DIPARTIMENTO MATEMATICA
DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Associazione Patavina Mathesis

Mathesis Venezia

Venerdì 12 novembre 16.30 - 18.00

Torre Archimede, aula 2AB40 e Zoom (link in corso di definizione)

Conferenza di *Paolo Bonavoglia*

Dalla cifra delle caselle (1577) al cifrario di Vernam (1917)

Aritmetica modulare e numeri casuali in crittografia

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. Quello 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, ha scritto diversi articoli sulla NSA e sulla crittografia classica, e ha partecipato come relatore ad alcune conferenze di crittografia storica del ciclo HistoCrypt (orcid.org/0000-0002-9110-3894). Attualmente è impegnato in una ricerca sulla crittografia veneziana all'Archivio di Stato di Venezia, sulla quale sta preparando un libro. Cura dal 1996 il sito web La Crittografia da Atbash a RSA (http://www.crittologia.eu).

Abstract: la cifra delle caselle è il più originale cifrario usato dalla Repubblica di Venezia, un *unicum*; se a prima vista colpisce l'uso della sovracifratura, assolutamente inusuale per la crittografia rinascimentale, altrettanto originali sono l'uso di operazioni aritmetiche, sottrazione e addizione modulo 20, e quello di una chiave molto lunga (624 numeri tra 0 e 19) e completamente disordinata, che in qualche misura sembrano precorrere il cifrario di Vernam basato su un'addizione/sottrazione modulo 2 e su una chiave casuale che deve essere infinita nel senso di non riutilizzabile,"usa e butta".

Pubblico: Docenti e studenti del triennio. Qualche minima nozione di crittografia è auspicabile.