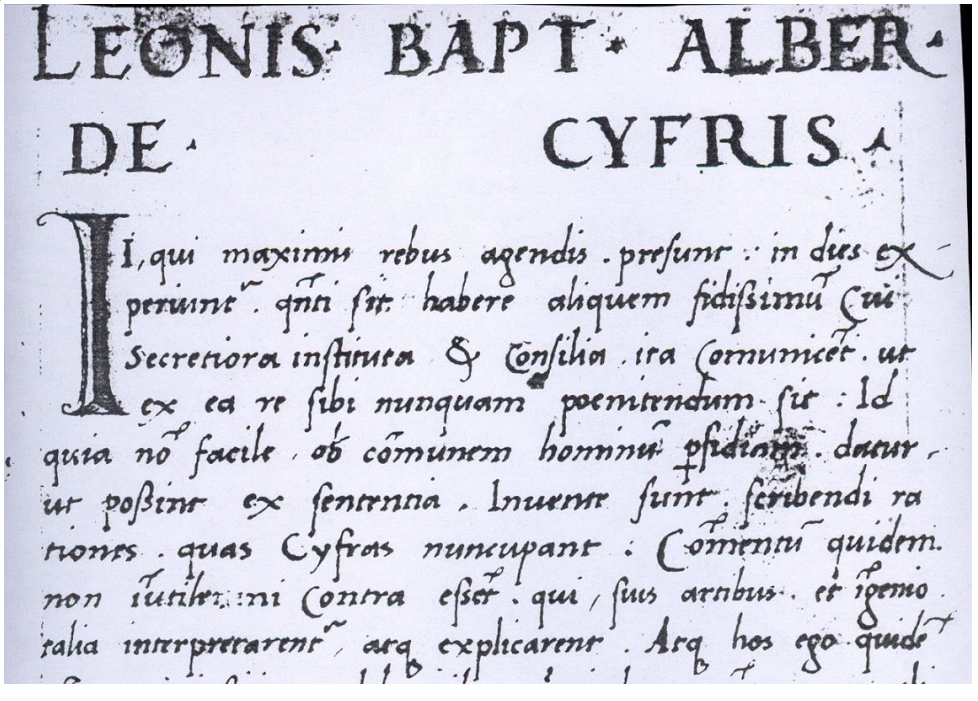
LEONIS BAPT. ALBER-
DE CYFRIS

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 ꝓsidiatũ . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutilem 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

ROMA TRE UNIVERSITÀ DEGLI STUDI

Friday 22nd November 2019 – at 10:00 a.m.
Department of Mathematics and Physics
Room 311, Roma Tre University

LORENZO GRASSI

IAIK, University of Technology of Graz

CRYPTANALYSIS OF AES: NEW RESULTS

Abstract: AES is the best known and most widely used secret key cryptosystem, and determining its security is one of the most important problems in cryptanalysis. Since no known attack can break the full AES significantly faster than via exhaustive search,

researchers had concentrated on attacks which can break reduced round versions of AES.

Recently, new secret-key distinguishers have been presented for 5- and 6-round AES. In this presentation, we mainly focus on the "multiple-of-8" property (presented at Eurocrypt'17) and on "mixture differential" cryptanalysis (presented at FSE/Tosc'19). These are the first secret-key distinguishers on 5-round AES which are independent of the secret key, improving over a 20 year old result on 4 rounds.

Contact person: Marco Pedicini

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it