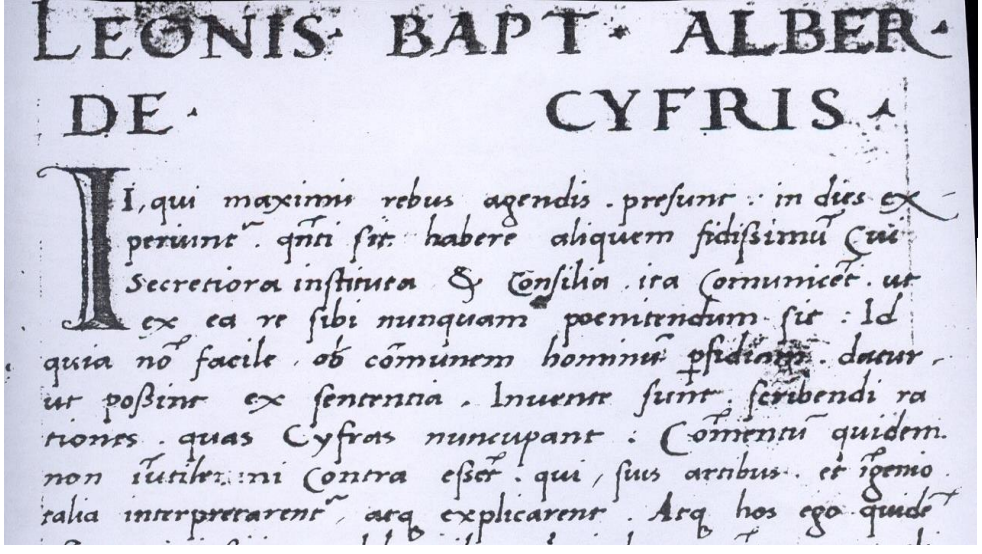
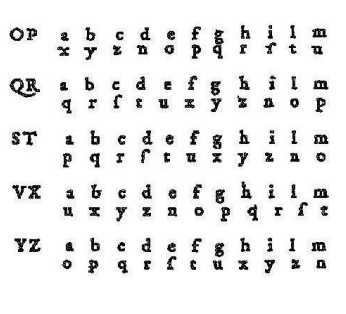

LEONIS BAPT. ALBER-
DE CYFRIS

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 ꝑsidiam datur
ut possint ex sententia. Inuenta sunt scribendi ra
tiones quas Cyfras nuncupant : Commenti quidem
non inutiles ni contra esset qui suis artibus et igno
ralia 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 4 Maggio 2022 – ore 16:00

Seminario Online via Zoom

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

Giovanni Zini

Università degli Studi di Modena e Reggio Emilia

Funzioni Generalized APN in caratteristica dispari e curve algebriche

Abstract: La nozione di funzione APN è stata recentemente generalizzata da Kuroda e Tsujie (2017) a quella di funzione Generalized APN (GAPN) su un campo finito di caratteristica p qualsiasi, richiedendo che la derivata discreta generalizzata in ogni direzione sia una mappa p-a-1. Presenterò alcune interessanti costruzioni di vari autori per funzioni GAPN, nonché una condizione sufficiente data da Ozbudak e Salagean (2021) per ottenere funzioni GAPN da polinomi di permutazione. Mostrerò inoltre condizioni necessarie (ottenute in collaborazione con Bartoli, Giulietti e Peraro) sotto le quali è possibile invertire il risultato di Ozbudak e Salagean. Questi ultimi risultati sono stati ottenuti dallo studio di particolari curve algebriche associate alla funzione.

Link al seminario su Zoom

ID riunione: 842 2315 9207
Passcode: 893313

Referente

Norberto Gavioli

Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it
matematica@decifris.it

UMI

seminariumi-cc@googlegroups.com