UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

“Advanced Analysis of Block Ciphers”

Docente: Prof. Massimiliano Sala (maxsalacodes@gmail.com).
Assistente: Dr. Marco Calderini
Luogo: Trento, Dipartimento di Università degli Studi di Trento.
Ore di lezione: 30 ore di lezione e 10 ore di laboratorio.
Periodo: 17-21 Ottobre 2016.

A chi è rivolto

Il corso è rivolto a professionisti 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.

Programma

In questo corso approfondiremo il ruolo del mixing layer e del key-schedule nella progettazione di un block-cipher.
Nello studio del mixing layer, verranno mostrati ed analizzati criteri di costruzione che garantiscano la sicurezza rispetto a tecniche crittanalatiche standard (e.g. differential cryptanalysis) e trapdoor (e. g. partiton-based trapdoor).
La trattazione del key-schedule verterà sulla classificazione dei modelli di key-schedule noti e la loro analisi comparativa.

Organizzazione e logistica

Il corso sarà effettuato nel mese di Ottobre 2016, da lunedì 17 a venerdì 21 Ottobre (compresi). Le lezioni si terranno la mattina dalle 9:00 alle 13:00 e il pomeriggio dalle 14:00 alle 18:00. Durante il pomeriggio verrà messo a disposizione dei partecipanti il Laboratorio di Matematica Industriale e Crittografia, dove si mostrerà come mettere in pratica le nozioni apprese.

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

Costo del corso

Il corso sarà attivato solo in presenza di almeno 4 persone iscritte entro il 26 Settembre 2016.

Il numero massimo di partecipanti è 6.

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: Banca Popolare di Sondrio

Indirizzo: Piazza Centa, Trento

Intestato a: Università degli Studi di Trento

IBAN: IT 06 N 05696 01800 000003108X60

Swift: POSOIT22

Causale: CRITTO16