UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

“Crifari Post-Quantum: finalisti NIST”

Docenti: Prof. M. Sala, prof. N. Murru, dott. R. Longo, dott. G. Santilli, dott. A. Meneghetti

Lingua: Il corso si tiene in italiano

Luogo: Online tramite applicativo Zoom (verranno inviati dettagli di collegamento ai partecipanti tramite mail)

Ore di lezione: 30 ore di lezione e 10 ore di laboratorio.

Periodo: 10 – 14 maggio 2021

A chi è rivolto

Il corso è rivolto a professionisti operanti nel campo della sicurezza informatica (PA o aziende private). Il corso è adatto sia a professionisti (di formazione tecnica, informatica o ingegneristica) interessati a vedere gli aspetti algebrici/matematici, sia a persone con buone competenze matematiche, interessate a vedere le applicazioni crittografiche.

Abstract:
In questo corso si presenteranno gli attuali finalisti per la competizione di PostQuantum cryptography del NIST.
Quelli basati sulla teoria dei reticoli sono: CRYSTALS-KYBER, NTRU, SABER, CRYSTALS-DILITHIUM, FALCON.
L’unico basato sulla teoria dei codici è CLASSIC McEliece.
L’unico basato sulla teoria dei polinomi multivariati è RAINBOW

UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

Organizzazione e logistica

Il corso sarà effettuato online nel mese di maggio 2021, da lunedì 10 a venerdì 14 (compresi).
Le lezioni si terranno la mattina dalle 9:00 alle 13:00 e il pomeriggio dalle 14:00 alle 18:00.

Costo del corso

Il numero minimo di partecipanti è 4, il numero massimo è 8.
Il costo didattico totale per il singolo corso è di 1.500 euro a persona (esente da IVA).

Informazioni

Per ogni informazione contattare la dott.ssa Francesca Stanca (cryptolabmat@unitn.it).

Modalità di pagamento

Il pagamento della relativa quota dovrà essere effettuato a ricezione della fattura, mediante bonifico bancario a:

Banca Popolare di Sondrio
p.zza Centa, 14 - 38122 Trento, Italy

IBAN: IT44P0569601800000003106X58

Causale: CRITTO21