LA SCACCHIERA DI POLIBIO

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”.

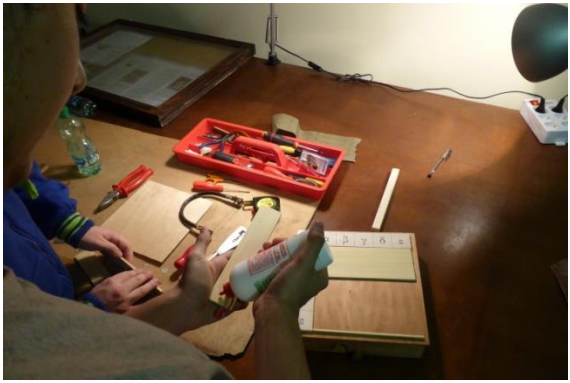
RIFERIMENTI STORICI

Polibio nato a Megalopoli, in Arcadia, tra il 205 - 200 a. C., storico greco, ricoprì incarichi militari di grande prestigio, arrivando nel 170 a.C. ad occupare la carica di ipparco, comandante di uno squadrone di cavalleria.
L'opera principale di Polibio, *Storie*, nasce direttamente dalla sua esperienza personale e narra le guerre puniche, documentando l'ascesa di Roma da potenza locale della penisola italica a dominatrice assoluta e incontrastata della realtà mediterranea
Polibio ideò il più antico codice poligrafico. Lo storico greco lo descrive come un metodo per inviare messaggi mediante l'uso di torce, come fosse un telegrafo ottico. Questo "telegrafo a fiaccole", nato come sistema di comunicazione a distanza divenne nei secoli successivi un sistema crittografico. Utilizzato dai Romani per le trasmissioni lungo le vie consolari e quelle costiere, il codice, adattabile a qualsiasi lingua, fu alla base di macchine cifranti fino alla Prima Guerra Mondiale.
Esso può essere applicato anche come cifrario a colpi, quello, per esempio, usato dai detenuti: il messaggio viene battuto lasciando una pausa breve tra i due numeri che sostituiscono la lettera e una pausa più lunga tra una lettera e l'altra.

Nel passo delle *Storie* (X,45-47), Polibio descrive l'uso del sistema ma non fornisce indicazioni per la realizzazione di un manufatto utilizzabile per la codifica.

IL MODELLO

Materiale: legno
Supporto: 25.5 cm x 25.5 cm x 5.5 cm
Scacchiera: 20 cm x 20 cm
Listelli: sei da 4 cm x 20 cm, uno da 24 cm x 4 cm
Spessore: 0.5 cm



L’officina

DESCRIZIONE

Il nostro è un manufatto di applicazione del codice di Polibio. È costituito da una griglia contenente le lettere maiuscole dell'alfabeto greco posta su un cassetto con apertura basculante. Tutte le lettere, necessarie alla codifica, sono state stampate ed incollate sulle apposite sagome in compensato che, dopo il taglio, sono state limate per raffinare i bordi. Per completare il modello e far risaltare lucentezza e colore sono stati applicati tintura per legno e vernice acrilica.

FUNZIONE

La scacchiera di Polibio è un cifrario per sostituzione che associa ad ogni lettera dell'alfabeto in chiaro una coppia ordinata di numeri. L'insieme di partenza è costituito dalle 24 lettere maiuscole dell'alfabeto greco, quello di arrivo dai primi cinque numeri, che i greci scrivevano utilizzando le lettere minuscole del loro alfabeto.

In questo metodo di cifratura si ha:

- l'alfabeto del messaggio in chiaro
- l'alfabeto del messaggio cifrato
- la corrispondenza biunivoca tra i due alfabeti, definita dalla forma della scacchiera
- la chiave, definita dalla particolare permutazione delle lettere poste sulla scacchiera.

MODALITÀ D'USO

Le lettere dell'alfabeto sono gli elementi di una tabella quadrata 5x5. Per la cifratura si legge la lettera del testo in chiaro sulla tabella e si trascrivono, nell'ordine, i numeri corrispondenti di riga e di colonna (Esempio 1). Per la decifratura, poiché la funzione cifrante è biunivoca, si legge la coppia ordinata di numeri e si individua la lettera corrispondente (Esempio 2).

	α	β	γ	δ	ε
α	A	B	Γ	Δ	E
β	Z	H	Θ	I	K
γ	Λ	M	N	Ξ	O
δ	Π	P	Σ	T	Y
ε	Φ	X	Ψ	Ω	

Esempio 1

testo in chiaro: **Π O Λ Y B I O Σ (Polibio)**

testo cifrato: **δα γε γα δε αβ βδ γε δγ**

Esempio 2

testo cifrato: **εβ αα βδ δβ αε**

testo in chiaro: **X A I P E (Salve)**

BIBLIOGRAFIA

S. SINGH, *Codici & segreti,* Milano, 1999
C. TOFFALORI, *Algoritmi*, Bologna, 2015
A. GUERAGGIO, *Matematica*, Milano, 2012
R. BETTI, La crittografia, *Lettera Matematica Pristem*, n°49, 2003

oggettivamente astratto

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