Criteri matematici per la sicurezza di un sistema crittografico

Docenti: Massimiliano Sala (`sala@science.unitn.it`)
Anna Rimoldi (`rimoldi@science.unitn.it`)
Luogo: Facoltà di Scienze, Università degli Studi di Trento.
Ore di lezione: 40 ore frontali (25 ore a disposizione in laboratorio).
Periodo: 6-17 Settembre 2010.

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

Il corso è diviso in due parti. Nella *prima* parte si illustrano i principali strumenti algebrici utili per la comprensione dei sistemi crittografici presentati nella *seconda parte*. Dallo studio algebrico nascono criteri e approcci per

`testare la robustezza/sicurezza di un block cipher`.

Tali criteri saranno introdotti man mano che si presentano i diversi sistemi.

La *prima parte* comprende:

- introduzione ai gruppi di permutazione; azione di un gruppo su un insieme: azione transitiva, k-transitiva, regolare, k sharply-transitive e primitiva; studio di qualche sottogruppo massimale del gruppo simmetrico;
- i cifrari come insiemi di permutazioni: attacchi di distinguibilità;
- richiami di campi finiti: campi, anelli commutativi, ideali, quozienti, anelli polinomiali, struttura dei campi finiti, elementi primitivi etc...;
- teoria dei polinomi di permutazione (su campi finiti);
- introduzione alle funzioni Booleane: proprietà della ANF;
- concetti di non-linearità nelle funzioni Booleane: non-linearità classica e funzioni MNL e AB, δ-uniformità e funzioni APN, δ-uniformità debole e funzioni debolmente APN, anti-invarianza, etc.. .

La *seconda parte* comprende:

- Studio dei sistemi translation-based: loro teoria generale con studio delle S-Boxes viste come funzioni Booleane; *Come garantire la sicurezza operando sulle S-Boxes?*
- Descrizione dei translation-based più noti: AES, SERPENT, PRESENT.
- Il ruolo del Mixing-Layer del Key-Scheduling nei translation-based: *Come garantire la sicurezza operando sul Mixing-Layer e sul Key-Scheduling?*
- Crittanalisi lineare e differenziale; potenziale differenziale e lineare (con applicazioni).
- Studio dei sistemi Feistel classici (e loro sicurezza): DES, 3DES
- Studio dei sistemi Feistel moderni (e loro sicurezza): Blowfish, Camellia, Kasumi, Twofish.
- Studio di altri interessanti block cipher: IDEA, IDEA-NXT/FOX, SAFER.

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 due settimane. Il corso sarà effettuato nel mese di Settembre, dal 6 al 10 e dal 13 al 17 (compresi).

Il pomeriggio degli stessi giorni, dalle 14:30 alle 17:00, 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 la mattina.

I partecipanti al corso riceveranno delle dispense complete.

Costo del corso

Il costo didattico totale (lezioni frontali, laboratorio e dispense) è di 1500 euro (esente da IVA).

Per dipendenti di aziende o enti che collaborano col laboratorio di Matematica Industriale e Crittografia il costo didattico totale è di 300 euro (esente da IVA).

È anche possibile seguire solo una o più lezione. Per il costo contattare la dott.essa Rimoldi (rimoldi@science.unitn.it). Sono possibili anche soluzioni agevolate per alloggio e vitto relativi alle lezioni del corso.

Vitto e alloggio

E' possibile usufruire del vitto e dell'alloggio presso strutture convenzionate secondo le due seguenti opzioni:

(1) al sovracosto di 500 euro (sempre IVA esente) è possibile usufruire di alloggio completo e vitto parziale:

- *tutte le notti*: dalla notte della Domenica antecedente al corso fino alla notte del Venerdì della seconda settimana (13 notti);
- *tutte le colazioni*: dal Lunedì della prima settimana al Sabato della seconda settimana;
- i pranzi dal Lunedi' al Venerdì della prima settimana e dal Lunedì al Venerdì della seconda settimana (10 pranzi in tutto).

(2) al sovracosto di 1100 euro (sempre IVA esente) è possibile usufruire di alloggio completo e vitto completo:

- *tutte le notti*: dalla notte della Domenica antecedente al corso fino alla notte del Venerdì della seconda settimana (13 notti);
- *tutte le colazioni*: dal Lunedì della prima settimana al Sabato della seconda settimana;
- *tutti i pranzi*: dal Lunedì della prima settimana al Venerdì della seconda settimana (12 pranzi in tutto).
- *tutte le cene*: dalla cena della Domenica antecedente al corso alla cena del Venerdì della seconda settimana (13 cene).

Modalità di pagamento

Il pagamento della relativa quota dovrà essere effettuato prima dell'inizio del corso ed a ricezione della fattura, mediante bonifico bancario

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

Causale: CRITTO10.