# E-mail Sicurezza Crittografia Hacker

**Glossario della sicurezza crittografia**

La crittografia è una metodologia che permette di scambiarsi informazioni confidenziali. L'obiettivo della crittografia è di rendere privata una comunicazione che si svolge su un mezzo pubblico (nella nostra Era tipicamente Internet), potenzialmente insicuro a cui chiunque può avere facile accesso. La crittografia su basa su una serie di principi: Segretezza, solo il destinatario è in grado di leggere il messaggio crittografato; Autenticità, il destinatario del documento è sicuro dell'origine del messaggio; Integrità, il destinatario è sicuro che il messaggio non abbia subito modifiche durante la trasmissione;

Non Ripudiabilità, il destinatario può avere, senza possibilità di incertezza, sicurezza dell'origine del messaggio al mittente. Le prime notizie di un sistema di crittografia si trovano negli scritti di Plutarco che descrive un metodo di scrittura nascosta adottato dagli spartani: una striscia di cuoio attorno ad un bastone caratterizzato da un certo diametro su cui il messaggio veniva scritto su colonne. Srotolata la striscia di cuoio il testo era incomprensibile e solo arrotolandola su un bastone di uguale dimensione a quello del mittente era leggibile. In Grecia, veniva usato anche il disco di Enea il Tattico, un disco con 24 fori per ciascuna lettera dell'alfabeto. La codifica del messaggio avveniva passando un filo attraverso i fori corrispondenti alle lettere. Giulio Cesare usava un sistema che consisteva nello scrivere i messaggi spostando tutte le lettere dell'alfabeto di 3 posizioni: tale sistema è noto come cifrario monoalfabetico. Nel Medioevo e nei secoli dopo si utilizzarono sistemi sempre più complessi: verso la fine dell'Ottocento arriva la tecnologia con macchine in grado di cifrare e decifare automaticamente i messaggi.

Il disco di Wheatstone era un sistema formato da due dischi concentrici. Durante la seconda guerra mondiale i tedeschi utilizzarono una macchina di cifratura chiamata Enigma, composta di vari dischi che ruotavano alla pressione di ogni tasto. In risposta gli inglesi costruirono una macchina chiamata Colossus in grado di decifrarne i loro messaggi.

**Glossario della sicurezza firewall**

Firewall significa "muro di fuoco". E' uno degli strumenti principali della sicurezza informatica, progettato per impedire accessi non autorizzati a/da reti private. Il suo utilizzo tipico quindi è quello di impedire agli utenti provenienti da Internet l'accesso non autorizzato ad una Intranet. Un firewall si occupa di filtrare i dati che passano da un computer ad un altro sulla rete, quindi applica un modello di sicurezza di tipo "perimetrale", per tenere fuori tutto ciò che non è necessario far entrare. Per reti private o Intranet con medi e alti livelli di complessità, o con necessità di particolari sicu-