DIPARTIMENTO MATEMATICA
DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Associazione Patavina Mathesis

Mathesis Venezia

Venerdì 1 dicembre 2023, 16.00 - 17.30

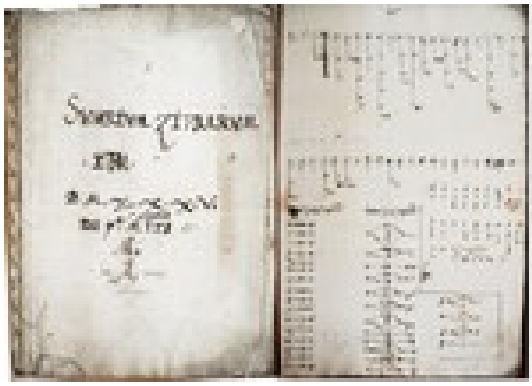
Torre Archimede, aula 2BC30

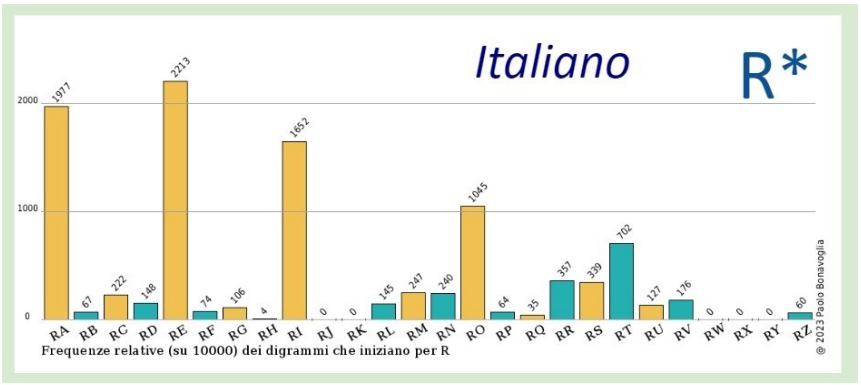
Zoom: https://unipd.zoom.us/j/86860624447

ID riunione: 868 6062 4447

Conferenza di *Paolo Bonavoglia*

Codebreakers: metodi per rompere i cifrari





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.

Abstract: la crittanalisi, decrittare messaggi cifrati senza conoscerne la chiave, nasce alla fine del Medio Evo come inevitabile contraltare della crittografia. Il crittografo progetta cifrari sicuri e il crittanalista inventa metodi per forzare quei cifrari.
Un percorso tra storia, crittografia, statistica, matematica e informatica sulle origini della crittanalisi e sui suoi metodi, dapprima empirici, poi statistici e via via sempre più di natura matematica, per la ricchezza e l'importanza delle loro proprietà.

Pubblico: chiunque sia interessato alla crittografia e alla sua storia abbia una buona preparazione matematica di base (verrà introdotta e usata la funzione logaritmo) grosso modo a livello del quarto anno delle superiori.