I "dischi cifranti" di Leon Battista Alberti

Paolo Severino Manca*

DOI:10.30449/AS.v9n18.164

Ricevuto 3-10.2022 Approvato 20-12-2022 Pubblicato 31-12-2022

Sunto: *Viene illustrato un contributo del genio universale Leon Battista Alberti nel campo della crittografia ; contributo importante a lungo ignorato e ripreso solo dopo quasi 500 anni con la macchina Enigma nella seconda guerra mondiale.*

Parole Chiave: dischi cifranti, crittografia classica, macchina Enigma.

Abstract: *A contribution by the universal genius Leon Battista Alberti is illustrated in the field of cryptography; important contribution long ignored and revived only after almost 500 years with the Enigma machine in the Second World War.*

Keywords: cipher disks, classical cryptography, Enigma machine.

Citazione: Manca P.S, *I "dischi cifranti" di Leon Battista Alberti*, «ArteScienza», Anno IX, N. 18, pp. 31-42 DOI:10.30449/AS.v9n18.164.

Di Leon Battista Alberti riporto quanto riferisce la Treccani :

> Letterato e architetto (Genova 1404, da padre bandito da Firenze - Roma 1472). Appassionato di letteratura ma anche di

* Già Professore Ordinario di Matematica Finanziaria all'Università di Pisa; paolo.severino.manca@gmail.com.

matematica, scrittore e grande architetto, pedagogista e teorico dell'arte, uomo di studi ma anche atleta, sintetizzò nella sua opera i caratteri tipici dell›Umanesimo: la curiosità per il vasto spettacolo del mondo; l'amore per gli antichi, in modo particolare per i Romani; la passione per le arti come suprema manifestazione della creatività umana e come ricerca dell'armonia; l'ideale dell'uomo virtuoso, che cerca di forgiare il proprio destino. L'arte dell'A. fu decisiva per i successivi sviluppi della architettura del Rinascimento. Dallo studio dei monumenti antichi l'A. ricavò un senso delle masse murarie e del movimento ben diverso dalla limpida semplicità del Brunelleschi, e se ne valse in modi originali che precorsero l'arte del Bramante.

Sottoscrivo ma lamento tuttavia che nessun riferimento venga fatto a un suo contributo nel campo della crittografia che si è rivelato a posteriori particolarmente significativo.

Per contro devo apprezzare quanto riferisce Wikipedia che richiama il suo libro *De cifris* del 1466 e cita il giudizio dello storico della crittologia David Kahn (1967) che attribuisce all'Alberti il titolo di padre della crittologia occidentale : *father of western cryptology.*[1]

Fig. 1 - Ritratto di Leon Battista Alberti. (1588), attribuito a Cristofano Dell'altissimo. Galleria degli Uffizi.

E in effetti di tutti i cifrari creati nel passato e fino alla nascita dei cifrari asimmetrici negli anni '70 del secolo scorso, i cifrari basati sul principio dei dischi rotanti dell'Alberti appaiono come i più sicuri ed efficienti.

Il principio dei dischi rotanti di Alberti è geniale e al tempo stesso semplice e insisto sul binomio genio-semplicità proprio perché il genio si manifesta quasi sempre nel vedere diversamente qualcosa di semplice che è sotto gli occhi di tutti e che nessuno vede : mi viene in mente Picasso che vede una testa di

1 La versione digitale del testo latino originale del *De componendis cifris* di Leon Battista Alberti è disponibile online all'indirizzo http://www.apprendre-en-ligne.net/crypto/alberti/decifris.pdf

Fig. 2 - Disco cifrante di Leon Battista Alberti.

toro nel sellino e nel manubrio di una bicicletta da corsa, Newton che vede la mela e la terra che si attraggono,

Il principio dei dischi cifranti di Leon Battista Alberti si descrive meglio con riferimento a due corone circolari concentriche , una fissa e l'altra ruotabile.

Sulla corona fissa, suddivisa in tacche, sono riportate in ordine le lettere dell'alfabeto, sulla corona rotante, in altrettante tacche, è riportata una permutazione[2] delle medesime lettere.

Se le due corone restassero sempre ferme, poiché la permutazione della corona ruotante fornisce una corrispondenza biunivoca tra le lettere dell'alfabeto e una permutazione di tali lettere, avremmo un cifrario monoalfabetico, cosiddetto di Cesare, avente come chiave proprio la permutazione della seconda corona.

Con 21 lettere le permutazioni sono 21! : un numero mostruoso che tuttavia serve a poco perché, con la struttura della lingua italiana (o comunque di una lingua conosciuta), è molto facile decriptare un messaggio cifrato anche senza conoscere la chiave: per l'italiano basta ad esempio notare che quasi tutte le parole terminano con una vocale , che le parole bilettere o trilettere sono veramente poche ; del resto la "Settimana Enigmistica" propone spesso l' "aneddoto cifrato" basato proprio su una permutazione delle lettere e che si risolve in qualche minuto.

2 Le permutazioni di *n* oggetti sono tutti i gruppi che si possono formare con gli *n* oggetti scambiandone l'ordine. Il loro numero è *n*! (fattoriale di *n*) = *1* x 2 x 3x...X (*n-1)* x *n,* ovvero il prodotto dei primi *n* numeri naturali. Il fattoriale di un numero cresce molto rapidamente al crescere del numero.

La trovata geniale del cifrario dell'Alberti consiste, ogni volta che sia criptata una lettera del messaggio in chiaro, di ruotare, secondo un intervallo o una serie di intervalli concordati, la corona mobile ; in questo modo ogni successiva lettera in chiaro viene criptata secondo una nuova e diversa permutazione delle lettere dell'alfabeto. In questo modo ogni analisi statistica del messaggio criptato diventa non interessante poiché alla stessa lettera del messaggio in chiaro corrispondono via via diverse lettere del messaggio criptato.

Così ad esempio se la permutazione iniziale del disco ruotante è la seguente :

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

e, ogni volta criptata una lettera, si conviene di ruotare in senso orario di una tacca la corona mobile, la seconda lettera da criptare farà riferimento alla nuova permutazione :

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

Con questa regola ad esempio la parola NONO diventa DDQQ, la parola NONNO diventa DDQPP, la parola MAMMA diventa COPNL.

La regola di ruotare di una tacca ogni volta il disco mobile è la più semplice ma ovviamente si può decidere di diversificare di volta in volta le regole dello spostamento, ad esempio ruotare ogni volta il disco mobile di un numero diverso di tacche, magari anche in dipendenza della lettera da criptare.

Alberti , oltre ai dischi cifranti, propose anche un altro sistema di cifratura polisillabica ma le sue proposte non ottennero il successo che avrebbero meritato soprattutto per la decisione dell'Alberti di tenere segreto il suo trattato, che fu pubblicato postumo, nella traduzione in italiano di Cosimo Bartoli, nel 1568 a Venezia e passò quasi inosservato.

Sembra comunque che i manoscritti del trattato fossero arrivati

ben prima del 1568 in diverse Cancellerie, sicuramente a Roma e a Venezia ed erano quindi noti ai cifristi vaticani e veneziani, essi però preferirono sempre l'uso dei nomenclatori a cifre polialfabetiche , in particolare il cifrario di Vigenère, considerate più adatto per messaggi molto lunghi perché più facile da utilizzare e con minor possibilità di errori di "distrazione" da parte degli addetti alla cifratura.

In effetti per utilizzare il cifrario di Alberti e criptare in tempi ragionevoli occorreva disporre fisicamente di coppie delle due corone con la necessità di costruire e segretare tali oggetti fisici. Era anche facile che il criptatore commettesse qualche errore nello spostare di volta in volta il disco rotante.

E tuttavia mentre il cifrario di Alberti non si presta ad essere violato se non con "la forza bruta", il cifrario di Vigenere , ritenuto per secoli inattaccabile, risulta più attaccabile come del resto tutti i cifrari polialfabetici: questi infatti rispettano la struttura linguistica del messaggio in chiaro e dunque possono venire violati attraverso l'esame delle frequenze con cui compaiono nel messaggio cifrato le polisillabe.

Non è questo il luogo per richiamare note questioni di crittografia classica[3] ma per evidenziare l'originalità della proposta dell'Alberti vale la pena accennare alle caatteristiche del ben più noto cifrario di Vigenere.[4]

Il cifrario di Vigenere prende spunto dal cifrario di Giulio Cesare e certamente si rifà al trattato esoterico *Steganographia* di Johannes Trithemius, pseudonimo umanista di Johann Heidenberg (1462 –1516).

Nel cifrario di Vigenere le lettere dell'alfabeto vengono rappresentate da altrettanti numeri quindi viene scelta una parola chiave detta "verme" da concordarsi tra mittente e destinatario.

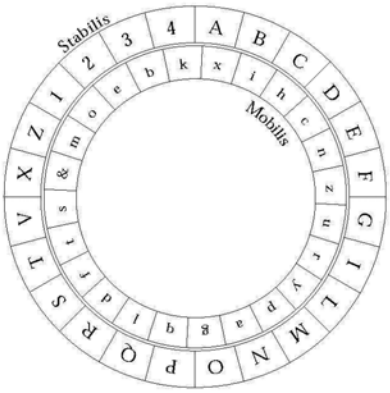
Di fatto per effettuare la criptazione:

1. sotto il messaggio in chiaro, lettera per lettera, si ripete la parola chiave. Ad esempio se la parola chiave è "armi" e il testo in chiaro è "arrivano i rinforzi" abbiamo:

3 Reperibili faciemente anche sul web

4 Blaise de Vigenere, vissuto tra il 1523 e il 1596, era un diplomatico francese che raccolse ed espose le conoscenze crittografiche del tempo nell'opera *Traitè des chiffres* pubblicato nel 1586.

XVII
Formula



1 Forma seu exemplum Rotae et tabellarum scilicet stabilis et mobilis, quae supra à nobis descripta et declarata fuit hic sequitur. *2ª m. exhibit tit. tantum* Ch. - figura: *om.* Co x; *tacent* La Pa; *in ultima charta* y*; *2ª m.* Ch

2 Mobilis: Stabilis - Mobilis *tantum* Fe

3 *Circulus stabilis*
A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4 *codd.*; *deleta* H Ch;
A B C D E F G H I K L M N O P Q R S T V X Y Z **2** Va;
A B C D E F G H I K L M N O P Q R S T V X Y Z - Mr

Circulus mobilis
om. Ba;
u s q o mk h f d b Ac e g i l n p r t x z & y Ar Fe Va Lt;
V S Q O M K H F D B A C E G I L N P - R T X Z 7 Mr;
X I H C N Z V R Y P A G Q L D F T S & M O E B K R²;
z y x u r o n mi l h g e d c b a &q t p s f k Ch

4 Tit.: Tabulae numeralium *tantum* x Va;
Sequitur tabula numerorum superius descriptorum *1ª m.* Ch - 12-Naves quas polliciti sumus militi frumentoque paravimus *in marg.* Ar Fe; *recepit* Ba

Fig. 3 - La pagina del *De componendis cifris* di Leon Battista Alberti dove è raffigurato il disco cifrante.

Testo chiaro	A	R	R	I	V	A	N	O	I	R	I	N	F	O	R	Z	I
Verme	A	R	M	I	A	R	M	I	A	R	M	I	A	R	M	I	A

2. si parte da una numerazione iniziale concordata delle lettere dall'alfabeto. Ad esempio nel caso più banale:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

3. si costruisce la sequenza che corrisponde in tal caso al verme Ad esempio se il verme è la parola "armi" la sequenza del verme è :

A	R	M	I
1	16	11	9

4. si allineano su due righe i numeri corrispondenti al testo in chiaro e la sequenza del verme ripetuta quanto basta per raggiungere il numero delle lettere del testo in chiaro. Matematicamente il metodo si riduce a un'addizione modulo 21, numero delle lettere dell'alfabeto italiano , ovvero modulo 26 nell'alfabeto internazionale.[5] Proseguendo nell'esempio con chiave "armi" e testo in chiaro "arrivano i rinforzi", passando ai numeri corrispondenti abbiamo:

5 Addizione modulo 21 significa che si applica l'addizione soltanto ai primi 21 numeri interi (0,1,2,3...20). I risultati sono ben diversi dalla normale addizione definita sull'insieme N degli infiniti numeri naturali. Infatti il secondo addendo dell'addizione modulo 21 aggiunge al primo addendo tanti numeri interi quanti ne indica rimanendo però sempre all'interno dell'insieme dei primi 21 numeri interi e quindi, nel caso in cui si supera il numero 20, si continua a contare riprendendo da 0. Per esempio 3 + 20 (mod 21) = 2. In pratica basta sottrarre il modulo (21) dalla somma che si otterrebbe nell'insieme infinito dei numeri interi (3+20-21 =2). L'aritmetica modulare fu creata da Carl Friedrich Gauss nel 1801nel trattato *Disquisitiones Arithmeticae*

Testo chiaro	1	16	16	9	20	1	12	13	9	16	9	12	6	13	16	21	9
Verme	1	16	11	9	1	16	11	9	1	16	11	9	1	16	11	9	1

5. si sommano modulo 21 (numero di lettere dell'alfabeto) le colonne ottenute. Proseguendo nell'esempio :

Testo cifrato	2	11	6	18	21	17	2	1	10	11	20	21	7	8	6	9	10
Verme	B	M	F	T	Z	S	B	A	L	M	V	Z	G	H	F	I	L

Risulta chiaro come per decifrare questo messaggio basta avere la chiave segreta e fare la decifratura al contrario, con una sottrazione.

Risulta altresì chiaro come il messaggio cifrato presenti una periodicità legata alla lunghezza del verme come evidenziato da Friedrich Kasiski, un ufficiale prussiano in pensione, che nel 1863 pubblicò un trattato crittografico in cui illustrava una tecnica per demolire il cifrario.

Kasiski osservò che ogni volta che parti del messaggio in chiaro sono uguali e vengono cifrate con la stessa porzione della parola chiave, allora anche le corrispondenti parti cifrate risultano uguali.

Dall'analisi delle parti ripetute del cifrato, e in particolare dalla loro distanza, può inferire la lunghezza della parola chiave : la lunghezza della chiave segreta deve essere un divisore comune delle distanze tra le parti identiche del testo cifrato.

Naturalmente il testo esaminato deve essere abbastanza lungo. È altresì chiaro che, una volta nota la lunghezza della chiave, ogni sottosequenza risulta cifrata attraverso un semplice cifrario monoalfabetico.[6]

6 Il massimo comun divisore *n* tra le distanze di lettere ripetute (metodo Kasiski 1863), è con

Fig. 4 - La macchina *Enigma* esposta al Museo Nazionale della Scienza e della Tecnologia "Leonardo da Vinci" - Milano.

Dopo secoli di oblio solo nel secolo ventesimo il disco di Alberti è stato riscoperto e rivalutato e ne sanno qualcosa quelli che decifrarono i messaggi trasmessi da *Enigma*, una macchina elettromeccanica resa celebre dal suo impiego bellico durante la seconda guerra mondiale da parte dei tedeschi.

L'*Enigma* venne ideata nel 1918 dal tedesco Arthur Scherbius sfruttando appunto il principio dei dischi cifranti di Leon Battista Alberti. La macchina venne complicata , fino alla fine della seconda guerra mondiale, aggiungendo via via il numero dei dischi rotanti e altri accorgimenti e si calcola che ne vennero costruiti circa 100.000 esemplari. Aveva le dimensioni di una valigetta e pesava circa 12 kg

elevata probabilità, la lunghezza della chiave. Una volta trovata la *n* si può dividere la frase in *n* parti, ognuna codificata con un codice Cesare distinto e dunque facilmente vulnerabile.

ed era dotata di una tastiera per la redazione del messaggio in chiaro, di differenti rotori per la cifratura, e infine di una tabella luminosa per il risultato. Alla pressione di una lettera in chiaro sulla tastiera, su un pannello luminoso si accendeva la lettera criptata che in quel momento gli corrispondeva.

Enigma aveva al suo interno diversi rotori intercambiabili di 26 celle corrispondenti alle lettere dell'alfabeto tedesco; i rotori erano meccanicamente collegati: ogni 26 scatti del primo rotore determinavano uno scatto del secondo e così via.

I primi modelli avevano in dotazione tre rotori che potevano essere posizionati in sei posizioni diverse all'interno della macchina, (3*2*1); in seguito l'esercito tedesco aumentò a cinque il numero di rotori disponibili portando a 60, (5*4*3), le disposizioni possibili dei rotori.[7]

La macchina *Enigma* non includeva la trasmissione diretta dei messaggi, il cui invio, inizialmente, era affidato ai corrieri. Successivamente, l'utilizzo delle trasmissioni radio ha agevolato l'invio dei messaggi, ma ne ha anche permesso l'intercettazione da parte dei nemici, dato che si utilizzavano apparecchiature facilmente violabili come il telegrafo, il telefono o la telescrivente.

La semplicità d'uso e la presunta indecifrabilità della macchina illusero i tedeschi di poter comunicare in modo sicuro e inviolabile.

Anche la storia dell'*Enigma* risulta piuttosto nota ed è stata ripresa nel film omonimo del 2001 con la regia di Michael Apted, ma il meccanismo di cifratura venne violato perché nel gruppo inglese dei decifratori c'era la mente straordinaria di Alan Turing: certamente perché tutti i messaggi iniziavano e terminavano con frasi similari e si ripetevano i meccanismi di cambiamento della chiave,[8] ma anche

7 Nel calcolo combinatorio, le disposizioni sono tutti i gruppi ordinati di k oggetti scelti fra n oggetti. Si parla di disposizioni di classe k di n oggetti. Il loro numero è il prodotto di k numeri interi consecutivi decrescti a partire da n: $n(n-1)(n-2).....(n-k+1)$. Quando $k=n$ le disposizioni prendono il nome di permutazioni, che quindi sono tutti i possibili gruppi ordinati che si possono formare con n oggetti, essendo ogni gruppo costituito da tutti gli n oggetti.

8 Anche se non strettamente attinente ricordo un'idea, semplice e geniale al tempo stesso, adottata dagli americani nella seconda guerra mondiale, che per le trasmissioni di messaggi riservati utilizzarono un gruppo di nativi che parlavano la lingua dei navaho.

perché qualche esemplare della macchina venne recuperato.[9]

Oggi quotidianamente si scambiano miliardi di messaggi riservati grazie alle tecnologie di trasmissione, alla potenza di calcolo dei computer, alle nuove crittografie a chiave pubblica, e tuttavia l'utilizzo di cifrari simmetrici è tuttora in auge[10] salvo utilizzare, per lo scambio delle chiavi, cifrari asimmetrici più sicuri ma più costosi, visto che vale sempre il Principio di Kerckhoffs,[11] per cui la sicurezza di un crittosistema dipende solo dalla segretezza della chiave.

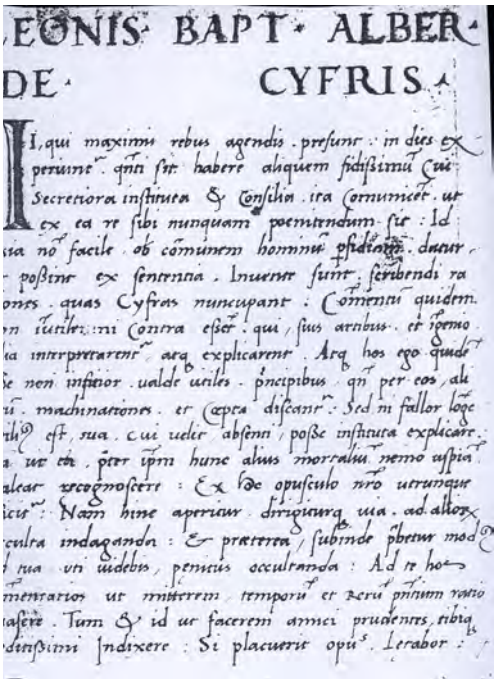

EONIS BAPT. ALBER-
DE CYFRIS

Fig. 5 - Frontespizio del *De cifris* di Leon Battista Alberti.

Al riguardo mi permetto di aggiungere che col principio dei dischi cifranti di Leon Battista Alberti sarebbe ancora oggi possibile costruire un cifrario simmetrico a blocchi.

Si tratta di aumentare i dischi ruotanti, ad esempio tanti quante le lettere dell'alfabeto, e procedere cifrando a blocchi il messaggio in chiaro.

La chiave è formata da una matrice di 26x26 , che rappresenta i dischi rotanti, e dalle regole di spostamento dei "dischi". Lascio al lettore il calcolo del numero delle permutazioni possibili.

9 Il 9 maggio 1941 la corvetta britannica HMS *Aubrietia* metteva le mani per la prima volta su una macchina *Enigma* perfettamente funzionante(operatore umano compreso), sottratta a un U-Boot tedesco.

10 Cito solo l' AES (Advanced Encryption Standard) adottato dalla National Institute of Standards and Technology (NIST) e dalla US FIPS PUB nel novembre del 2001.

11 Dal linguista franco-olandese August Kerckhoff nel suo celebre articolo *La cryptographie militaire* apparso nel «Journal des sciences militaires» nel 1883.

Bibliografia

KAHN David (1967). *The codebreakers*. New York: Scribner

ALBERTI Leon Battista (1994). *Dello scrivere in cifra*, trad. it. di M. Zanni. Prefazione di David Kahn. Torino: Galimberti Tipografi Editori. Edizione originale *De componendis cifris* o semplicemente *De cifris*, 1466.

ALBERTI Leon Battista (1998). *De Componendis Cyfris*, edizione critica a cura di A. Buonafalce. Torino: Galimberti Tipografi Editori.

ArteScienza

Rivista telematica semestrale
http://www.assculturale-arte-scienza.it
Direttore Responsabile: Luca Nicotra
Direttori onorari: Giordano Bruno, Pietro Nastasi
Redazione: Angela Ales Bello, Gian Italo Bischi, Luigi Campanella, Antonio Castellani, Isabella De Paz, Maurizio Lopa
Registrazione n.194/2014 del 23 luglio 2014 Tribunale di Roma - ISSN on-line 2385-1961