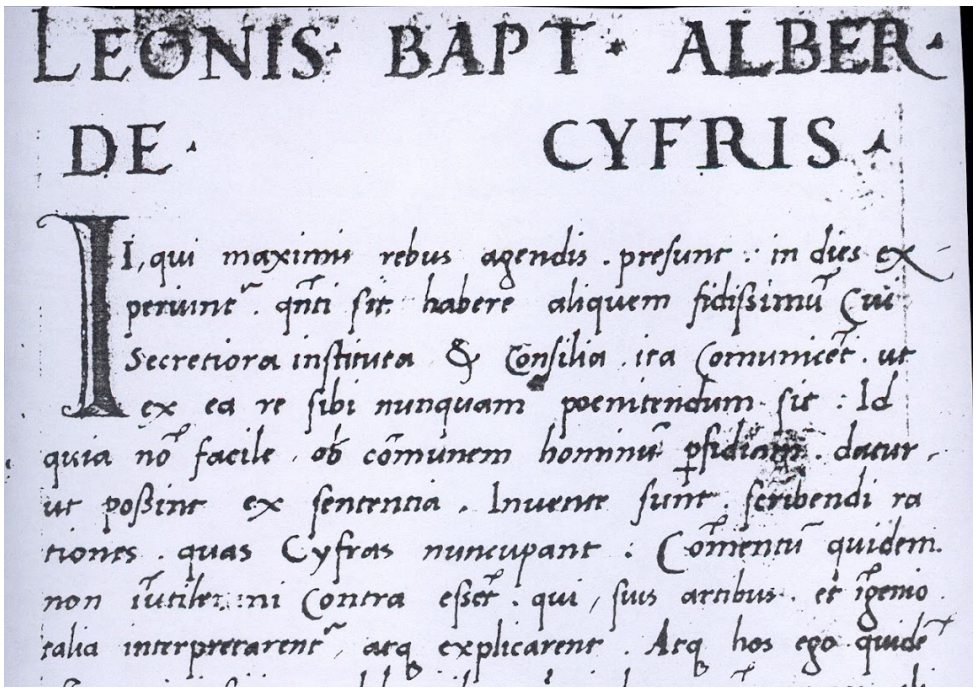
LEONIS BAPT. ALBER-
DE CYFRIS.

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 nõ facile, ob cõmunem hominũ ꝓfidiam, datur,
ut possint ex sententia. Inuenta sunt scribendi ra
tiones, quas Cyfras nuncupant: Comentũ quidem
non inutile, ni contra esset, qui suis armis, et igenio
talia interpretarent, atq; explicarent. Atq; hos ego quide

CifrisChain

lunedì 20 luglio 2020 - ore11:00

Seminario Online via Zoom

Domenica Sogiorno

Università di Bari

Una famiglia di chiavi deboli nel Bitcoin

Abstract: L'algoritmo che genera gli indirizzi Bitcoin è sicuro? In linea generale si: la sua robustezza è basata sulla complessità esponenziale del problema del logaritmo discreto sulla curva Secp256k1 usata in Bitcoin. Cosa succederebbe però se le chiavi fossero in un sottogruppo moltiplicativo del gruppo degli elementi non nulli del campo base su cui la curva ellittica è definita?

In questo seminario è spiegato come è stato possibile attuare un attacco di tipo Brute Force e, risolvere in tempi brevi il problema di cui sopra, rendendo di fatto vulnerabili 4 indirizzi Bitcoin.

Iscrizione dell'evento online da effettuare entro il 19 luglio tramite il seguente link:

click here

Gli iscritti riceveranno ID ZOOM un'ora prima dell'inizio dell'evento

Contatti : Massimiliano Sala

CONTATTI

Associazione De Componendis Cifris

seminari@decifris.it

segreteria@decifris.it