Leon Battista Alberti e la nascita dei codici polialfabetici

Franco Eugeni*

DOI:10.30449/AS.v11n21.187

Ricevuto 22-06-2024 Approvato 26-06-2024 Pubblicato 30-07-2024

Sunto: *Leon Battista Alberti, nella sua molteplice attività, fu anche autore di un lavoro, il De Componendis Cyfris, che costituisce il seme dell'intera crittografia moderna della quale, non a torto, è considerato uno dei padri fondatori. Fu lui a comprendere la debolezza dei sistemi monoalfabetici, scoprendo che in ciascuna lingua esiste un naturale frequenza delle cifre quale che sia il modo simbolico di indicarle. Per cui non appena il testo da decrittare sia sufficientemente lungo il critto-analista può individuare gran parte delle cifre e quindi il testo. Una possibile soluzione stava nel cambiare l'alfabeto durante la cifratura. Il suo sistema polialfabetico basato sul disco cifrante e le considerazioni statistiche che lo muovono rappresentano l'inizio di una nuova metodologia e il tentativo di dare una maggiore sicurezza, ai sistemi cifranti, sicurezza che fu raggiunta da questi sistemi e da altri successivi, per quel tempo.*

Parole Chiave: codici monoalfabetici - codici polialfabetici – disco cifrante – frequenza delle cifre.

Abstract: *Leon Battista Alberti, between his various activities, has been also author of a paper, the De Componendis Cyfris, which could be considered the seed of the whole modern cryptography of which he's considered one of the father founders. Alberti understood the weakness of all monoalphabetic systems, and to discover that in each different language there is a natural frequency of digits, whatever is the symbolic way to indicate them. So if the text, to be decrypted, is sufficiently long, the cryptanalyst can identify most of the digits and therefore all the text. One possible solution was to change the alphabet during*

* Già Professore di Filosofia della Scienza. Presidente dell'Accademia di Filosofia delle Scienze Umane (AFSU); eugenif3@gmail.com.

the encryption. His polyalphabetic system, based on the ciphering disk, and his statistical basic ideas represent the beginning of the new methodology and the apex in the safety reached at that time.

Keyword: Keywords: monoalphabetic codes - polyalphabetic codes - cipher disc - frequency of digits

Citazione: Eugeni F., *Leon Battista Alberti e la nascita dei codici polialfabetici*, «ArteScienza», Anno XI, N. 21 giugno 2024, pp. 19-34, DOI: 10.30449/AS.v11 n21.187.

1 - Introduzione

L'opera di Leon Battista Alberti sulla quale graviterà il nostro interesse è il *De Componendis Cyfris.*

Si tratta di un opera di crittografia, insolita per un genio dell'Architettura, che viene oggi considerata la prima nel suo genere. Fu scritta dall'Alberti tra il 1466 e il 1467, su richiesta del segretario papale Leonardo Dato (?1399-1470) che, come si racconta, in una memorabile passeggiata nei Giardini Vaticani, gli illustrò la preoccupazione e l'interesse della Chiesa, per alcune problematiche connesse ai messaggi segreti, che venivano spesso intercettati e decrittati e parimenti per quei messaggi che loro stessi avevano difficoltà a comprendere, diceva Dato: "…alcune volte ci sono portate lettere intercette dalle spie, scritte in cifra e di difficile intendimento,

Fig. 1 - Leon Battista Alberti, *De Componendis Cyfris* (1466-1467)

che non sono da farsene beffe".

Leon Battista Alberti, da genio quale era, studiò ed esaminò il problema in dettaglio e fu a quanto ci risulta il primo a comprendere l'importanza di un'analisi statistica, anche perché ne fu di fatto l'inventore. Scoprì l'Alberti che i codici allora in uso, essenzialmente monoalfabetici, erano molto deboli per il fatto che in ciascuna lingua in uso, allora che il messaggio sia sufficientemente ampio, si presenta una vulnerabilità per il fatto che ogni cifra, in una fissata lingua, ha una sua propria frequenza. In altre parole se prendo una pagina, dieci pagine , cento pagine, ad esempio in francese, la lettera a compare un ugual numero di volte indipendentemente dal numero delle pagine esaminate. Si tratta in altre parole della scoperta del fenomeno statistico, che non ci risulta fosse stato osservato prima d'allora da altri.

Fig. 2 - Leon Battista Alberti (1404-1472)

Ma l'Alberti non si limita a questo fenomeno di decrittazione, ovvero alla comprensione del messaggio cifrato, senza conoscerne il segreto e solo usando la statistica delle frequenze delle lettere di una lingua. Parallelamente l'Alberti offre un nuovo sistema di cifratura che consiste nel passare dall'allora classico sistema monoalfabetico ad un sistema polialfabetico, così da eliminare la possibilità di un attacco statistico da parte dei crittoanalisti. Ideò anche un secondo sistema, nel quale rappresentava la stessa cifra in più modi, come vedremo, per nasconderne la frequenza, sistemi questi da chiamarsi omofonici. Scrive David Kahn[1] al riguardo:

1 cfr., L.B. Alberti, Dello scrivere in cifra [De componendis cyfris], a cura di A. Buonafalce, prefazione di D. Kahn, traduzione di M.F. Zanni, Galimberti Tipografi Editori, Torino 1994

> Questo volume elegante e sottile riproduce il testo più importante di tutta la storia della crittologia; un primato che il De cifris di Leon Battista Alberti ben si merita per i tre temi cruciali che tratta: l'invenzione della sostituzione polialfabetica, l'uso della crittanalisi, la descrizione di un codice sopracifrato.

L'opera fu segreto di stato per decenni, anche per volontà dello stesso Alberti che scrisse:

> Io vorrei che questa mia operetta si conservasse appresso degli amici miei, cioè non andasse in mano del popolo, né si pubblicasse questa mia invenzione che è veramente degna d'un Re, che abbia capacità a maneggiare cose grandi.

In realtà l'opera venne pubblicata postuma soltanto nel 1568 a Venezia, da tale Cosimo Bartoli (1503-1572). Il Bartoli fu un insigne studioso di filologia, che ebbe notorietà per la sua opera di traduzione e divulgazione dei trattati dell'Alberti quali il *De Statua* e il *De Architectura*, ma interessandosi anche di crittografia, pubblicò anche il *De Componendis Cyfris*, che tuttavia rimase poco conosciuta fino ai primi del Novecento

Fig. 3 - Il generale Luigi Sacco (1883-1970).

Fu proprio ai primi del Novecento che per merito del Generale Luigi Sacco (1883-1970), lo studioso italiano che fu il personaggio di maggior spicco in campo crittografico del tempo, che all'Alberti fu riconosciuta la primogenitura dei cosiddetti metodi "polialfabetici" e "omofonici". Il generale Sacco fu anche un giovane collaboratore di Guglielmo Marconi (1847-1937), per la radiotelegrafia, e oltre a mettere in piedi sistemi di controspionaggio molto efficienti dal punto di vista operativo, non disdegnò gli studi teorici avendo prodotto circa una settantina di

pubblicazioni specialistiche, di alto e significativo valore.

Concludiamo questo primo paragrafo con un cenno sul personaggio Leon Battista Alberti. L'Alberti nacque a Genova nel 1404 e morì a Roma nel 1472. Figlio illegittimo di una ricca famiglia di commercianti fiorentini, famiglia che fu bandita da Firenze nel 1382 per motivi politici. Leon Battista compì gli studi a Venezia, Padova e Bologna dove si specializzò in lettere, diritto canonico, greco, musica, pittura, scultura, architettura, fisica e matematica. Nel 1421 prese gli ordini religiosi e nel 1432 fu nominato abbreviatore apostolico sotto Papa Eugenio IV (1383-1447) appena eletto.

Gli abbreviatori furono un corpo di funzionari della cancelleria pontificia il cui incarico consisteva nel redigere le bozze e poi preparare in forma compiuta le bolle papali, le note pontificie e i decreti concistoriali, prima che questi venissero scritti in extenso dagli scriptores, importanti anche per inviare le disposizioni che il Papa inviava ai vescovi.

Questo incarico l'Alberti mantenne per ben 34 anni, durante i quali visse tra Roma, Ferrara, Bologna e Firenze. Fu agli ordini di ben cinque Pontefici dal 207° al 211°, precisamente sotto Eugenio IV, Nicolò V (1397-1455), Callisto III (1378-1458), Pio II (1405-1464), e

Paolo II (1417-1471) che nel 1466 soppresse il collegio degli abbreviatori, anni durante i quali visse tra Roma, Ferrara, Bologna e Firenze.

Alberti fu a Mantova nel 1459 con Papa Pio II Piccolomini, città dove soggiornò in occasione del celebre Concilio di Mantova o dieta convocato dal Papa Piccolomini, eletto l›anno prima. Lo scopo della dieta era finalizzato a promuovere una Crociata contro gli Ottomani che avevano preso Costantinopoli nel 1453. La dieta fu sciolta nel 1460, la Crociata venne bandita ufficialmente dal Papa il 14 gennaio. Vi furono difficoltà organizzative e la Crociata rimase sulla carta, del resto lo stesso Pio II morì tre anni dopo ad Ancona, sempre cercando, ma inutilmente, di spingere i principi cristiani a prendere le armi per liberare Costantinopoli.

Gli successe Papa Paolo II, al secolo il veneziano Pietro Barbo, che non fu amato dai cardinali e morì per "indigestione" a soli 54 anni. Alberti non fu certo con le mani in mano. Dapprima tra il 1450 e eil 1460 iniziò la costruzione delle chiese di Sant'Andrea e San Sebastiano entrambe a Mantova e completate da altri dopo la sua morte.

Fu uno dei più colti umanisti, scrisse vari trattati e fu autore di poesie e morali, scrisse di geometria, topografia e meccanica, pittura, giochi matematici, architettura, e i primi tre grandi trattati dell'Età Moderna, tra il 1447 al 1463: il *De pictura* , il *De re Aedificatoria* e il *De statua*.

Il *De Componendis Cyfris* rimase conosciuto solo in ambienti vicini alla corte papale per ragioni "di sicurezza" e non si hanno notizie della sua diffusione verso l'esterno. Non sappiamo dunque se, coloro che intrapresero studi analoghi, avessero conoscenza o meno del geniale lavoro dell'Alberti.

2 - L'analisi statistica della lingua e gli alfabeti omofonici

Le considerazioni dell'Alberti, che oggi potrebbero apparire ovvie agli addetti ai lavori, furono cruciali per comprendere la debolezza dei sistemi di cifra fino ad allora utilizzati. I propositori dei codici monoalfabetici, ovvero di coloro che all'alfabeto in uso, detto "in chiaro" associarono inizialmente un secondo alfabeto diversa-

mente ordinato. Così all'alfabeto " in chiaro":

ABCDEFGHILMNOPQRSTUVZ

possiamo associare il codice di Cesare, ottenendo spostando le cifre di alcuni posti (ad. es. tre come in quello usato da Cesare):

ABCDEFGHILMNOPQRSTUVZ
DEFGHILMNOPQRSTUVZABC

con il che la frase ALEIAACTAEST diviene DOHNDDFZDHVZ .

Possono essere usati altri sistemi come l'Atbash (alfabeto rovesciato), l'utilizzo di una qualsiasi delle 21! permutazioni dell'alfabeto in chiaro.

ZVUTSRQPONMLIHGFEDCBA (atbash , alfabeto rovesciato)

ERACFLQTVGNPOMIHMSTZB (una delle 21! permutazioni).

Ancora vi fu l'illusione di crittografi monoalfabetici di sostituire all'alfabeto in chiaro un alfabeto simbolico come in figura 5, per i quali si costruirono macchine cifranti a dischi ruotanti.

Significativi furono gli alfabeti simbolici costruiti, ad esempio, dal napoletano Giovan Battista Della Porta (1535-1615), uno dei quali è in figura 4 . Di detti alfabeti si costruivano dischi cifranti intercambiabili chesimettevano nelle machine cifranti (fig.5).

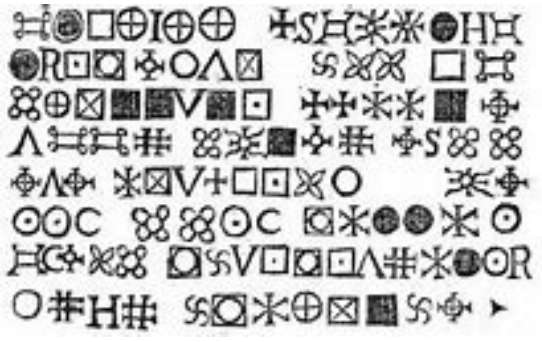

Fig. 4 - Alfabeto simbolico di Giovan Battista Della Porta (1535 – 1615).

Della Porta passò la vita in attività scientifiche. Per la sua enorme erudizione dominò il mondo scientifico italiano prima

Fig. 5 - Cifrario di Giovan Battista Della Porta.

di Galileo.

Ma la questione era debole poiché in un rapporto 1 ad 1 tra un alfabeto in chiaro e un secondo alfabeto cifrante, anche fatto di strani ideogrammi inventati, si conservano le frequenze, ed è questo il punto debole. D'altra parte ogni lingua si differenzia dalle altre per caratteristiche statistiche, quali la frequenza delle singole lettere, dei bigrammi e dei digrammi e tali caratteristiche costituiscono una vera e propria impronta digitale della lingua.

È proprio di questo che si accorge l'Alberti con una serie di osservazioni "sperimentali" su più lingue, ad esempio latino, italiano, francese, tedesco, inglese o altro.

Osserva l'Alberti che l'italiano è una lingua molto vocalizzata, l'inglese, al contrario, presenta un'alta frequenza di consonanti. Il francese è anch'esso molto vocalizzato anche se é ricco di lettere come la J, che in italiano sono poco frequenti. La lettera E è la più frequente in quasi tutte le lingue europee, in particolare in francese e in tedesco hanno una prevalenza nettissima. Così la "O" sembra la meno frequente, mentre la "E" e la "I" sembrano le più frequenti. Ma Alberti osserva che la vocale meno utilizzata, in realtà, non è la "O", bensì la "U", che usualmente si identificava con la "V". L'Alberti completa poi l'indagine statistica delle lingua considerando i bigrammi ed i trigrammi e scopre in ciascun caso quali siano i più ricorrenti nelle varie lingue d'uso con una analisi in realtà piuttosto

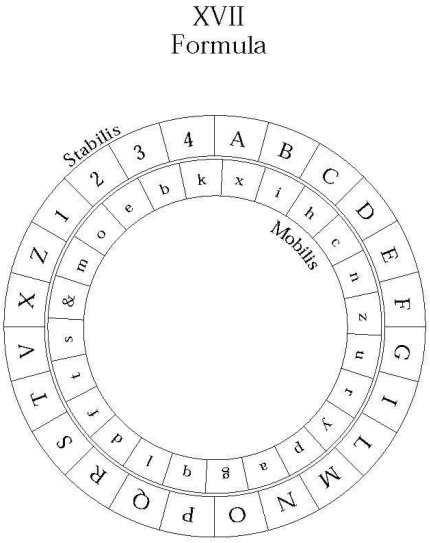

Fig. 6 - Il disco cifrante di Leon Battista Alberti a pag. 29 di *De Componendis Cifris.*

raffinata per le applicazioni.

Occorre trovare rimedi adeguati, invenzioni nuove, tecniche più potenti. Per il sistema omofonico occorre disporre di un numero di caratteri maggiore di quelli di cui si ha bisogno nella lingua normale, in modo da attribuire ad una stessa lettera una serie di caratteri diversi ed utilizzarli in modo alternato, perlomeno per quelle lettere usate con maggiore frequenza. Ad esempio nella lingua italiana si hanno i seguenti esempi di traduzione omofonica:

E (11,79) cioè 12 si traduce in E1, E2, …, E12
A (11,74) cioè 12 si traduce in A1, A2, …, A12
I (11,28) cioè 11 si traduce in I1, I2, …, I11
N (6,88) cioè 7 si traduce in N1, …, N7
U-V (0,51+2,10) cioè 2 si traduce in U1, U2 o con U, V alternate.

L'Alberti dice solo che occorre inventare un alfabeto più ampio, per tradurre, evidentemente, i simboli da noi indicati con Ei , Ai etc.

A tutto questo si può aggiungere un nomenclatore, cioè associare ad alcuni caratteri, o a sequenze predefinite, il significato di intere sillabe o parole: "come per esempio accordarsi che la A significhi il Papa; il B l'esercito; il D l'armata di mare; e per la medesima regola

che la R esprima che i nemici si fossero mossi di alloggiamento; la S che l'esercito avesse carestia di vettovaglie e simili altre cose…". L'esempio dell'Alberti, riportato in tabella a fine opera, è di un nomenclatore imperniato sulle sequenze di numeri. Ritiene l'Alberti che un sistema crittografico debba essere facile da leggere e inaccessibile ad estranei se si ignorano gli accordi convenuti fra le parti che si scambiano il messaggio. Nel prossimo paragrafo parleremo del sistema polialfabetico dell'Alberti.

3 - Il Disco Cifrante: costruzione e funzionamento

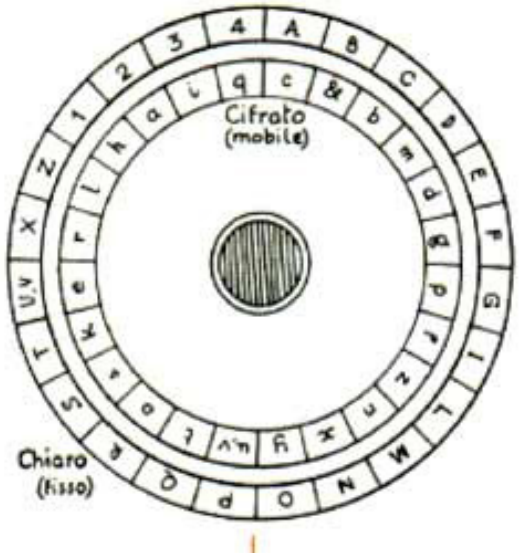

Fig. 7 - Per la costruzione del disco cifrante di Leon Battista Alberti.

Il nuovo metodo di cifratura ha bisogno di un dispositivo meccanico, il disco cifrante che l'Alberti chiama "Mondine". Di questo dispositivo devono esistere, ovviamente, almeno due copie, delle quali una a disposizione del mittente e l'altra a disposizione di ciascun destinario, in modo che ci possano essere più destinari.

Si costruiscono due lamine a forma di cerchio, tra loro concentriche ma con diametro diverso, disposte come in figura 7. Si divide ciascuna circonferenza in 24 parti eguali[2] o case. Sulle case dei due cerchi si riportano le lettere dell'alfabeto nel modo seguente. Nel cerchio esterno, quello piu grande (detto cerchio del chiaro o solo

2 Operazione agevole con riga e compasso, che l'Alberti aveva descritto nel *De Re Aedificatoria.*

chiaro), si riporta un alfabeto in lettere maiuscole, mancante delle lettere H, K, W, Y (dette lettere inutili) e con le lettere U, V accorpate in una unica lettera, sono in tutto 20 lettere, a queste si aggiungono i numeri 1,2,3,4 che come vedremo servono ad un uso speciale durante la cifratura. Dunque il chiaro è composto dalle 24 lettere seguenti:

1,2,3,4,A,B,C,D,E,F,G,I,L,M,N,O,P,Q,R,S,T, (UV), X,Z

Nel disco interno, di raggio minore (detto cerchio del cifrato, o solo cifrato) compaiono le lettere in carattere minuscolo dell'intero alfabeto, meno la u identificata con la v, e la w, mentre si aggiunge il simbolo &, al posto della w, per avere esattamente 24 cifre; dunque si hanno precisamente le lettere:

a,b,c,d,e,f,g,h,k,i,l,m,n,o,p,q,r,s,t,v,x,y,z,&

In realtà, l'Alberti al posto del cifrato, scritto come sopra, sostituisce una permutazione dello stesso, precisamente andando in senso orario scrive la seguente (quella di figura 7):

(α) a,c,e,g,k,l,n,p,r,t,v,z,&,x,y,s,o,m,q,i,h,f,d,b

L'intento di Alberti è comprensibile, lui vuole disporre di molti dischi interni, ovvero di molte permutazioni del cifrato, in maniera che con accordi tra mittente e destinatario, il disco interno può essere modificato a piacere, introducendo così una ulteriore difficoltà per un eventuale tentativo esterno di decrittazione, oggi diremmo per un hackeraggio. Del resto il numero delle permutazioni possibili è enorme, avendosi:

24! = 24x23x22x...x3x2 > 10…..0 (25 zeri)

Per esemplificare, useremo solo la permutazione (α).

Vogliamo adesso permettere ai nostri lettori di costruirsi una macchina di Alberti, per imparare ad usarla, con il semplice uso di due fogli formato A4.

Allo scopo il lettore stampi, in formato A4 la figura 7, riproducente i due dischi del cifrato (esterno) e del chiaro (interno). La fotocopia ottenuta si sovrapponga ad un foglio "formato A4", quindi di egual misura, e si blocchi l'uno contro l'altro con una cucitrice. Fatto questo si individui il centro comune ai due cerchi e si inserisca una puntina da disegno nel centro dei due cerchi (che sono concentrici) così da prendere entrambi i fogli. A questo punto si tagli il contorno del cerchio minore, e lo si fissi con la puntina al disco piccolo, così da poterlo far ruotare attorno al centro, si blocchi la puntina con un pezzetto di cartone. Abbiamo costruito la macchina dell'Alberti!

Siamo ora pronti a cifrare da parte del mittente (M) e a decifrare da parte del destinatario (D). Naturalmente dovranno (M) e (D) accordarsi su due punti:

a.-Dovranno condividere il medesimo cerchio piccolo, ovvero la medesima permutazione, useremo come detto la permutazione (α), scelta tra un mare di possibilità da 24 zeri.

b.- La seconda condivisione che che occorre , per (M) ed (D) inizializzare la macchina scegliendo un coppia (maiuscolo / minuscolo) tra le possibili 20x24 = 480 coppie. Scegliamo come inizializzazione lacoppia (A,g).

Siamo pronti, almeno in parte, a cifrare il seguente messaggio:

L'INGEGNERE LUCA NICOTRA HA ORGANIZZATO UN INCONTRO

Togliamo, come è usuale, apostrofo e spazi vuoti, e semplifichiamo per avere:

INGNICOTRAHAORGANIZINCONTRO

Ciò fatto inseriamo a caso, ovvero a piacere, i numeri da 1 a 4 nel mezzo del testo, come nell'esempio:

ING4NICO1TRA2HAORG1ANIZI3NCO2NTRO

Si noti che i numeri sono inseriti in modo che tra due numeri

consecutivi non vi siano due lettere eguali.

Prendiamo ora la macchina inizializzata in (A,g) con la permutazione (α). Sotto I, trovo v, sotto N trovo x, sotto G trovo t, sotto 4 trovo e ho la prima parte di cifratura: vxte, ma avendo trovato un numero, opero un cambio di alfabeto, ruotando il disco interno in maniera da portare g sotto 4, continuo a cifrare. Sotto N trovo y,sotto I trovo z, sotto C trovo n, sotto O trovo s, sotto 1 trovo a, ho trovato un numero e cambio alfabeto, portando g sotto 1. Ottengo finora: vxteyznsa.

Continuando sotto T trovo b, sotto R trovo f , sotto A trovo p , poi ho 2 e cambio alfabeto, e così via… ottenendo: vxteyznsabfp…..

È chiaro come si cifra!

Passiamo ora dalla parte del destinatario (D) che riceve il messaggio: vxteyznsabfp…..

L'utente (D) prende la macchina, predisposta con la permutazione (α), che lui sa essere quella giusta, la inizializza con la coppia (A,g). Ha sistemato le chiavi del sistema in modo corretto. Va a leggere nel disco interno: vxteyznsabfp…..

Sopra v trova I, sopra x trova N, sopra t trova G, sopra e trova 4, allora porta g su 4 e continua, sopra y trova N, sopra z trova I, sopra n trova C, sopra s trova O, sopra a trova 1, allora porta g su 1 e continua, sopra b trova T, sopra f trova R, sopra p trova A, … ha ottenuto:

ING4NICO1TRA…. ovvero INGNICOTRA…. ovvero

ING NICOTRA ….

Si può per esercizio cifrare l'inero messaggio iniziale e poi decifrarlo.

4 - Conclusioni

Leon Battista Alberti è considerato il precursore dei moderni temi di crittologia; ignoriamo l'influenza che egli può aver avuto su coloro che si occuparono di tali studi al suo tempo. Furono infatti molti gli studiosi che dopo l'Alberti si occuparono di metodi di cifratura polialfabetica. Tra il 1467 ed il 1590 si possono indicare le seguenti tappe:

1947 Roma - L.B. Alberti manoscritto *De Componendis Cyfris*
1518 Mainz - Tritemio 1° metodo con l0 Ziruph (Tavola recta)
1553 Brescia - G.B.Bellasio probabile primo uso "parola chiave"
1557 Lione - Cardano ideazione di varie tecniche
1563 Napoli - G.B.Porta Trattato *De Furtivis Literarum Notis*
1586 Parigi - B. Vigenere Tecnuca dello Ziruph (*Tavola recta*)

Tali tappe condussero alla "messa a punto" del metodo, per anni riconosciuto come il più difficile ed il più impenetrabile codice, attribuito erroneamente a Vigénère (in realtà era il metodo inventato da Belaso) che lo aveva diffuso.

Parleremo in dettaglio del cosiddetto metodo di Vigénère,in altro articolo. Fu considerato intrattabile per circa 300 anni ed ebbe più fortuna del metodo di Alberti, che tuttavia fu usato come sistema sopra-cifrante durante la II guerra.

La tecnica usata nel disco cifrante dell'Alberti è in realtà la stessa dei vari metodi polialfabetici di Tritemio, Belaso, Cardano e Vigénère che utilizzano la tabula recta. Questo perché ad ogni rotazione del disco interno corrisponde una nuova serie di corrispondenze, ovvero un nuovo alfabeto.

Un attacco ad un messaggio cifrato con un codice di Alberti a disco interno variabile può essere solo di tipo sperimentale anzi esaustivo. L'attaccante allora ha davanti un tale numero di possibilità tra cui scegliere che la sua probabilità di successo è dell'ordine di 1/24!, cioè è l'insuccesso, allora che il codice sia usato nella sua completa potenzialità.

A tutto questo va aggiunto che Alberti suggerisce l'uso dei nomenclatori, cioè sequenze, in questo caso numeriche, che hanno significati prestabiliti e che rendono ancora più arduo ogni tentativo di decrittazione. Che il metodo di L.B. Alberti sia più sicuro è in sintesi testimoniato proprio dal numero di convenzioni segrete, che in termini di dischi variabili sono quantificabili (ad esempio la probabilità di rottura), mentre in termini di nomenclatore non sono quantificabili pur essendo chiaro e intuibile che l'uso di questi, in tempi brevi irrobustisce il codice, ma in tempi lunghi una parola del nomenclatore può essere sottoposta ad analisi statistica, allora che il crittoanalista abbia le giuste informazioni.

Probabilmente anche perché inizialmente non conosciuto, il metodo di cifratura di L.B. Alberti non ha ricevutoa un riconoscimento pari alla sua grandezza. Infatti il più famoso è il metodo di Vigénère, che però dal confronto con il metodo di Alberti non risulta affatto il miglior metodo polialfabetico, nonostante sia stato largamente adottato fino agli inizi del secolo scorso.

Bibliografia

Bartoli Cosimo (1568). *Opuscoli Morali di L.B. Alberti*… tradotti et in parte corretti, Venezia: Franceschi, pp. 198-219.

Berardi Luigia e Beutelspacher Albrecht (1991). *Crittografia.* Milano: FrancoAngeli.

Beutelspacher Albrecht (1994). *Cryptology.* Washington: The Mathematical Association of America Ed.

Buonafalce Augusto (cur.), (1994). *De Componendis Cyfris*, prefazione di D. Kahn, traduzione di Zanni M.F. Torino: Galimberti Tipografi Editori.

Eugeni Franco (1992). "Combinatorics and Cryptography". In «*Annals of Discrete Math.*», pp. 159-174.

Eugeni Franco e EUGENI Diana (1998). "Matematica e Scienza Applicata tra Oriente e Occidente e i prodromi della moderna Teoria dell'Informazione. In *Le identità e i saperi*, Teramo: Edilgraphital, pp. 31-60. Reperibile in www.afsu.it/discipline/le rivoluzioni …, anche in www.afsu.it/periodici/Periodico di matematica, anno 34°- vol.I, n.1-2 , Antologia.

Eugeni Franco e Mascella Raffaele (2001). "Leon Battista Alberti, Crittografia e Crittoanalisi". In *Atti del Convegno nazionale della Mathesis, sugli Scienziati mantovani*, Mantova. Anche in : www.afsu.it/discipline/informatica/articoli di .../

Della Porta Giovan Battista (1563). *De Furtivis Literarum Notis (De Ziferis)*, Neapoli, apud Ioanni Maria Scotum, MDLXIII.

Galimberti Niccolò (2010). Il De componendis cyfris di Leon Battista

Alberti tra crittologia e tipografia, in *Atti dei Convegni, Abbazia di Santa Scolastica 2006- 2007*, Subiaco, Iter edizioni.

KAHN David (1980). "On the Origin of Polyalphabetic Substitution", in «I*sis*», LXXI pp. 122–127 (rist. in Kahn on Codes, Macmillan, New York 1983).

MANCA Paolo Severino (2018). "I dischi cifranti di Leon Battista Alberti". In: «*ArteScienza*», Anno IX, N. 18, pp. 31-42 DOI:10.30449/AS.v9n18.164.10.-

SACCO Luigi (1947a). *Un primato italiano. La crittografia nei secoli XV e XVI*, vedi Bollettino dell' ISBAS (1958), Roma. (Ristampa di un lavoro del 1947, a cura dell'Istituto Storico e di cultura dell'arma del Genio).

SACCO Luigi (1947b). *Manuale di Crittografia*, 3° Edizione, Istituto Poligrafico dello Stato (1987, L'Aquila. (Ristampa dal 1947, a cura della Scuola Superiore G. Reiss Romoli).

SGARRO Andrea (1989). *Codici Segreti*. Milano: Mondadori .

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,
Isabella De Paz, Franco Eugeni, Maurizio Lopa, Paolo Severino Manca, Ezio Sciarra
Registrazione n.194/2014 del 23 luglio 2014 Tribunale di Roma - ISSN on-line 2385-1961