UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

# "Mathematical trapdoors in block ciphers: evaluation and attack exploitation"

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

**Assistente**: Dott. Marco Calderini.

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

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

**Periodo**: 21 – 25 settembre 2015.

**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) Introduzione alle funzioni Booleane e alle loro proprietà crittografiche (APN, weakly APN, anti-invarianza, anti-crooked).
2) Descrizione del concetto di Trapdoor in Crittografia Simmetrica, primo esempio noto in letteratura di trapdoor su block cipher (Rijmen-Preneel block cipher), crittoanalisi su questi block cipher.
3) Definizione di imprimitività di un gruppo di permutazioni, gruppo generato dalle funzioni di round di un block cipher, trapdoor derivanti dall'imprimitività di tali gruppi (Paterson)
4) Definizione di translation-based cipher, ruolo delle S-Box e del mixing layer in tb cipher, condizioni sufficienti sulla primitività in tb cipher (Caranti-Dalla Volta-Sala)
5) Descrizione di somme alternative definibili sullo spazio dei messaggi (hidden-sum), hidden-sum trapdoor, toy cipher con hidden-sum trapdoor, ruolo dell'S-Box nelle hidden-sum trapdoor.

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

- come sfruttare le debolezze dei cifrari per implementare una trapdoor
- come implementare attacchi basati sulla trapdoor
- come evitare attacchi basati sulla trapdoor

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 2015, da lunedì 21 a venerdì 25 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 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**

La deadline per le iscrizioni al corso è il 1 settembre 2015.
Il numero massimo di partecipanti è 6.
Il costo didattico totale per il singolo corso è di 1000 euro a persona (esente da IVA).

**Informazioni**
Per ogni informazione contattare la dott.essa 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:

Banca Popolare di Sondrio
p.zza Centa, 14 - 38122 Trento, Italy
**IBAN: IT06 N 05696 01800 000003108X60**
**Swift: POSOIT22**
Causale: CRITTO15.
*Nota: Non aggiungere altro alla causale, solo CRITTO15.*

*Trento, 8/6/2015*

*Il docente del corso*
*Prof. Massimiliano Sala*