UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

“Debolezze dei Cifrari a Blocchi: attacchi recenti e contromisure”

Docente: Prof. Massimiliano Sala (maxsalacodes@gmail.com).

Assistente: Dott. Riccardo Aragona.

Luogo: Trento, Dipartimento di Università degli Studi di Trento.

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

Periodo: 9-13 Settembre 2013.

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.

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

Programma

La parte *teorica* si articola in 5 giornate e comprende i seguenti argomenti:

1) Descrizione generale della struttura dei cifrari a blocchi moderni e dei loro componenti principali: S-Box, mixing-layer, key-schedule.

2) Descrizione dettagliata dei crittosistemi piu' interessanti (AES, Serpent, Kasumi) .

3) Debolezze derivanti da cattive scelte della S-Box, attacchi relativi e contromisure da adottare nella costruzione di un cifrario.

4) Debolezze derivanti da cattive scelte del mixing-layer, attacchi relativi e contromisure da adottare nella costruzione di un cifrario.

5) Debolezze derivanti da cattive scelte del key-schedule. Attacchi related-key e l'attacco* "biclique" a AES: il primo attacco noto estendibile a tutti i round con complessità minore della ricerca esaustiva.

**Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, "Biclique Cryptanalysis of the Full AES", in Advances of Cryptology – ASIACRYPT 2011, Lecture Notes in Computer Science 7073 (2011), Springer, pp 344-371.*

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

I partecipanti al corso riceveranno delle dispense complete per la parte teorica e dei programmi per la parte di laboratorio.

Organizzazione e logistica

Il corso sarà effettuato nel mese di Settembre 2013, da lunedì 9 a venerdì 13 settembre (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

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

Matematica Industriale e Crittografia, dove si mostrerà come mettere in pratica le nozioni apprese.

Costo del corso

Il corso sarà attivato solo in presenza di almeno cinque persone iscritte entro il 29 marzo 2013.
Il numero massimo di partecipanti è 8.
Il costo didattico totale per il singolo corso è di 1500 euro a persona (esente da IVA). In caso di iscrizione sia al corso in oggetto che al corso previsto per maggio "Sorgenti di Randomicità in Crittografia e Crittanalisi: specifiche e criticità", il costo complessivo per entrambi i corsi è pari a 2000 euro a persona.

Informazioni

Per ogni informazione contattare la dott.ssa Francesca Stanca (francesca.stanca@gmail.com).

Modalità di pagamento

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

Unicredit Banca Spa
Sede di Trento - Via Galileo Galilei, 1
IBAN IT37L0200801820000100807242
SWIFT UNCRIT2B0HV.
Causale: CRITTO13.
Nota: Non aggiungere altro alla causale, solo CRITTO13.

Trento, 13/12/2012

Il docente del corso
Prof. Massimiliano Sala