IL CIFRARIO DI CESARE

Museo della Matematica “Lucio Lombardo Radice”

MAMIANI
LICEO STATALE - ROMA

PRESENTAZIONE

L'importanza di comunicare senza essere intercettati è sempre stata una necessità molto sentita fin dalla più remota antichità: re, papi, generali e addetti alle segreterie di stato, tutti hanno cercato di avere a disposizione dei sistemi per nascondere i loro segreti. Ognuno aveva al suo servizio qualche specialista in crittografia, che fosse capace di inventare algoritmi inviolabili. Per contro, l'Intelligence di queste stesse corti, mentre da un lato cercava di nascondere il vero significato dei propri dispacci, dall'altro si adoperava per carpire il segreto di quelli nemici intercettati. Poteva anche darsi che il "matematico" autore dell'algoritmo per criptare i messaggi fosse anche quello che cercava di mettere in chiaro gli scritti dei nemici, come un Giano bifronte: ma nel primo caso faceva della crittografia, mentre nel secondo si trasformava in un crittoanalista. Due mestieri simili, ma non uguali. In breve, si potrebbe dire che la storia della crittografia altro non è se non l'evolversi di algoritmi sempre più sofisticati, che vengono man mano inventati per sostituire i precedenti non più inviolabili. Criptare e decrittare non è un gioco per ragazzi con una certa predisposizione al calcolo matematico: se un tempo su quest'arte si reggevano intrighi, amori, potere e guerre, oggi il suo impiego civile è fondamentale per la sicurezza della nostra identità telematica, dell'intero sistema bancario e quindi dell'economia mondiale.

La crittografia è dunque lo studio di come scrivere messaggi in forma segreta in maniera tale che solo i destinatari autorizzati siano in grado di leggerli in chiaro e capirne così il contenuto. Un criptosistema, o sistema cifrato, è quindi un modo per rendere le comunicazioni più sicure.
Lo schema del sistema crittografico è il seguente:
• il mittente **M** prepara il messaggio **x**, testo in chiaro, da spedire;
• **M** applica al messaggio **x** una procedura, algoritmo di cifratura, definita da una chiave che genera il messaggio **y**, testo cifrato, da spedire al destinatario **D**;
• **D** riceve il messaggio **y** al quale applica un algoritmo di decifratura con chiave, riottenendo il testo in chiaro;
• un eventuale intruso che intercetta il messaggio cifrato **y** non deve poter risalire al messaggio **x**.

I criptosistemi più antichi sono tutti a “chiave privata” cioè chi invia il messaggio e chi lo riceve conoscono entrambi l'algoritmo che tramuta il messaggio da linguaggio naturale, in chiaro, in quello criptato e viceversa. La chiave è un segreto che il mittente e il destinatario conservano gelosamente. Il maggiore svantaggio dei sistemi a chiave privata è il fatto che due utenti devono scambiarsi una chiave in qualche modo sicuro prima di poter cifrare qualunque dato. Inoltre tali chiavi devono essere cambiate spesso e ciò costituisce sicuramente un problema a cui si è cercato di ovviare introducendo dei sistemi a “chiave pubblica”.

RIFERIMENTI STORICI

Svetonio nella *Vita dei dodici Cesari,* opera del II secolo d.C., scrive nel Cap I, paragrafo 56:

”Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si quis investigare et persequi volet, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.”

Dunque Giulio Cesare adoperava per le sue corrispondenze riservate un sistema crittografico per sostituzione. Questo cifrario monoalfabetico è il più antico algoritmo crittografico di cui si abbia traccia storica e il primo in cui si introduce l’uso di una chiave che è il modo con cui opera l’algoritmo di sostituzione delle lettere cifrate a quelle in chiaro. Risultò per molto tempo sicuro ed efficace grazie alle successive forme più raffinate che presero in considerazione per la cifratura tutte le possibili permutazioni delle lettere dell’alfabeto. Furono i crittoanalisti arabi attorno all'anno 1000 a trovare il punto debole della sostituzione monoalfabetica. L’idea vincente fu quella di notare che in ogni lingua le lettere dell’alfabeto appaiono con una loro frequenza caratteristica e il metodo di sostituzione non altera la statistica del messaggio. Da allora questi modelli crittografici divennero decifrabili.

Nella *Vita dei dodici Cesari*, Svetonio descrive l'uso del sistema ma non fornisce indicazioni per la realizzazione di un manufatto utilizzabile per la codifica.

IL MODELLO

Materiale: legno
Lunghezza: 46 cm
Larghezza: 9 cm
Listelli: 1.5 cm
Spessore: 1.5 cm

L’officina

DESCRIZIONE

Il nostro è un manufatto di applicazione del metodo crittografico di Giulio Cesare. È stato realizzato utilizzando due listelli mobili di legno, da incassare nelle apposite guide, e uno centrale fisso. Su ogni listello è stato applicato l'alfabeto italiano. Il listello mobile inferiore ci permette di spostare verso sinistra le lettere rispetto all'alfabeto centrale, il listello superiore ci permette invece di spostarle verso destra a completamento della sequenza alfabetica.

FUNZIONE

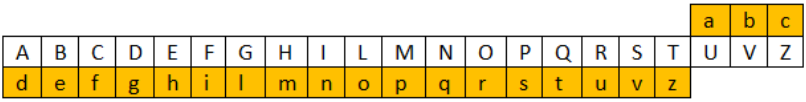
Il cifrario di Cesare è un sistema crittografico per sostituzione monoalfetica in cui l'alfabeto cifrante è ottenuto dall'alfabeto in chiaro traslando di k=3 posizioni le lettere. L'insieme di partenza e quello di arrivo sono costituiti dalle 21 lettere dell'alfabeto.

In questo metodo di cifratura si ha:

- l'alfabeto del messaggio in chiaro in lettere maiuscole
- l'alfabeto del messaggio cifrato in lettere minuscole
- la corrispondenza biunivoca tra i due alfabeti
- la chiave, definita dalla scelta del numero naturale k, con $0 < k < 21$.

MODALITÀ D'USO

Le lettere maiuscole dell'alfabeto chiaro sono gli elementi del listello centrale fisso. Si fa scorrere verso sinistra il listello inferiore fino a far corrispondere la lettera **d** con la **A** del fisso e quello superiore verso destra fino a far corrispondere la **a** con la **U**. Per la cifratura si legge ogni lettera **n** del testo in chiaro sul listello centrale e si trascrive la corrispondente **n'** sui listelli mobili. Operando così una traslazione ***n' = n + k***, con ***k* = 3**.



Esempio

testo in chiaro: CAESAR

testo cifrato: fdhvu.

Il numero delle chiavi possibili, ossia dei possibili cifrari, nel caso della lingua italiana, è 21 come le lettere dell'alfabeto, anzi 20, perché ovviamente se una lettera trasla di *k* = 21 posizioni il testo cifrato coincide con quello in chiaro.
Si può complicare la cifratura ricorrendo ad una funzione affine del tipo ***n' = a·n + k***, con **0 < *k* < 21** e il numero ***a*** primo con 21. Si passa così da 21 cifrari a 252, uno dei quali è ancora l'identità.

BIBLIOGRAFIA

C. SVETONIO TRANQUILLO, *Le vite dei Cesari*, a cura di G. Vitali, Vol. I, 56, Bologna, 1951 (Biblioteca Mamiani)
S. SINGH, *Codici & segreti,* Milano, 1999
A. GUERAGGIO, *Matematica*, Milano, 2012
R. BETTI, La crittografia, *Lettera Matematica Pristem*, n°49, 2003

Progetto Alternanza Scuola Lavoro
realizzato in collaborazione con

ROMA
Sovrintendenza Capitolina ai Beni Culturali
U.O. Musei Scientifici e Planetario-Museo Civico di Zoologia
Museo della Matematica

OFFICINE TERENZIO

Responsabile: Patrizia Cassieri
Tutor esterni: Wilma Di Palma (Comune di Roma), Ezio Bonfanti,
Diego Urbani (Officine Terenzio)
Tutor interni: Nicoletta Allegretti, Alessandra De Angelis
Studenti: Irene Azzara (Project Manager),
Lorenzo Riola (Chief Engineer), Pietro Salviati (Workshop Assistant)
Giovanni Mancini (Art Director),
Renato Bettini (Webmaster), Adriano Consolo (Web Designer)
Francesca Valeria Samà, Francesca Agostinelli, Giorgia Sacco (Writers)

www.mamianilab.it/oa