Atti del Convegno nazionale Scienziati mantovani – Mantova 2001

LEON BATTISTA ALBERTI, CRITTOGRAFIA E CRITTOANALISI

Franco Eugeni e Raffaele Mascella[*]

SUNTO – L.B. 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. In questo volume dedicato a Scienziati Mantovani, considerando che lui a Mantova operò, non può non essere presente un saggio sul suo lavoro crittografico. Il suo sistema polialfabetico basato sul disco cifrante e le considerazioni statistiche che lo muovono rappresentano l'inizio della nuova metodologia e l'apice nella sicurezza, raggiunta da questi sistemi e da altri successivi, a quel tempo.

ABSTRACT – L.B. 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. In this volume dedicated to Scientists from Mantova, considering that he worked in Mantova, it could not be missing an essay to present his cryptographic paper. 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 by these systems.

[*] Dipartimento di Metodi per l'Economia ed il Territorio, Università degli Studi di Teramo, Colle S. Agostino, 64100 Teramo.

1. Introduzione

Leon Battista Alberti nacque a Genova nel 1404 e morì a Roma nel 1472. Figlio illegittimo di una ricca famiglia di commercianti fiorentini bandita da Firenze dal 1382 per motivi politici, compì gli studi a Venezia, Padova e Bologna dove si specializzò in lettere, diritto canonico, greco, musica, pittura, scultura, architettura, fisica e matematica.

Fig. 1 – *Frontespizio degli "Opuscoli Morali di Leon Battista Alberti", opera postuma del 1568 a cura di C. Bartoli.*

Nel 1421 prese gli ordini religiosi e nel 1432 fu nominato abbreviatore apostolico (controfirmava i "brevi" apostolici, cioè le disposizioni che il Papa inviava ai vescovi), incarico che egli mantenne per ben 34 anni fino alla soppressione del collegio degli abbreviatori, durante i quali visse tra Roma, Ferrara, Bologna e Firenze. Fu a Mantova nel 1459 con Papa Pio II, dove soggiornò in occasione della celebre dieta per la crociata, nel 1463 e poi nel 1470 e 1471, ideando le chiese di San Sebastiano e Sant'Andrea. Scrisse diverse opere su temi quali famiglia, pittura, giochi matematici, architettura, ecc.

L'opera su cui appunteremo il nostro interesse è il *De Componendis Cyfris*,opera di crittografia che viene oggi considerata la prima nel suo genere, composta dall'Alberti fra il 1466 e il 1467 su suggerimento dell'amico, nonché segretario papale, Leonardo Dato che in una memorabile passeggiata nei Giardini Vaticani gli illustrò l'interesse della Chiesa per la conoscenza dei metodi crittologici: "*…alcune volte ci sono portate lettere intercette dalle spie, scritte in cifra, che non sono da farsene beffe*".

L'opera fu tenuta segreta per decenni, anche per volontà dello stesso Alberti che nella conclusione scrisse: "*Io vorrei che questa mia operetta si conservasse appresso degli amici miei, cioè non andasse in potere del popolo, né si pubblicasse questa invenzione degna veramente di un Re, atto*


COSIMO BARTOLI
AL MOLTO MAGNIFICO SIGNOR
BARTOLOMEO CONCINI.

Fig. 2 – *Introduzione di Cosimo Bartoli all'opera postuma dell'Alberti "La Cifra" con dedica al Signor Bartolomeo Concini.*

200

LA CIFRA DI LEONBATTISTA ALBERTI.

COLORO che hanno la cura di maneggiare le cose grandi & d'importanza, fanno per persona di quanto gran momento sia, havere alcuno che sia fidelissimo, con il quale essi possino conferire i loro consigli, & le loro deliberationi, in maniera tale, che essi per tempo alcuno non si habbino di ciò a pentire. Et perche mediante la commune malignità degli huomini non è loro così facilmente concesso il poter far questo, si sono trovate alcune inventioni, o maniere di scrivere, che si chiamano Cifre; inventioni certamente non difficili, se dall'altra parte non si trovassino alcuni, che con le loro arti, & con il loro ingegno, le ritrovano & le interpretano. Ne dico io, che questi tali non sieno molto utili a Principi: Conside-

Fig. 3 – *L'inizio dell'opera "La Cifra".*

o inclinato a maneggiare cose grandi". Fu pubblicata postuma nel 1568 a Venezia da Cosimo Bartoli ma rimase poco conosciuta fino ai primi del Novecento e fu solo per merito del Generale Luigi Sacco, lo studioso italiano di maggior spicco in campo crittografico nella prima metà del secolo, che ad Alberti fu riconosciuta la primogenitura dei cosiddetti metodi "polialfabetici" e "omofonici".

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, inoltre l'Alberti fu decisamente il primo a comprendere l'importanza di un'analisi statistica, anche perché ne fu sostanzialmente l'inventore. Tuttavia il *De Componendis Cyfris* rimase conosciuto solo in ambienti molto vicini alla corte papale per ragioni, diciamo oggi, "di sicurezza", in auge anche allora, e vivamente consigliate dallo stesso Alberti, come ricordato nell'introduzione. Non si hanno notizie circa la sua diffusione, anche parziale, verso l'esterno. E' dunque difficile comprendere se, coloro che di lì a breve intrapresero gli stessi studi, primo fra tutti Tritemio, avessero seguito le idee dell'Alberti.

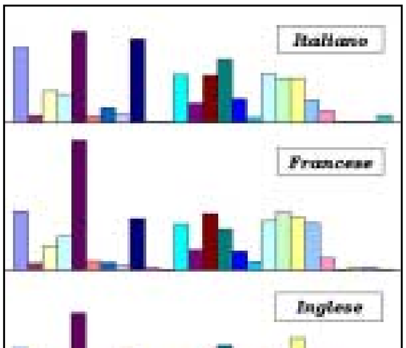

Fig. 4 – *Frequenze delle lettere in alcune lingue.*

L'Alberti inizia la sua opera con una serie di osservazioni "sperimentali" su una lingua, ad esempio latino, italiano o altro. Una lingua è composta da parole, sillabe e caratteri. Possiede diverse peculiarità, ad esempio legate alla necessità della presenza delle vocali per formare le sillabe. Le vocali dunque sono molte usate: ad esempio osserva che fra i poeti il loro uso è dei 7/8 delle consonanti, fra gli oratori raggiungono i 2/3 delle consonanti. Inoltre esse si usano con frequenze diverse, così la "O"

sembra la meno frequente, mentre la "E" e la "I" sembrano le più frequenti. Ma Alberti precisa che la vocale meno utilizzata, in realtà, non è la "O", bensì la "U", per la quale, come ricordiamo, si usava la stessa cifra della consonante "V". Pertanto la frequenza della "V" rappresentativa della vocale "U" risulta alterata per il significato, a volte, anche di consonante. Egli stesso si fa peraltro promotore dello sdoppiamento linguistico delle due lettere.

L'analisi statistica della lingua prosegue poi anche con le consonanti. In questo ambito Alberti esprime il suo rammarico per il sempre minor uso della lettera K, "*…della qual lettera avremo forte bisogno di scrivere in molte cose…*".

L'Alberti completa poi l'indagine statistica della lingua considerando i bigrammi ed i trigrammi e determina in ciascun caso quali siano quelli più ricorrenti.

Notiamo che la sua "analisi statistica" non è affatto grossolana o di prima intuizione. L'analisi effettuata fino ai trigrammi è piuttosto raffinata per le applicazioni.

Da questa analisi generale emergono alcune considerazioni fondamentali ai fini della cifratura dei messaggi: i caratteri che ricorrono con maggiore frequenza e che si trovano abbastanza vicini saranno vocali; le stesse consonanti, per via degli indizi raccolti, saranno di facile individuazione.

Occorre trovare rimedi adeguati, invenzioni nuove, tecniche più potenti. E in queste invenzioni bisogna avere a disposizione 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. Elementi quali la frequenza con cui si ripetono le lettere, la loro posizione all'interno delle parole, le accoppiate che sono possibili e quelle che sono impossibili, semplificano e di molto il lavoro del crittoanalista.

Lettera	Frequenza	Simboli
A	9	$A_1, A_2, A_3, \ldots, A_9$
B	1	B_1
C	5	$C_1, C_2, \ldots, C_5$
D	4	$D_1, \ldots, D_4$
…	…	…
…	…	…
Y	1	Y_1
Z	2	Z_1, Z_2

Fig. 5 – *Un esempio teorico di codice omofonico.*

Le considerazioni fin qui esaminate sono quelle che conducono alla scoperta più importante dell'Alberti in ambito crittografico, cioé gli alfabeti omofonici, di cui, tuttavia, non si trova traccia nei suoi lavori. L'Alberti dice solo che occorrerebbe fare ricorso ad un alfabeto più ampio, per tradurre, evidentemente, i simboli da noi indicati con A_2, B_1, etc. (Fig. 5).

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 che la A significassi il Papa; il B lo esercito; il D la armata di mare; e per la medesima regola che la R esprimessi che i nemici si fussero mossi di alloggiamento; la S che lo esercito avessi 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.
Prima di passare alla descrizione della sua tecnica l'Alberti chiarisce la natura del suo ragionamento prettamente scientifico, trascurando quei metodi suggestivi, allora molto in voga, quali lo scrivere con il latte o con il liquore insalato o cose del genere, poiché egli le ritiene "*sciocche*". La sua preferenza va tutta al suo nuovo metodo, che "*… io giudico, e a ragione, che questa si fatta cifra sia cosa da Re, della quale senza aver ad aspettare un segretario che la decifri, esso Re possa con pochissima fatica comodissimamente servirsene…*". Dunque molto rapido, facile da leggere e inaccessibile ad estranei se si ignorano gli accordi convenuti fra le parti che si scambiano il messaggio.
In questo l'Alberti sembra precorrere i tempi poiché da questi ultimi discorsi si comprende come egli non teneva in conto il metodo (matematico, chimico o altro) ma fosse portato a fare affidamento su un'idea che riponesse la sua forza in un segreto variabile. Non arriva a definire una chiave, ma l'idea di un segreto variabile è molto significativa nei suoi codici.

3. Il Disco Cifrante: costruzione e funzionamento

Il nuovo metodo di cifratura ha bisogno di un dispositivo meccanico, il disco cifrante, che l'Alberti chiama "Modine". Di questo modello devono esistere due copie, il primo a disposizione del mittente, il secondo presso il destinatario.
Si costruiscono due lamine a forma di cerchio con diametro diverso e si divide la circonferenza di ciascuna in 24 parti uguali o *Case* (operazione agevole con riga e compasso che Alberti aveva descritto nel De Re Aedificatoria)[1].
Sulle case dei due cerchi si riportano i caratteri dell'alfabeto, inserendo solo nel più grande i numeri da 1 a 4 e togliendo le lettere "inutili" come H e K, quindi i due dischi si sovrappongono e si fissano in modo che possano ruotare intorno al loro centro. A questo punto siamo pronti per cifrare ogni messaggio.
Le due parti scelgono una chiave cifrante, chiave che serve esclusivamente per iniziare la cifratura "*… come quasi per una chiave per aprirci l'entrata…*", e che deve essere composta di una coppia di caratteri che determinano la corripondenza iniziale fra i caratteri del disco più grande e caratteri del disco più piccolo. Così, scegliendo la chiave (A,r), i dischi devono avere inizialmente la disposizione illustrata in Fig. 6.

[1] Ricordiamo che è possibile dividere, con riga e compasso, una circonferenza in n parti uguali se e solo se l'intero n decomposto in fattori primi è del tipo $n = 2^h \cdot p_1 \cdot p_2 \cdot p_3 \cdot \ldots$ dove i numeri p_i sono dei numeri primi di Fermat, cioè della forma $\left(2^{2^h}+1\right)$. Si conoscono solo i primi corrispondenti ad $h = 0,1,2,3,4$ e non si sa se esistono o meno altri primi di Fermat. Nel nostro caso $n = 24 = 2^3 \cdot 3$ e 3 è il primo di Fermat corrispondente ad $h = 0$.

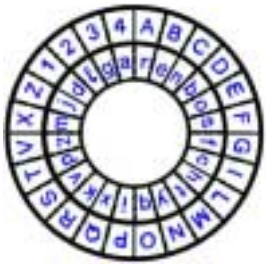

Fig. 6 – *Disposizione di chiave (A, r).*

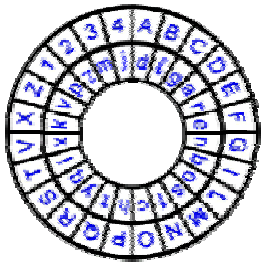

Fig. 7 – *Disposizione di chiave (A, d).*

Supponiamo che le due parti vogliano scambiarsi il seguente messaggio:

IL PROFESSOR MERCANTI HA ORGANIZZATO BENE QUESTO CONVEGNO

Allora il mittente effettua le seguenti operazioni:
1) elimina gli spazi ed inserisce, a caso, numeri da 1 a 4 nel mezzo del testo, ad esempio:

ILP1ROFE2SSORME4RCANTI2HAORG3ANIZZATOBE4NEQUES3TOCONVEG1NO

2) ad ogni lettera del messaggio in chiaro, lettera che va letta sul disco più grande, associa la lettera corrispondente nel disco più piccolo fino a che non si incontra uno dei numeri: a quel punto la lettera corrispondente al numero determina una nuova disposizione: alla lettera A (la prima lettera della chiave) si fa corrispondere proprio questa lettera. Nell'esempio che stiamo considerando la nuova disposizione si ha in corrispondenza del numero 1: questo individua la lettera "d" (vedi Fig. 6) per cui si ruota il disco più piccolo fino a portare la "d" in corrispondenza della "A" (vedi Fig. 7).
Procedendo in questo modo la traduzione del messaggio avviene nel seguente modo:

I	L	P	1	R	O	F	E	2	S	S	O	R	M	E	4	R	C	A	N	T	I	2	H	A	…
c	h	i	d	y	c	e	r	z	h		o	c	n	l	p	f	m	p	n	h	a	x		x	…

ottenendo la seguente cifratura:

chidycerzhocnlpfmpnhaxxrbjqalmfqbgivydkakehrjyjmeikokv.

E' utile e simpatico esercizio per il lettore operare ora a rovescio. Supponiamo di ricevere, come messaggio, la sequenza sopra indicata e naturalmente di essere in presenza della macchina di Alberti azzerata con la coppia (A, r). Allora in corrispondenza di "chi" avrò "ILP" ma in corrispondenza di "d" ho il numero "1",

dunque ruoterò la macchina al contrario portando il carattere "d" in corrispondenza di "A" e ricomincerò a decifrare.

4. Confronto con gli altri metodi polialfabetici

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:

1467	*Roma*	L.B. Alberti	manoscritto del *De Componendis Cyfris*
1518	*Oppenheim*	J. Tritemio	pubblicazione del primo metodo con la tabula recta
1553	*Brescia*	G.B. Belaso	sembra essere il primo a far uso della parola-chiave
1557	*Lione*	G. Cardano	ideazione di varie tecniche
1563	*Napoli*	G.B. Porta	pubbl. del trattato *De Furtivis Literarum Notis*
1568	*Venezia*	C. Bartoli	pubblicazione del *De Componendis Cyfris* di L.B. Alberti
1586	*Parigi*	B. de Vigénère	ideazione di varie tecniche

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.

Il cosiddetto metodo di Vigénère, fa uso della tabula recta (Fig. 8), e di una parola chiave. La tecnica è molto semplice: si riporta la parola chiave lungo tutto il messaggio, ripetendola fino a coprirne tutta la sua lunghezza; ogni lettera del messaggio ed ogni lettera della chiave individuano colonna e riga nella tabella il cui punto di incrocio restituisce il carattere cifrante.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	X	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
V	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
X	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
Y	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
Z	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Fig. 8 – *La tabula recta.*

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, e considerando tutte le possibili disposizioni del disco interno si può costruire una tabella analoga alla tabula recta, che è quella qui riportata (Fig. 9).

Dunque tutti i metodi polialfabetici si basano su tavole che danno le corrispondenze; a cambiare sono le tecniche, cioè gli algoritmi di cifratura, e l'ordinamento degli alfabeti.

I vantaggi del metodo di Vigénère rispetto a quello dell'Alberti consistono in due aspetti ben precisi. In primo luogo la modifica dell'alfabeto utilizzato avviene comunque ad ogni lettera, pertanto lettere vicine provengono da cifrature che utilizzano alfabeti differenti, mentre nel metodo dell'Alberti la modifica è legata all'inserimento dei numeri, che può essere saltuaria, e che solo in teoria potrebbe anche effettuarsi dopo ogni lettera del messaggio in chiaro. In secondo luogo in Vigénère il cambio degli alfabeti avviene in modo "coperto", cioè per mezzo della chiave che è un "oggetto" di cui non si ha alcuna traccia all'interno del messaggio. Su questo aspetto il metodo di Vigénère è decisamente più sicuro. Anzi, è stata proprio questa caratteristica a decretarne la plurisecolare fortuna.

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

Fig. 9 – *Tabella degli alfabeti corrispondenti ad ogni singola disposizione del disco cifrante.*

Viceversa il metodo di Alberti ha un vantaggio spesso sottovalutato in un'ottica generale (anche uno dei metodi proposti da Vigénère, mai utilizzato, sfrutta un'idea simile): l'alfabeto sul disco più piccolo, ovvero l'alfabeto cifrante, non è ordinato nel modo convenzionale ma in modo casuale. Il grande pregio del disco cifrante è proprio questo e, sebbene Alberti non lo precisa in modo netto, si intende che tale ordine può essere scelto arbitrariamente, magari come convenzione tra le due parti, cioè come ulteriore segreto da condividere. Infatti il disco interno si può cambiare in esattamente 24! – 1 modi e quindi si può a priori scegliere un disco in funzione, ad esempio, della data. 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.

5. Conclusioni

Il metodo di cifratura di L.B. Alberti non ha ricevuto, ma probabilmente anche perché inizialmente non conosciuto, un riconoscimento pari alla sua grandezza. Infatti il più famoso metodo di Vigénère, che dal confronto con il metodo di Alberti non risulta affatto il miglior metodo polialfabetico, è stato largamente adottato fino agli inizi del secolo scorso. D'altro canto la stessa evoluzione dei metodi cifranti attraverso Tritemio, Belaso, Della Porta, Vigénère, ecc. non è stata sempre felice. Più spesso si è trattato invece di una involuzione. A tal proposito si legge, nel trattato del Generale Sacco, un parere molto negativo sul codice di Vigénère: *"… il desiderio di semplificare* (i codici usati) *per ingraziarsi i cifratori ha determinato un progressivo peggioramento dei tipi* (metodi) *proposti, fino al massimo* (degrado) *raggiunto con la cosiddetta tavola di Vigénère…"*.

In generale, uno dei punti deboli degli ultimi sistemi polialfabetici (in senso cronologico), risiede nell'uso della frase chiave che indica, ad ogni passo della cifratura, l'alfabeto da utilizzare. È chiaro che, maggiore è il numero di messaggi cifrati nello stesso modo che il crittanalista ha a disposizione, maggiori sono le possibilità che riesca ad individuare tale chiave.

L'ideale sarebbe:

- avere una chiave che cambia ad ogni messaggio, ad esempio legata a fatti o situazioni decise convenzionalmente;
- utilizzare un ordinamento diverso, seguendo l'idea di L.B. Alberti, ma modificare anche la struttura della tabella: ad esempio un quadrato latino.

Si è scoperto successivamente che la lunghezza della parola-chiave è importante. Se la parola fosse idealmente lunga come il testo da cifrare il messaggio non potrebbe essere decrittato. Ma per muoversi in questa direzione occorre ricorrere alle scrittura binaria in ottiche differenti e non pensabili al tempo dei nostri crittografi del 1500.

L'opera dell'Alberti in questo contesto appare in tutta la sua grandezza: oltre all'invenzione della cifratura polialfabetica, le idee che muovono la stessa costruzione della tecnica di cifratura sono essenzialmente le migliori.

Ma troviamo molto interessante una ulteriore considerazione. Il grande umanista si era dedicato alla stesura del De Componendis Cyfris su invito della segreteria papale testimoniando l'importanza che egli stesso attribuiva a due strutture chiave dello stato moderno, cioé la diplomazia ed i servizi segreti, che hanno necessità di corrispondenza segreta e sicura, e quindi di un sistema di cifratura impenetrabile, facile da utilizzare e difficile da rompere.

BIBLIOGRAFIA

1. C. BARTOLI, *Opuscoli Morali di L.B. Alberti… tradotti et parte corretti*, Franceschi, Venezia, 1568, pp. 198-219.

2. A. BUONAFALCE (a cura di), *De Componendis Cyfris*, Galimberti Ed., Torino, 1998.
3. L. SACCO, *Manuale di Crittografia*, 3° Edizione, Ristampa a cura della Scuola Superiore G. Reiss Romoli, L'Aquila, 1986.
4. A. SGARRO, *Codici Segreti*, A. Mondadori Ed., Milano, 1989.
5. A. BEUTELSPACHER, *Cryptology*, The Mathematical Association of America Ed., Washington, 1994.
6. F.EUGENI, *Combinatorics and Cryptography*, in Annals of Discrete Math., 1992, pp. 159-174.
7. L. BERARDI e A. BEUTELSPACHER, *Crittografia*, F. Angeli Ed., Milano, 1991.
8. F. EUGENI, Le due rivoluzioni matematiche del secolo: da Bourbaki alla matematica del discreto, Periodico di Matematiche 1 (1992), pp. 3-21.
9. F. EUGENI e D. EUGENI, *Matematica e Scienza Applicata tra Oriente e Occidente e i prodromi della moderna Teoria dell'Informazione*, Atti del Convegno "La Metodologia Storica nell'Insegnamento della Matematica e della Fisica", Ripattoni di Bellante (TE), 1998, pp. 186-200.