DIPARTIMENTO MATEMATICA
DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Associazione Patavina Mathesis

Mathesis Venezia

Venerdì 28 gennaio 2022, 16.30 - 18.00

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

Conferenza di *Angela Zottarel*

Curve ellittiche e crittografia

Angela Zottarel si è laureata in Matematica all'Università di Padova, seguendo il programma ALGANT e ha conseguito il Dottorato in Crittografia all'Università di Aarhus in Danimarca. Durante il periodo di Dottorato ha avuto modo di collaborare con diversi gruppi di ricerca a Boston, Tokyo e Pechino. Dal 2014 è insegnante di Matematica alle scuole superiori.

Abstract: Nel 1985 Koblitz e Miller suggerirono l'uso delle curve ellittiche all'interno della crittografia a chiave pubblica. Questa presentazione intende spiegare come i gruppi abeliani costruiti su curve ellittiche possano essere usati per implementare sistemi crittografici estremamente efficienti e con la stessa sicurezza fornita dallo schema RSA .

Pubblico: Studenti di quarta e quinta superiore e relativi insegnanti.