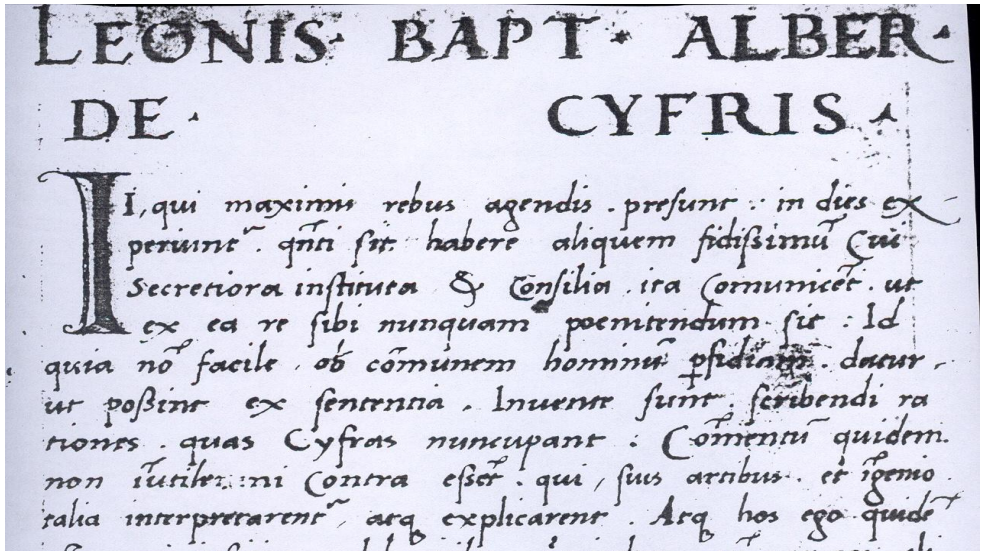
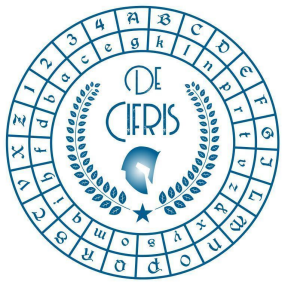
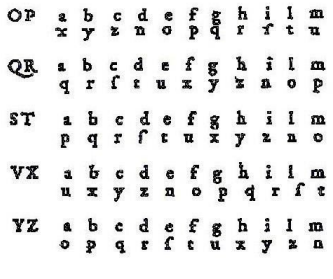

LEONIS BAPT. ALBER.
DE CYFRIS.

II, qui maximis rebus agendis præsunt : in dies ex
periuntur, quàm sit habere aliquem fidissimum Cui
Secretiora instituta & Consilia ita communicet, ut
ex ea re sibi nunquam pœnitendum sit : Id
quia nō facile ob cōmunem hominū ꝓfidiam datur,
ut possint ex sententia. Inuenta sunt scribendi ra
tiones, quas Cyfras nuncupant : Cōmentū quidem
non futile, ni Contra esset, qui suis armis, et ingemo
dalia interpretarent, atq; explicarent. Atq; hos ego quide




OP a b c d e f g h i l m
x y z n o p q r s t u
QR a b c d e f g h i l m
q r s t u x y z n o p
ST a b c d e f g h i l m
p q r s t u x y z n o
VX a b c d e f g h i l m
u x y z n o p q r s t
YZ a b c d e f g h i l m
o p q r s t u x y z n

Mercoledì 7 Luglio 2021 – ore 16:00

Seminario Online via Zoom

Seminario congiunto UMI - Gruppo Crittografia e Codici e Iniziativa De Componendis Cifris - Gruppo MathCifris

Roberto La Scala

Università degli Studi di Bari Aldo Moro

Cifrari ed Equazioni alle Differenze

Abstract: Molti cifrari a flusso o a blocchi di interesse applicativo quali sistemi di LFSR con combinatore (E0 di Bluetooth), Trivium, Keeloq, etc possono essere modellizzati come sistemi di equazioni esplicite alle differenze su campi finiti. Tali sistemi infatti determinano l'evoluzione nel tempo dei registri interni di questi "cifrari alle differenze".

L'utilizzo della teoria formale delle equazioni alle differenze permette lo studio di alcune proprietà di questi cifrari, quali la loro invertibilità e periodicità. Queste proprietà sono essenziali alla corretta definizione di attacchi algebrici generali ai cifrari alle differenze e quindi alla stima della loro sicurezza. Tale modellizzazione e la corrispondente crittanalisi può permettere quindi lo sviluppo di nuovi cifrari applicabili.

Link al seminario su Zoom

ID riunione: 837 4634 3305
Passcode: 936009

Referente	Associazione De Componendis Cifris	UMI
Norberto Gavioli	seminari@decifris.it segreteria@decifris.it matematica@decifris.it	seminariumi-cc@googlegroups.com