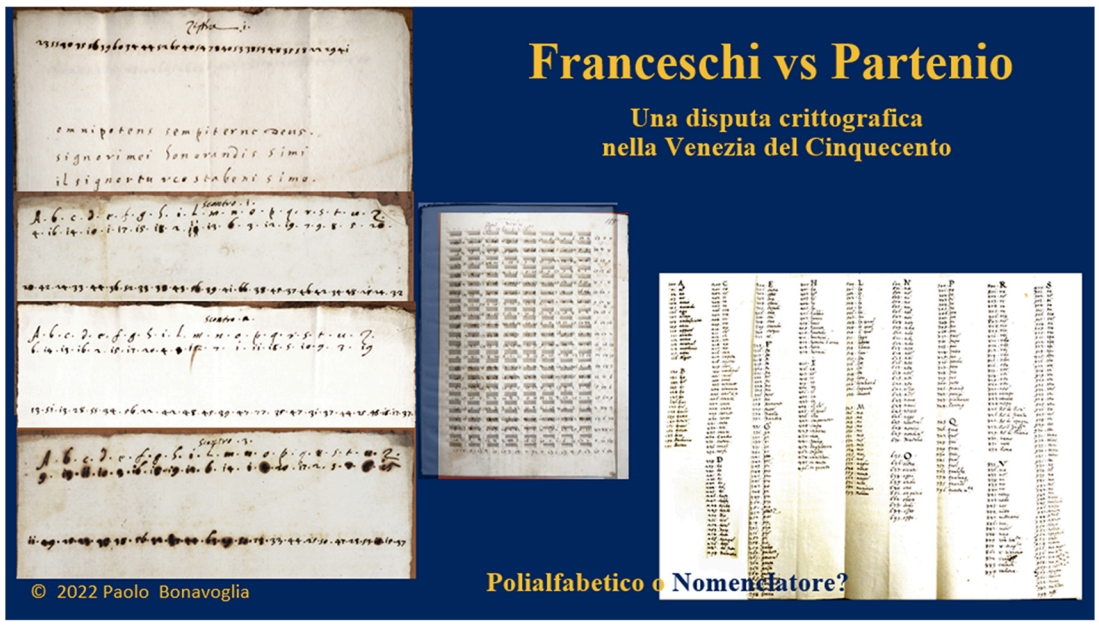

Paolo Bonavoglia ha insegnato Matematica e Informatica nelle scuole superiori dal 1978 al 2017.
I suoi interessi principali sono l'Analisi Non Standard (NSA) e la crittografia.
L'amore per la crittografia risale al nonno materno Luigi Sacco, fondatore dell'ufficio cifra dell'Esercito italiano nella Grande guerra, e autore di un affermato Manuale di Crittografia.
Ha curato l'ultima edizione, 2014, del Manuale e ha scritto diversi articoli sul NSA e crittografia classica, ed ha partecipato come relatore ad alcune conferenze di crittografia storica del ciclo HistoCrypt.
Attualmente è impegnato in una ricerca sulla crittografia veneziana all'Archivio di Stato di Venezia.
Cura dal 1996 il sito web La Crittografia da Atbash a RSA (http://www.crittologia.eu).

DIPARTIMENTO MATEMATICA
DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Associazione Patavina Mathesis

Mathesis Venezia

Mercoledì 21 Dicembre 2022 h 15.00

Prof. PAOLO BONAVOGLIA

Franceschi vs Partenio.
Una disputa crittografica nella Venezia del Cinquecento.

Abstract: Nella seconda metà del Cinquecento a Venezia irrompono sulla scena crittografica, fino allora dominata dai grandi crittanalisti, da Zuan (Giovanni) Soro fino a Zuan Francesco Marin, due singolari personaggi, entrambi interessati alla progettazione delle cifre, più che alla crittanalisi: *Hieronimo di Franceschi* che nel 1572 propone al Consiglio di Dieci (CX) una *cifra vera* ispirata alle cifre polialfabetiche del Tritemio, del Bellaso e del Porta, ma con l'originale introduzione delle operazioni aritmetiche in luogo delle sostituzioni e di una lunga chiave di numeri casuali, che entrò in uso presso le principali ambasciate nel 1577 e ci restò, scomparendo progressivamente, fino al 1595; *Pietro Partenio* che a partire dal 1590 comincia a presentare al CX cifre molto sofisticate ma ispirate a una filosofia opposta a quella di Franceschi: niente cifre polialfabetiche, ma nomenclatori con cifre di tre numeri decimali o due lettere e con sistemi di sovracifratura per proteggersi in caso di furto del cifrario.
Sul finir del secolo, nella laguna, si apre un acceso dibattito dettato (anche) da mozioni pragmatiche che si conclude nel 1600 quando Franceschi muore e, di fatto, entrambe le cifre vengono abbandonate.
La disputa Franceschi vs Partenio segna al tempo stesso, il vertice della crittografia veneziana e l'inizio del suo declino.

Riunione Webex pianificata per mercoledì 21 dicembre 2022
14.30 | (UTC+01:00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna | 3 ore 30 minuti

Accedi dal collegamento alla riunione
https://elearningmarina.webex.com/elearningmarina/j.php?MTID=me3be9401a4709b3d4afd2da88e4a6b1c

Accedi per numero riunione
Numero riunione (codice di accesso): 2730 707 1851
Password riunione: VDfpCCcS657

Toccare per accedere da un dispositivo mobile (solo partecipanti)
+49-619-6781-9736,,27307071851## Germany Toll

Accedi per telefono
+49-619-6781-9736 Germany Toll

Accedi da un sistema o un'applicazione video
Chiama 27307071851@elearningmarina.webex.com
È possibile anche chiamare 62.109.219.4 e immettere il numero della riunione.

Serve aiuto? Vai a https://help.webex.com