UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

"Cifrari a blocchi e identificazione relative vulnerabilità"

Organizzatore scientifico: Prof. Massimiliano Sala

Docenti: prof. Massimiliano Sala, dott. Roberto Civino (UnivAQ)

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

Luogo: Roma

Ore di lezione: 40 ore di lezione, compreso laboratorio e videolezioni

Periodo: dal 30 novembre al 4 dicembre 2020

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:

I cifrari a blocchi sono algoritmi crittografici che offrono elevata sicurezza nell'ambito della crittografia simmetrica. La loro progettazione inizia dalla scelta di componenti robuste (SBox, mixing layer, key schedule) e finisce con l'organizzazione accorta delle suddette componenti. In questo corso sarà esaminata la progettazione dei cifrari a blocchi, partendo dallo studio delle proprietà matematiche richieste alle loro componenti, e arrivando alla valutazione della loro mutua interazione. Il corso si concluderà con una spiegazione dei metodi che portano a individuare eventuali debolezze di un dato cifrario.

Organizzazione e logistica

Il corso sarà effettuato a Roma nella settimana dal 30 novembre al 4 dicembre 2020.
Le lezioni si terranno la mattina dalle 9:00 alle 13:00 e il pomeriggio dalle 14:00 alle 18:00, per un totale di cinque giorni consecutivi.

Costo del corso

Il numero di partecipanti massimo è 10.
Il costo didattico totale per il singolo corso è di 2000 euro a persona (esente da IVA).
In caso di iscrizione di quattro persone, il costo è forfettariamente fissato in 7.334,00 euro.

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.

INTESTAZIONE: Università degli Studi di Trento

BANCA: Banca Popolare di Sondrio - Piazza Centa, 14 - 38122 Trento, Italy

IBAN: IT06 N 05696 01800 000003108X60
Swift: POSOIT22

Causale: CRITTO20.