UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

“Crittoanalisi avanzata di RSA”

Docente: Prof. Massimiliano Sala

Assistenti: dott. Alessio Meneghetti, dott. Federico Pintore, dott. Daniele Taufer

Lingua: il corso si tiene in italiano, con parte del materiale in inglese.

Luogo: Roma

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

Periodo: 9 – 13 aprile 2018

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:

L'obiettivo del corso è di spiegare in dettaglio il metodo più efficiente noto al mondo per fattorizzare grandi interi, che è particolarmente performante su i semiprimi usati come chiavi pubbliche del crittosistema RSA.
Partendo da una panoramica sulla parte algebrico/matematica necessaria alla sua comprensione, descriveremo l'algoritmo in maniera da arrivare assieme, docenti e discenti, a realizzarne una implementazione nella parte di laboratorio del corso.
Come prerequisito richiediamo solamente una comprensione di base dell'algoritmo RSA oppure dell'aritmetica modulare.

Organizzazione e logistica

Il corso sarà effettuato a Roma nel mese di aprile 2018, da lunedì 9 a venerdì 13 (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

La deadline per le iscrizioni al corso è il 23 marzo 2018.
Il numero minimo di partecipanti è 4, il numero massimo è 8.
Il costo didattico totale per il singolo corso è di 1500 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: IT06 N 05696 01800 000003108X60
Swift: POSOIT22

Causale: CRITTO18.