Breve storia della crittografia

Leonardo Miliani | 25 novembre 2007

Si parla molto della **crittografia**… ma quando è nata? Chi sono stati i primi crittografi? Che tecniche venivano utilizzate quando non c'erano i computer a dare una mano ai crittografi? A queste e ad altre domande cercherò di rispondere in questo breve articolo, che abbraccia temporalmente un arco di 3900 anni, partendo dalle prime testimonianze certe di origine egiziana fino ad arrivare alla Seconda Guerra Mondiale, conflitto che servì a sviluppare diversi campi della scienza e della tecnica, compresa la crittografia. Infatti durante una guerra uno dei requisiti principali che deve possedere un buon esercito è l'avere un modo per far comunicare i suoi vertici con le truppe sparse sui fronti di battaglia senza che tali messaggi possano venir interpretati dal nemico anche se questo riesce ad intercettare le comunicazioni.

La crittografia come tecnica per celare un messaggio esiste fin da tempi antichissimi: i primi rudimentali messaggi cifrati sembra siano contenuti già in alcuni geroglifici egizi della tomba di Knumotete II, risalente al 1900 a.C. In Grecia gli Spartani usavano intorno al 400 a.C. la **scitala** lacedemonica, un bastone verticale su cui erano incisi in ordine le lettere dell'alfabeto. Avvolgendoci sopra un papiro e scrivendo il messaggio verticalmente si aveva il testo trasposto sul papiro: solo riavvolgendolo su un bastone di diametro identico al precedente si poteva ricostruire senza sforzi il messaggio originale.

Quasi dello stesso periodo sono i primi cifrari ebraici, di cui il più noto è senz'altro il codice di **Atbash**, dove si aveva una semplice sostituzione della prima lettera dell'alfabeto con l'ultima, poi della seconda con la penultima, e così via.

Un altro famosissimo cifrario storico è quello di **Cesare**, che è stato usato per diversi secoli fino all'Alto Medioevo. In questo cifrario, la *sostituzione delle lettere* avviene l'uso di un secondo alfabeto costruito partendo da quello in chiaro con le lettere spostate di un certo intervallo numerico prefissato (intervallo che rappresenta quindi la chiave). Cesare utilizzava uno spostamento di 3 locazioni. Ecco quindi il nostro alfabeto italiano e quello creato con i 3 spostamenti utilizzati da Cesare:

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

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

Usando questo cifrario la parola CIAO diventa FNDR (C->F, I->N, A->D, O->R). Ovviamente la robustezza di questo cifrario è molto bassa ma per l'epoca rappresentava senz'altro un buon metodo per far giungere ai propri comandanti i messaggi sulle manovre militari senza che il nemico potesse decifrarli in caso fosse riuscito a metter mano ai testi.

La crittografia nel Medioevo conosce un forte sviluppo ad opera di 2 grandi menti italiane, **Leon Battista Alberti**, che ha inventato il disco cifrante che porta il suo nome, e **Giovan Battista Bellaso**, che per primo utilizza una sorta di "chiave di cifratura".

Il **disco cifrante di Alberti** è costituito da 2 dischi concentrici e rotanti l'uno rispetto all'altro su cui sono trascritti 2 alfabeti: su quello esterno abbiamo l'alfabeto maiuscolo in ordine regolare del messaggio in chiaro mentre su quello interno l'alfabeto è riportato con lettere minuscole ed in modo disordinato. E', questo, il primo esempio di **cifrario polialfabetico**.

Giovan Battista Bellaso ideò invece un sistema per alternare alcuni alfabeti segreti formati utilizzando una parola chiave controllata da un lungo versetto chiamato "*contrassegno*". Questo sistema verrà poi ripreso dal francese **Blaise de Vigenère**, che utilizzerà anche un sistema di un matematico tedesco, Giovanni Tritemio, creando quello che verrà conosciuto per alcuni secoli come

il cifrario indecifrabile, o "**Cifrario di Vigenère**". Questo cifrario conobbe un lungo periodo di fortuna: solo nel 1863 l'ufficiale prussiano **Friedrich Kasiski** pubblicò un metodo per violare un testo cifrato con tale sistema. Ma cosa aveva di particolare il cifrario di Vigenère? Offuscava il testo in chiaro, vale a dire nascondeva quella che era la debolezza dei precedenti cifrari: analizzando la frequenza con cui comparivano le lettere nel testo cifrato si poteva, faticosamente ma sicuramente, risalire, al messaggio in chiaro. Il sistema di Vigenère annullava quasi del tutto tale dato (in crittografia si utilizza il termine "offuscare"): fu proprio quel "quasi" che venne sfruttato da Kasiski per il suo metodo di forzatura.

Arrivando all'epoca moderna, lo sviluppo della tecnica permise di abbandonare la carta e la penna per delegare alle macchine il compito di cifrare i messaggi. Ed arriviamo così alla macchina **Enigma**, adoperata dai Tedeschi nella II Guerra Mondiale per cifrare i messaggi militari. La macchina era basata su una telescrivente collegata ad un sistema di 3 rotori attraverso cui passavano in maniera non nota dei fili elettrici che collegavano il tasto della telescrivente con una lettera luminosa. Premendo un tasto, l'impulso elettrico viaggiava all'interno dei rotori per poi accendere la lettera cifrata che l'addetto doveva trascrivere per cifrare o decifrare il messaggio. La chiave era costituita dalla posizione dei 3 rotori, che veniva cambiata ogni giorno secondo una regola matematica basata sulla data. Verso la fine del conflitto fu costruita anche una seconda macchina, la **Lorenz**, che rispetto all'Enigma presentava 12 rotori ed un sistema di cifratura basato sul **codice di Vernam** (proposto dall'omonimo ingegnere americano nel 1926 e fondato sull'utilizzo di una chiave lunga quanto il messaggio da cifrare)e su un algoritmo di cifratura simile a quello di Cesare ma dove invece della trasposizione delle lettere si usava la somma delle stesse tramite la rappresentazione di queste con il codice Baudot (una specie di codice binario inventato per le telescriventi basato sulla rappresentazione binaria a 5 cifre delle lettere dell'alfabeto).

Sia la macchina Enigma che la Lorenz non erano perfette: né lo erano i loro operatori… Fu l'insieme di queste 2 debolezze che permise a dei crittanalisti polacchi di violare le trasmissioni cifrate con l'Enigma ed ai calcolatori "**Colosso**" (i primi computer della storia) della Royal Air Force britannica di violare quelle cifrate con la Lorenz.

Nello stesso periodo gli USA dovevano fronteggiare il Giappone nell'Oceano Pacifico, il cui dominio si stava espandendo a macchia d'olio, arrivando lentamente a coprire tutte le isole della Polinesia e Micronesia. Le trasmissioni cifrate non erano sicure: i Colossi avevano dimostrato che la conoscenza crittografica di quei tempi non era sufficientemente progredita per creare un cifrario resistente agli attacchi di potenti elaboratori elettronici. Il Governo americano decise così di ricorrere all'antico: quale cifrario era più sicuro di un dialetto parlato da un ristretto numero di persone? Studiosi incaricati dal Governo iniziarono perciò a girare fra le tribù di pellerossa alla ricerca di un dialetto indiano da poter utilizzare per le comunicazioni segrete. Alla fine fu scelto quello parlato dalla tribù dei Navajo perché, fra tutti i dialetti, era l'unico che non avesse assolutamente nessuna somiglianza con qualsiasi lingua europea o asiatica ed anche perché le tribù Navajo erano le uniche che non erano mai state visitate da studiosi tedeschi (alleati dei Giapponesi). Indiani Navaho vennero quindi spediti al fronte, altri furono dislocati nei centri di trasmissione creando quel corpo che andava sotto il nome di NAC, **Native American Codetalkers** (*Parla-codice*). Ma il progetto doveva essere talmente segreto che nessuno sapeva del motivo per cui persone dai tratti non occidentali vestissero le divise americane. Così succedeva spesso che i Navajo venissero scambiati per spie giapponesi. Il Governo corse ai ripari affiancando al Navaho una specie di accompagnatore-tutore, un soldato informato della missione del Navajo e che, in caso di pericolo per il suo accompagnato, doveva spiegare la presenza di quello strano individuo. Ma, soprattutto, doveva proteggere il codice: così, in caso di cattura da parte dei Giapponesi, l'ordine dato al tutore era quello di uccidere il Parla-codice… Solo nel 1968 fu svelata questa cosa. Che sulla carta potrebbe sembrare anche semplice, ma in realtà non lo era: il linguaggio Navajo non comprendeva tutti i termini inglesi necessari alla trasmissione dei messaggi, così che fu approntato un codice vero e proprio. Così si decise di usare nomi di uccelli per gli aerei e di pesci per le navi. Ecco quindi che si parlava di "sparviero" per indicare un bombardiere, oppure di "gufo" per l'aereo-

spia; la “balena” era invece un incrociatore mentre lo “squalo” era il cacciatorpediniere. Per i termini che non potevano proprio essere sostituiti con qualche altro presente nel vocabolario Navajo si decise di utilizzare un sistema di trasmissione lettera per lettera mediante termini particolari.

Dopo i Parla-codice, un’altra tappa fondamentale è l’introduzione del **DES**, che ha rivoluzionato la crittografia e la crittanalisi a livello mondiale. Ma di questo parlo in un altro articolo.