Introduzione

In questo quaderno, gli autori presentano gli argomenti sviluppati nelle lezioni tenute dal professore Alessandro Montinaro nel corso di Crittografia per gli studenti della Laurea Magistrale in Matematica dell'Università del Salento nell'a.a. 2018-2019.

Come il termine stesso suggerisce, la Crittogrfia è la disciplina che si occupa di "nascondere i messaggi", ovvero non di occultarli, ma di renderli incomprensibili a persone non autorizzate a leggerli. In passato, la Crittografia è stata utilizzata soprattutto in ambito militare. Oggi, invece, tutti noi facciamo uso quotidiano della Crittografia, anche senza rendercene conto. Lo sviluppo della comunicazione telematica e l'utilizzo crescente di internet per effettuare operazioni delicate (come, ad esempio, operazioni bancarie) ha fatto sì che il problema della segretezza diventasse sempre più importante.

La storia della Crittografia permette di capire come i metodi crittografici si siano evoluti nei secoli, attraverso conoscenze matematiche sempre più avanzate, intrecciandosi sempre di più con le nuove tecnologie e con il mondo dell'informatica. Durante le lezioni, infatti, si è cercato di dare importanza sia all'aspetto matematico della Crittografia, fornendo nozioni provenienti da diverse aree matematiche, come la probabilità discreta o la teoria dei numeri, sia all'aspetto computazionale, analizzando gli algoritmi utilizzati nei crittosistemi, con particolare riguardo alla loro complessità computazionale.

Nei primi capitoli di queste note, sono analizzate le tappe più importanti dello sviluppo dei sistemi crittografici dal I secolo a.C. fino alle tecniche utilizzate durante la seconda guerra mondiale. Successivamente, viene introdotta una particolare classe di cifrari a blocchi: i cifrari iterati, e viene descritto dettagliatamente il crittosistema AES (Advanced Encryption Standard), utilizzato come standard dal governo degli Stati Uniti d'America a partire dal 2001. In seguito, vengono analizzate le Funzioni Hash Crittografiche e il loro utilizzo per assicurare l'integrità dei dati. Un'ampia sezione è dedicata allo studio del crittosistema RSA, concentrandosi principalmente su tre aspetti: l'implementazione del crittosistema, l'efficienza della cifratura e il problema della sicurezza. Sono stati analizzati, infatti, i principali metodi di attacco al Crittosistema RSA, come l'Algoritmo Rho di Pollard, l'Algoritmo di Dixon per i quadrati casuali per la fattorizzazione dei moduli e, infine, l'Algoritmo di Wiener per la determinazione dell'esponente di decifratura. Successivamente, è stato introdotto il Problema del Logaritmo Discreto, alla base della sicurezza di numerosi crittosistemi. In seguito, sono state introdotte le curve ellittiche e la loro applicazione alla Crittografia nella costruzione degli analoghi dei crittosistemi basati sul Problema del Logaritmo Discreto, e l'Algoritmo di Lenstra utile per fattorizzare un intero composto dispari e quindi come ulteriore metodo di attacco al Crittosistema RSA. La parte finale del quaderno è dedicata allo studio di vari sistemi di firma

digitale, come il sistema di firma di ElGamal e le sue varianti, il sistema di firma one-time di Lamport e, infine, i sistemi di firma non ripudiabili di Chaum - Van Anterwerpen e fail-stop di Pedersen - Van Heyst.

Lecce, giugno 2019.

Alessandro Montinaro
Dipartimento di Matematica e Fisica "Ennio De Giorgi"
alessandro.montinaro@unisalento.it

Pierluigi Rizzo
Dipartimento di Matematica e Fisica "Ennio De Giorgi"
pierluigi.rizzo@unisalento.it