Valutazione matematica della sicurezza di un cifrario a blocchi

Docente: Massimiliano Sala (maxsalacodes@gmail.com)
Luogo: Facoltà di Scienze, Università degli Studi di Trento.
Ore di lezione: 20 ore frontali e 20 ore in laboratorio.
Periodo: 6-10 Giugno 2011.

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.

Programma

La *parte teorica* comprende:

- le componenti di un cifrario a blocchi;
- valutazione robustezza di una S-box;
- valutazione robustezza di un mixing-layer;
- valutazione robustezza di un key-schedule;
- discussione su variazioni del cifrario per creare personalizzazioni robuste.

Durante il *laboratorio* verranno spiegati algoritmi e programmi per testare le proprietà discusse a lezione (con il software package MAGMA).

Organizzazione e logistica

Le lezioni si terranno la mattina dalle 9:00 alle 13:00 presso la Facoltà di Scienze dell'Università degli Studi di Trento, per una durata di una settimana. Il corso sarà effettuato nel mese di Giugno, da lunedí 6 a venerdí 10 (compresi).

Il pomeriggio degli stessi giorni, dalle 14:00 alle 18:00, verrà messo a disposizione dei partecipanti il laboratorio di Matematica Industriale e Crittografia, dove si mostrerà come mettere in pratica al computer le nozioni apprese.

I partecipanti al corso riceveranno delle dispense complete e dei programmi per testare le proprietá ed i criteri.

Costo del corso

Il numero massimo di partecipanti è di 10 persone.
Il costo didattico totale (lezioni frontali, laboratorio e dispense) è di 1000 euro (esente da IVA). Per dottorandi e neo laureati il costo è ridotto a 100 euro.

È anche possibile seguire solo una lezione o più. Sono possibili anche soluzioni agevolate per vitto e alloggio relativi alle lezioni del corso. Per ogni informazione contattare la dott.essa Stanca (francesca.stanca@gmail.com).

Modalità di pagamento

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

Unicredit Banca Spa
Sede di Trento - Via Galileo Galilei, 1
IBAN IT37L0200801820000100807242
SWIFT UNCRIT2B0HV.

Causale: CRITTO11.

`Nota`: Non aggiungere altro alla causale, solo `CRITTO11`.