



Conferenza sul tema

LA CRITTOGRAFIA E LE SUE APPLICAZIONI

Relatore Prof. Antonio LIOY

Docente di “Sicurezza dei sistemi informatici” al Politecnico di Torino

Torino, 4 Marzo 2008, ore 18:00

Sala **AGORÁ DELLA CITTADELLA POLITECNICA - I3P**
INCUBATORE IMPRESE INNOVATIVE POLITECNICO

Corso Castelfidardo 30 Torino

Segreteria ANIPLA

Sig.ra Antonella MAFFIA

011 0905121

Storicamente la crittografia è stata usata per rendere segrete delle informazioni (tipicamente nell'ambito di comunicazioni militari, politiche o amorose).

Anche nell'odierna società dell'informazione la crittografia ricopre un simile ruolo e, grazie alla potenza di calcolo ed alla diffusione dei Personal Computer, non è più limitata solo alle grosse organizzazioni ma può essere facilmente usata anche da piccole e medie imprese o dai singoli individui.

Inoltre è stata individuata una nuova area applicativa: non solo la segretezza delle informazioni ma anche la loro integrità ed autenticità, che spesso sono le proprietà più importanti dei nostri dati (si pensi anche solo al fenomeno dei falsi messaggi di posta elettronica con cui si conducono molti attacchi). Soprattutto nel caso di procedimenti giudiziari è molto importante poter dimostrare se dati programmi sono stati modificati o meno.

Nel corso della conferenza verranno presentati sia i principi della crittografia sia le sue applicazioni base alla segretezza ed alla verifica di integrità ed autenticità delle informazioni.

Cenni Storici

La parola crittografia deriva da due parole greche *kryptos*, che significa nascosto, e *graphein*, che significa scrivere.

La crittografia è una scienza antica che si occupava dei metodi di cifratura delle informazioni al fine di rendere trasparenti i messaggi tra un emittente e un destinatario ma senza essere leggibili da altre persone.

Gli Spartani 2500 anni fa utilizzavano una striscia di papiro avvolta a spirale attorno ad un bastone che costituiva la chiave di codifica e decodifica; altri documenti fanno risalire al tempo degli Egiziani, nel 1990 AC (Tomba di Knumotete II°), l'uso della crittografia come modifica volontaria di un testo.

Il cifrario di Giulio Cesare è il più antico algoritmo crittografico, del quale si abbia una traccia storica; è un cifrario a sostituzione monoalfabetica, in cui ogni lettera del testo in chiaro, è sostituita nel testo cifrato dalla lettera che si trova ad un certo numero "n" di posizioni dopo nell'alfabeto. In particolare Cesare utilizzava uno spostamento di 3 posizioni, per cui "n" = 3, come da esempio qui riportato :

Testo in chiaro a b c d e f g h i l m n o p q r s t u v z

Testo cifrato D E F G H I L M N O P Q R S T U V Z A B C

Nel XX secolo sono nate nuove tecniche di cifratura, prima macchine cifranti come la celebre macchina Enigma usata dai tedeschi nella II guerra mondiale, poi con l'avvento dei computer che ha di colpo resi inaffidabili e superati quasi tutti i metodi classici, metodi specifici per l'uso informatico come il DES della IBM e il rivoluzionario RSA capostipite dei cifrari a chiave pubblica.

Oggi con il largo uso di Internet e della posta elettronica, delle comunicazioni telefoniche via cavo o con cellulari, i fax ed il sempre maggior uso dei sistemi wireless, i nostri messaggi possono essere intercettati con normali apparecchiature elettroniche, e per questo la moderna crittografia assume sempre maggiore importanza per la protezione dei nostri documenti.