La Crittografia

Introduzione alla crittografia

di G.Falco dic 2016

La crittografia (dall'unione di due parole greche: κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo.

Un tale messaggio si chiama comunemente **crittogramma** e i metodi usati sono detti tecniche di cifratura. Il messaggio da cifrare inceve è chiamato **testo in chiaro**

La storia della crittografia ha origini remote ed inizia con la **crittografia classica**, con metodi di cifratura che utilizzavano carta e penna o, al massimo, semplici supporti meccanici.
Agli inizi del XX secolo l'invenzione di **dispositivi elettromeccanici**, come ad esempio la **macchina Enigma** a rotori, elevò a più sofisticati ed efficienti livelli la cifratura; la successiva introduzione dell'elettronica e dei computer ha permesso l'utilizzo di schemi di cifratura sempre più complessi, molti dei quali non ottenibili con carta e penna.

Crittografia classica

La storia della crittografia ha origini remote ed inizia con la crittografia classica, con metodi di cifratura che utilizzavano carta e penna o, al massimo, semplici supporti meccanici
Il più antico esempio di utilizzo della crittografia è stato rinvenuto in alcuni geroglifici egiziani scolpiti in antichi monumenti dell'Antico Regno (risalenti a più di 4500 anni fa)
Gli antichi Greci si dice avessero conoscenze di crittografia (ad esempio il bastone per cifrare **scitala**, che sembra fu utilizzato dall'esercito di Sparta)

video sulla crittografia

La Scitala

I Romani conoscevano certamente la crittografia: l'esempio più noto è il cifrario di Cesare.

Breve storia dei metodi classici di crittografia

La crittografia non eve essere confusa con la **steganografia** che invece è la tecnica di nascondere i messaggi piuttosto che offuscarli.
Si desidera cioè che il messaggio non appaia crittato ad un osservatore esterno, che non deve accorgersi che dentro messaggi apparentemete innocenti, si nascondono significati alternativi.
Nell'era digitale queste tecniche permettono ad esempio di nascondere testi in file immagine o audio. Si potrebbe semplicemente dire che mentre la crittografia nasconde il significato dei messaggi, la steganografia nasconde il messaggio stesso.

Utilizzo di strumenti di cifratura

Lo strumento più famoso e importante per le implicazioni che ebbe nella conclusione della seconda guerra mondiale, fu senz'altro la macchina Enigma, utilizzata dall'esercito tedesco per crittografare e decodificare i messaggi militari.
Considerata inviolabile dal suo progettista e dai vertici militari, fu invece possibile giungere con immensi sforzi da parte dei serivizi segreti britannici, e al genio di un gruppo di crittanalisti capeggiati da **Alan Turing** alla sua decrittazione. Moltissimi libri sono stati scritti su questa vicenda storica e recentemente un film intitolato **'The imitation game'** ripercorre quell'impresa che a detta di molti esperti, contribuì ad accorciare gli esiti della seconda guerra mondiale di almeno due anni.


Enigma

La crittografia moderna

L'avvento dei computer ha profondamente modificato sia le tecniche crittogriche, rendendole più veloci e sicure, sia quelle crittoanalitiche, ossia i tentativi di decodificare messaggi cifrati, senza possedere la **'chiave'**.
Nell'approccio meoderno infatti, si considera sufficientemente sicuro un metodo crittografico, se non sia necessario tenere segreto il metodo utilizzato, per garantire l'impossibilità a persone non autorizzate di decodificare il messaggio. Ma sia necessario nascondere soltanto la **chiave** intesa come sequenza di caratteri o numeri, condivisa fra le persone che desiderano proteggere la riservatezza dei messaggi.
Chi possiede la chiave dunque è in grado di codificare un messaggio e renderlo illeggibile o meglio non interpretabile, da chi non la possiede.
Rimane il problema però della segretezza della chiave, che deve essere scambiata tra i partecipanti alla comunicazione cifrata, attraverso un 'canale sicuro', non intercettabile o spiabile da persone estranee.
In un epoca di comunicazioni veloci e globali come quella moderna, questo limite rappresenta un ostacolo all'applicazione delle tecniche crittografiche ai commerci.
Oltre alla riservatezza delle informazioni, una ulteriore necessità moderna è quella di garantire l'identità delle persone che comunicano, attraverso le reti digitali, in situazioni nelle quali sia necessario assicurarsi che chi scrive sia effettivamente la persona che afferma di essere e non qualuno che si spaccia per lui.
Ne caso di sottoscrizione di contratti, inoltre, non vi deve essere la possibilità di ripudio da parte di chi ha ad esempio inviato un contratto, in forma digitale, con la propria firma.
Una svolta decisiva in questo senso si è avuta con la scoperta di procedimenti crittografici a **'chiave asimmetrica** che risolvono brillantemente questi problemi.

Con questi metodi, la chiave utilizzata per crittare un documento, ossia renderlo non interpretabile, è differente da quella che serve a 'decrittare' ossia ad applicare il procedimento inverso che lo renderà nuovamente leggibile.
L'invio della prima chiave, chiamata **chiave pubblica**, non consente di risalire alla seconda chiamata **chiave privata**.

Quindi può essere inviata su un canale insicuro. Il metodo può essere inoltre utilizzato per la **firma digitale**.
L'algortimo più utilizzato oggi di questo tipo è **RSA** dal nome dei ricercatori che lo hanno scoperto e brevettato: Rivest, Shamir, Adleman.


Ronald Rivest (al centro) - 2007

Riferimenti: wikipedia