design Strategy" can be exploited in order to guarantee security against such attack.

Contact person: Marco Pedicini

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it