UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

“Sorgenti di Randomicità in Crittografia e Crittanalisi: specifiche e criticità”

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

Assistente: Dott. Alessandro Tomasi.

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

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

Periodo: 3 – 7 giugno 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.
Durante il corso ci si avvalerà della collaborazione di personale di idQuantique, nota azienda svizzera di dispositivi quantistici per la crittografia.

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

Programma

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

1) L'importanza della randomicità in crittografia per la generazioni di chiavi simmetriche ed asimmetriche, di stati iniziali per gli stream cipher, di successioni di numeri random. Differenze tra sorgenti di entropia basate su processi fisici e generatori deterministici di numeri pseudo-casuali con discussioni di aspetti critici.
2) Algoritmi pseudorandom basati su registri lineari e non-lineari: applicazione negli stream-cipher e possibili debolezze.
3) Algoritmi pseudorandom basati su azione di permutazione: applicazione nei block cipher e possibili debolezze.
4) Meccanismi di costruzione di randomicità e sorgenti fisiche con riferimento ai recenti documenti del NIST*.
5) Randomicità ottenuta da fenomeni quantistici (le lezioni di questa giornata sono tenute in collaborazione con una nota azienda svizzera di dispositivi quantistici per la crittografia: *IdQuantique*).

**SP800-90 A (Jan 2012) Recommendation for Random Number Generation Using Deterministic Random Bit Generators; SP800-90 B (Aug 2012) DRAFT Recommendation for the Entropy Sources Used for Random Bit Generation; SP800-90 C (Aug 2012) DRAFT Recommendation for Random Bit Generator (RBG) Construction. Documenti disponibili all'indirizzo: http://csrc.nist.gov/publications/PubsSPs.html#800-90A*

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 Giugno 2013, da lunedì 3 a venerdì 7 giugno (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 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).

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:

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, 15/2/2013

Il docente del corso
Prof. Massimiliano Sala