Valutazione matematica della sicurezza degli stream-cipher

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: 5-9 Settembre 2011.

A chi è rivolto

Il corso è rivolto a professionisti operanti nel campo della sicurezza informatica (PA o aziende private), sia con formazione matematica che con formazione tecnica (informatica, ingegneria, etc).

Programma: overview

Il corso si articolerà nel seguente modo:

- Descrizione delle componenti di uno stream-cipher e il loro ruolo. Presentazione dei principali cifrari a flusso.
- Il ruolo della chiave e della fase di inizializzazione.
- Attacchi statistici.
- Attacchi algebrici.
- Relazione tra stream-cipher e altre primitive crittografiche.

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 Settembre, da lunedí 5 a venerdí 9 settembre (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.

Programma: dettagli

- Introduzione
- Definizione Stream Cipher
- Stato, Key, IV
- Toy Cipher
- Classificazione
- LFSR
- Combination Generator, Clock Control, Shrinking Generator
- Trivium e Bivium
- Considerazioni su resistenza
- A5/1 A5/2 A5/3
- CA Cellular Automata
- Attacco Cube
- OFB
- LEX-AES128
- Weak Keys
- Riscaldamento in fase iniziale
- Key Entropy
- Attacchi A5/1 A5/2
- Attacchi A5/3
- Specifiche di ZUC
- Valutazione ZUC
- Funzioni Boleane non lineari con la somma modulare 2n e 2n-1
- Risolvere DEA
- RC4
- HC
- Conclusione

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 200 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 a:

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

Causale: CRITTO11.

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