UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

“Random Number Generation for Cryptography”

Docente: Prof. Massimiliano Sala, Dott. Alessio 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: 7 – 11 giugno 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:

Il corso presenta sia una panoramica delle basi algebriche e probabilistiche necessarie allo studio dei generatori di numeri random sia una descrizione di alcuni generatori fisici.
Vengono poi dettagliate le seguenti tematiche:

- Linee guida per la costruzione di sorgenti di entropia per applicazioni crittografiche;
- Generatori fisici di numeri random basati su sorgenti quantistiche;
- Metodi algebrici per la manipolazione di sequenze random;
- Procedure di analisi statistica di sequenze random.

Gli argomenti presentati verranno inoltre approfonditi tramite l'uso di strumenti software dedicati.

UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

Organizzazione e logistica

Il corso sarà effettuato nel mese di giugno 2021, da lunedì 7 a venerdì 11 (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