Per saperne di più

Leon Battista Alberti (a cura di Augusto Bonafalce), *De componendis cyfris* , Torino, Galimberti , 1998

R. Betti, *La crittografia* , in Alice & Bob , (supplemento a) Lettera Matematica Pristem 61, pp.021-028

P. Ferragine, F. Luccio, *Crittografia. Principi, algoritmi, applicazioni.* Torino, Bollati Boringhieri 2001

E. Garin, *Studi su Leon Battista Alberti* , Bari, Laterza 1976

D. Kahn, *On the origin of polyalphabetic susbtitution,* ISIS (256) 1980, pp.122-127

S. Singh, *Codici e segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet,* Milano, BUR, Saggi 2001

G. Wolff, *Leon Battista Alberti als Mathematiker* , Scientia LX 1936 pp.553-556

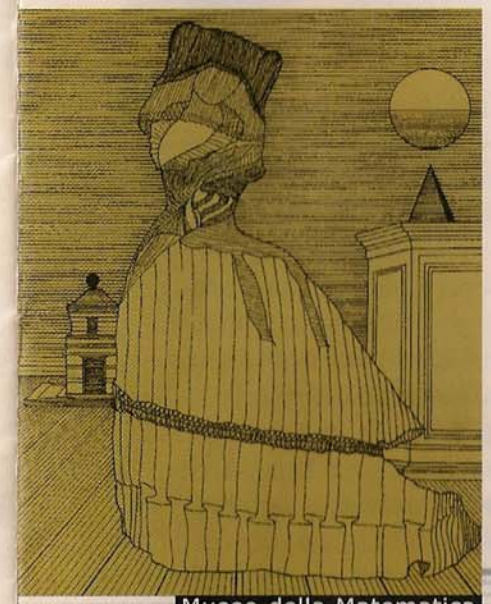
MUSEI SCIENTIFICI ROMA

Direttore: Vincenzo Vomero
Responsabile Museo della Matematica
"I Racconti di Numeria": Wilma Di Palma

Comune di Roma
Assessorato
alle Politiche Culturali

Sistema dei Musei Scientifici
della Sovraintendenza comunale
Museo della Matematica
"I Racconti di Numeria"

LAit LAZIO innovazione tecnologica



Kit interattivo per l'uso del crittografo di Leon Battista Alberti

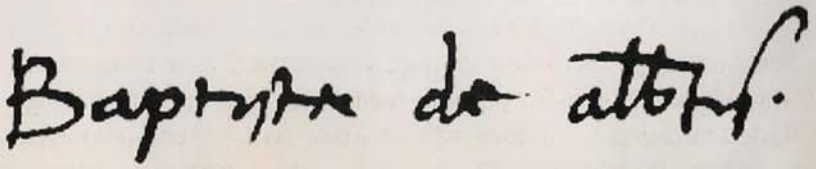
Museo della Matematica
"I Racconti di Numeria"

Si ringrazia:

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI MATEMATICA
"GUIDO CASTELNUOVO"

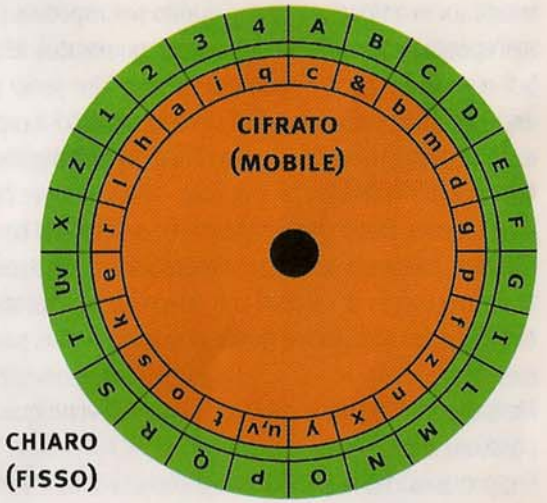
Leon Battista Alberti (Genova 1404 - Roma 1472) è una delle figure più significative dell'Umanesimo italiano, di cui seppe interpretare le ambiguità e gli splendori, contribuendo a tracciare una nuova mappa di valori critici ed un diverso modo d'interpretare il mondo. Alberti fu, dunque, un pensatore ed 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 ed un astuto diplomatico.

Fu proprio rivestendo i panni di funzionario vaticano che gli venne in mente - su sollecitazione di un suo amico, segretario particolare del Papa - di progettare un nuovo modo per inviare i dispacci diplomatici, senza temere che fossero intercettati dai nemici. Alberti elaborò così un sistema semplice e geniale, che riusciva a farsi beffe delle spie e che è spesso considerato il primo sistema di crittografia moderno. Alberti descrisse questo suo metodo per cifrare i messaggi in un piccolo libro, il *De componendis Cyfris*. Ma, per ovvie ragioni di sicurezza, il testo rimase inedito e fu dato alle stampe solo nel 1568, quasi un secolo dopo la morte dell'autore. Da quel momento restò un vero classico del genere, un punto di partenza ineludibile per storici della matematica e studiosi di crittografia. Questo lavoro, pur non trattando direttamente di argomenti classici di matematica, rappresenta tuttavia un esempio di applicazione di alcuni suoi metodi. Infatti, per portare in chiaro un messaggio cifrato occorre un lavoro razionale che molto assomiglia al rigore logico che un matematico deve impiegare nella dimostrazione di un teorema e non è un caso se al giorno d'oggi, chi si occupa di crittografia è spesso un matematico di professione. La crittografia è, attualmente, una branca della matematica: questa concezione applicativa del pensiero astratto è - per i tempi di Alberti - una vera e propria rivoluzione intellettuale. Per il Nostro, infatti, la matematica non era un ramo isolato dell'attività umana, ma un elemento fondamentale della società, al cui benessere e progresso contribuiva con il suo metodo, fornendo strumenti preziosi per lo sviluppo delle arti e della tecnologia.



§ 1. Il disco cifrante

Cifrare un messaggio a partire da un testo in chiaro significa sostituire ciascuna sua lettera con un'altra, mediante una qualche legge fissata, che - invertita - consenta la sua decifrazione.



Un criptosistema si dice **monoalfabetico** se ciascuna lettera viene sempre sostituita da un'altra ben determinata. Si dice, invece, **polialfabetico** se la lettera che sostituisce quella del testo in chiaro dipende sia dalla lettera stessa che dalla sua posizione nel messaggio. Ad esempio, un criptosistema monoalfabetico è quello attribuito a Giulio Cesare, dove ogni lettera viene sostituita da quella che la segue di tre posizioni nel consueto ordine alfabetico. Per fare invece un semplice esempio di criptosistema polialfabetico, possiamo suddividere il testo in chiaro in stringhe tutte della medesima lunghezza ed applicare a ciascuna di esse un diverso sistema monolfabetico: ad esempio, nella prima stringa sostituiamo ciascuna lettera con

quella che la segue di tre posti, nella seconda con quella che la segue di sette posti, nella terza con quella che la segue di quattro e così via.
Pertanto, un concetto fondamentale in crittografia è quello di **permutazione:** se S è un insieme di **n** oggetti, una permutazione di S non è altro che un "riordinamento" dei suoi elementi. Ad esempio: 3,5,4,1,2 è una permutazione di 1,2,3,4,5.
Il crittografo di Alberti realizza permutazioni variabili delle lettere dell'alfabeto mediante un dispositivo meccanico: il **disco cifrante.** Di questo dispositivo - due cerchi concentrici con diametro diverso e ciascuno diviso in 24 caselle - devono esistere due copie: una in uso al mittente ed una per il destinatario. Sulle caselle dei cerchi - grande e piccolo - si riportano le lettere dell'alfabeto. Sul disco grande si riportano - scritte in maiuscolo - tutte le lettere dell'alfabeto nel naturale ordine alfabetico, meno le lettere H,K,Y, W e J. Sul disco piccolo si riportano tutte le lettere minuscole in ordine casuale incluse h, k, y ed in più il simbolo & che sta ad indicare la congiunzione latina *et* . Si noti che Alberti assegna una sola casella alle lettere u,v in ambedue i dischi: questo per rispettare l'uso comune della scrittura dell'epoca che considerava equivalenti queste due lettere.
Sul cerchio maggiore - cioè quello fisso che serve per il testo in "chiaro" - si inseriscono anche le cifre da 1 a 4 che servono a cambiare chiave e - quindi - a dare maggiore sicurezza al testo cifrato. Il cerchio grande e quello piccolo sono fissati al centro in modo che il minore - che si usa per cifrare il testo - possa ruotare a piacimento. Dopo che il mittente e il destinatario hanno concordato una "chiave cifrante", che serve ad iniziare l'operazione di cifratura e che deve essere costituita da una coppia di caratteri che determinano la corrispondenza iniziale tra le lettere del disco maggiore e quelle di quello minore, siamo pronti a cifrare qualsiasi messaggio.
Mettiamo che la chiave sia (A,c): i dischi devono quindi essere inizialmente nella posizione del disegno.
Supponiamo che le due parti vogliano scambiarsi il seguente messaggio:

Numeria è la dea della matematica

Il mittente, per crittografare questa frase, deve fare le seguenti operazioni:
i) eliminare gli spazi tra una parola e l'altra, gli accenti e gli eventuali segni di interpunzione ed inserire, a caso, le cifre da 1 a 4 nel mezzo del testo, ad esempio:

Nume1riaela4deadella3mate2mat4ica

ii) ad ogni lettera del messaggio in chiaro, lettera che va letta sul disco fisso, si associa la lettera corrispondente sul disco piccolo mobile e si procede in tal modo fino a che non si incontra un numero. A questo punto la lettera corrispondente al numero determina un cambiamento di disposizione della chiave: alla lettera A - la prima della nostra chiave concordata - si fa corrispondere la lettera minuscola che corrisponde al numero 1, nel nostro caso la nuova chiave è (A,h). Si procede allo stesso modo, cambiando chiave all'occorrenza, per tutto il messaggio da cifrare.
Nel nostro esempio, dal testo in chiaro:

NUME1RIAELA4DEADELLA3MATE2MAT4ICA

si ottiene il seguente messaggio cifrato:

x e n d h x m h c d h l i q l i q m l e b e n a o q o p t h s t

Si noti come le lettere doppie del testo in chiaro - nel nostro caso la doppia elle - nel sistema di Leon Battista Alberti vengono accorpate in una sola lettera nel messaggio cifrato.

§2. Decifrare un messaggio criptato

Proviamo ora a decifrare il seguente messaggio:

fznesdymdzcnckqmzqsp&qbpln
pdlxbabldlecfeldmnchcmxbafce

Poniamo per prima cosa il nostro disco nella posizione (A,c) come prevede la nostra chiave concordata e incominciamo a fare l'operazione inversa di quella fatta da chi ha cifrato il messaggio: partiamo dal disco piccolo e leggendo a cosa corrispondono le lettere della nostra frase cifrata risaliamo al testo in chiaro.

f=I; z= L; n= M; e=U; s = S; d= E; y= O;

m=D; d=E; z= L; c= A; n= M; c= A; k= T; q=4

ILMUSEODELAMAT4 , ovvero, IL MUSEO DELLA MAT4

Avendo trovato il numero 4, dobbiamo spostare la chiave da (A,c) in (A, q) e procediamo come sopra, ottenendo:

m=E; z=M; q=A; s=T; p=I; &=C; q= A; b=D; p= I; l=1

EMATICADI1

Unendo questo spezzone con la frase precedente si ottiene:

IL MUSEO DELLA MATEMATICA DI 1

Avendo trovato il numero 1, dobbiamo spostare la chiave da (A,q) in (A,l) e procedere a porre in chiaro il testo cifrato come al solito:

n=R; p=O; d=M; l=A; x=S; b= I; a=C; b=I; l= A;
d=M; l=A; e=3

Ovvero:
IL MUSEO DELLA MATEMATICA DI ROMA SI C (H) IAMA3...

Il metodo per decifrare il messaggio misterioso dovrebbe essere a questo punto chiaro per tutti:
Finisci tu di decifrare il messaggio ed otterrai l'indicazione di un luogo dove sarai sempre il benvenuto!

§ 3. Che cosa succede oggi in crittografia?

Il disco cifrante di Leon Battista Alberti genera un criptosistema polialfabetico nel quale si hanno una "macchina cifrante", il disco stesso, una chiave privata - o simmetrica, nota soltanto a mittente e destinatario - la quale deve venire trasmessa attraverso un canale sicuro, cioè che non consenta ad alcuna persona non autorizzata di impadronirsene. Dispositivi analoghi sono stati utilizzati fino alla prima guerra mondiale. Successivamente, vennero resi più complessi e le "macchine" cifranti usate durante la seconda guerra mondiale utilizzavano, essenzialmente, dispositivi meccanici ed elettromeccanici, che forniscono sequenze di dischi cifranti. Quindi, in ogni caso, si trattava dell' utilizzazione di sequenze di diverse permutazioni, applicate sia agli elementi del testo vero che ad insiemi di questi. L'avvento dei calcolatori ha sostituito le macchine cifranti con programmi, i quali effettuano tutte le opportune permutazioni e rimescolamenti dei blocchi del messaggio ed utilizzano una chiave privata, che - di solito - viene a sua volta suddivisa in "subchiavi", ciascuna delle quali viene adoperata in una fase del processo di cifratura. Un esempio di tale criptosistema è il **DES** (Data Encryption Standard), tuttora in uso. Anche qui, come in tutti i criptosistemi a chiave simmetrica, la medesima chiave viene utilizzata sia per cifrare che per decifrare. La necessità di scambiarsi tale chiave attraverso un canale sicuro ha suggerito (1976) l'idea di un criptosistema a **chiave pubblica.** L'idea di base è semplicemente quella di usare chiavi diverse per cifrare e per decifrare. Ciò consente di rendere pubblica la chiave che occorre per inviare un messaggio ad un certo utente, il quale è il solo che, possedendo la sua chiave privata, è in grado di decifrarlo. I criptosistemi a chiave pubblica si basano sempre su un problema matematico ritenuto non risolvibile, cioè la cui risoluzione richiede tempi lunghissimi e capacità computazionali molto elevate. Nel **RSA** (dai nomi degli inventori Rivest, Shamir ed Adleman) questo problema è quello di fattorizzare un intero che sia prodotto di due numeri primi distinti e sufficientemente grandi (almeno dell'ordine di 2^{160} oppure meglio ancora 2^{1024}). I criptosistemi a chiave pubblica vengono utilizzati per scambiarsi chiavi private da usare in criptosistemi come il DES, per le firme digitali, per la protezione delle carte di credito ed altre cosiddette "*smart cards*".

Marialuisa J. de Resmini*
Wilma Di Palma**

* Docente di Algebra. Dipartimento di Matematica. Sapienza Università di Roma
** Museologa, Storica della Matematica. Responsabile del Museo della Matematica del Comune di Roma " I Racconti di Numeria"

R S T Uv X Z 1 2 3 4 A B C D E F G I L M N O P Q
z n x y u,v t o s k e r l h a i q c & b m d g p f

M N O P Q R S T Uv X Z 1 2 3 4 A B C D E F G I L
d g p f z n x y u,v t o s k e r l h a i q c & b m