Associazione Subalpina MATHESIS

c/o Dipartimento di Matematica

dell'Università di Torino

Via Carlo Alberto 10, 10123 Torino

http://www.associazionesubalpinamathesis.it/

AVVISO DI CONFERENZA

Il problema della fattorizzazione nella crittografia a chiave pubblica

Nadir Murru

Università di Trento

Presso l'**aula S** del Dipartimento di Matematica,

Via Carlo Alberto 10, primo piano

e

trasmessa in streaming presso

https://unito.webex.com/unito/j.php?MTID=m7008f9e93bc72cad137449690402c9f6.

Il giorno

19 gennaio 2023, ore 17:00

Abstract. Nella prima parte di questo seminario faremo una breve panoramica sulla crittografia (la scienza che studia i metodi per proteggere messaggi e informazioni), concentrandoci in particolare sulla cosiddetta crittografia a chiave pubblica (dove dalla chiave di cifratura non è possibile risalire a quella di decifratura). La sicurezza di tali sistemi crittografici si basa sulla difficoltà computazionale di alcuni problemi come, in particolare, il problema della fattorizzazione dei numeri interi. Nella seconda parte del seminario ci concentreremo quindi sullo stato dell'arte dei metodi di fattorizzazione, a partire dalla brillante idea di Fermat su cui si basano gli attuali metodi più efficienti.