IL DISCO DI ALBERTI

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.

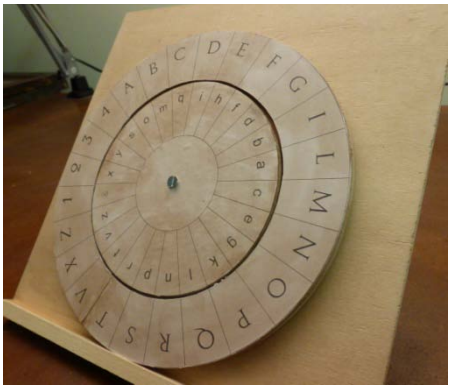
Lo schema del sistema crittografico è il seguente:
• il mittente **M** prepara il messaggio **x**, testo in chiaro, da spedire;
• **M** applica al messaggio **x** una procedura, algoritmo di cifratura, definita da una chiave che genera il messaggio **y**, testo cifrato, da spedire al destinatario **D**;
• **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

Leon Battista Alberti (Genova 1404 - Roma 1472), una delle figure più significative dell'Umanesimo italiano, di cui seppe interpretare le ambiguità e gli splendori, contribuì, attraverso i suoi studi, a tracciare una nuova mappa di valori critici e un diverso metodo di interpretare il mondo. Alberti fu un pensatore e uno scienziato "universale", dai mille interessi e ribelle ad ogni definizione: è stato al tempo stesso un grande architetto, un matematico, un fine letterato, un latinista, un musicista, un uomo di Chiesa e un astuto diplomatico. Nel primo trattato di storia della crittografia, *De componendis Cyfris* (1467), egli, con approccio scientifico, analizza l'uso delle vocali, delle consonanti e la frequenza delle lettere nelle parole. Comprende, così, le inefficienze dei sistemi monoalfabetici e, al fine di renderli meno vulnerabili, introduce un codice crittografico polialfabetico che applica attraverso il **Disco cifrante**, primo dispositivo nella storia della crittografia. Il testo rimase volutamente inedito e fu dato alle stampe solo nel 1568. Da allora divenne punto di partenza ineludibile per storici della matematica e studiosi di crittografia. Nel metodo di Alberti gli alfabeti sono due e la chiave varia in continuazione durante la codifica. Dunque, lo studio delle frequenze non dà risultati perché la stessa lettera chiara è cifrata sempre con lettere diverse. Enigma, utilizzata dai nazisti nel corso della Seconda Guerra Mondiale, è considerata la versione elettromeccanica ed evoluta del disco cifrante di Leon Battista Alberti.

IL MODELLO



Materiale: legno
Ø esterno:20 cm
Ø interno: 13 cm
Spessore: 0.5 cm

L’officina

DESCRIZIONE

Il nostro modello è costituito da due cerchi concentrici, uno esterno fisso e l'altro libero di ruotare, sui quali sono incollate sagome di carta. Quello di minor raggio contiene, con caratteri minuscoli, le lettere dell'alfabeto cifrante in ordine casuale, escluse j - u - w, e il simbolo & che sta ad indicare la congiunzione latina *et*. Sulla corona circolare fissa sono presenti: l'alfabeto ordinario a caratteri maiuscoli, escluse le lettere H - K - J - U - Y - W, e i numeri 1, 2, 3, 4 per la scrittura del messaggio in chiaro. Nel modello non compare la lettera u per rispettare l'uso comune della scrittura dell'epoca che considerava equivalenti le lettere v e u. Per rendere solida la struttura è stata ritagliata una terza sagoma in legno che funge da supporto. Il tutto è stato trattato con il mordente per fornire all'oggetto un aspetto anticato.

FUNZIONE

Il crittografo di Alberti è un dispositivo meccanico che realizza permutazioni variabili delle lettere dell'alfabeto. Di questo oggetto devono esistere due copie: una in uso al mittente e l'altra per il destinatario. Essi concordano segretamente la chiave cifrante costituita da una coppia di caratteri che determinano la corrispondenza iniziale tra i caratteri del disco di diametro maggiore e quelli del disco interno. Al termine di questa procedura i due interlocutori sono pronti a scambiarsi i loro messaggi segreti.

MODALITÀ D'USO

Per crittografare una frase utilizzando il nostro modello, il mittente deve applicare il seguente algoritmo;
1) eliminare gli spazi tra una parola e l'altra, gli accenti e gli eventuali segni di interpunzione ed inserire a caso, nel mezzo del testo chiaro, anche le cifre da 1 a 4;
2) inizializzare il disco con la chiave concordata. (A,c) nell'**Esempio**;
3) ad ogni lettera del messaggio in chiaro, letta sul disco fisso, si associa la lettera corrispondente sul disco mobile e si procede in tal modo fino a che non si incontra un numero, per esempio 1. A questo punto, dopo aver cifrato il carattere 1 con la lettera minuscola corrispondente, per noi f, si effettua un cambiamento della chiave. Poiché la prima chiave concordata era la coppia (A, c) adesso la nuova chiave è la coppia (A, f). Si itera il procedimento, cambiando chiave all'occorrenza.

Esempio

Si concorda la **chiave (A, c)** e si applica l'algoritmo.

Testo: **Cifrario di Alberti →CI1FRA4RIODI2ALBE3RTI → grfezfhvgpbgmmcqfslpd.**

Per la decodifica il ricevente deve inizializzare il disco, come prevede la chiave concordata, e, questa volta, partire dal disco mobile per leggere i caratteri corrispondenti alle lettere e ai numeri della frase cifrata, risalendo così al testo in chiaro.

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
P. PRETO, I servizi segreti di Venezia, Milano 2010

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