Ratio Math. n. 7 - 1994
179 - 186

IL CODICE DI LEON BATTISTA ALBERTI

Franco Eugeni e Diana Eugeni***
**Facoltà di Ingegneria della Terza Università di Roma*
***Facoltà di Ingegneria dell'Università dell'Aquila*

INTRODUZIONE

La necessità di trasmettere messaggi segreti è antichissima. Svetonio (140-69 a.C.) nella sua "Vita dei Cesari", presenta un codice usato da Giulio Cesare (100-44 a.C.): ogni lettera è sostituita con quella che la segue di un certo numero di posti

a b c d e f g h i l m n o p q r s t u v z - chiaro
U V Z A B C D E F G H I L M N O P Q R S T - cifrato

Ad esempio:
testo chiaro: romaeunagrandemetropoliurbana.....
testocifrato: OLHUBRI..... ROVUIU...etc.

Sul finire del Medio Evo, l'inizio di relazioni diplomatiche tra stati e staterelli, conduce all'uso dei codici segreti e con esso la ricerca della rottura dei codici in uso. Nasce quindi *"la necessità di costruire sempre nuovi codici in grado di rimpiazzare quelli ormai noti agli avversari"*.

Inizia anche l'idea graduale di sostituire le lettere degli alfabeti latini con quelle di altre culture (greche, ebraiche o inventati) o con parole (Nomenclatori). Si era infatti intuita la debolezza dei codici *monoalfabetici*, cioè degli alfabeti in biezione con un alfabeto classico, e si voleva di tanto in tanto sostituire a singole lettere intere parole, forse con un incoscio desiderio di impedire intuitive statistiche: il tallone di Achille dei codici monoalfabetici. Nacque l'uso dei Nomenclatori. La difficoltà principale era il trasporto del Nomenclatore. I tentativi di superamento di questi sistemi condussero all'idea di trovare metodi facilmente memorizzabili e trasportabili, cioè algoritmi e chiavi.

IL CONTRIBUTO DELL'ALBERTI

I vecchi codici sono più o meno legati al fatto che ad un alfabeto, diciamo in chiaro, se ne sostituisce uno nuovo, il cifrato, in una corrispondenza di simboli "uno ad uno". Il sistema usato si dice monoalfabetico.

Leon Battista Alberti - architetto, urbanista, ed anche matematico e crittografo si accorge per primo di due fatti fondamentali: (cfr. "La cifra" in "Opuscoli morali").

a) Considerata una qualsiasi lingua, e come esempio la lingua italiana, possiamo esaminare la percentuale con cui una data lettera si presenta in un discorso "abbastanza" lungo. Si scopre che ogni lettera si presenta con una frequenza che è propria della lingua. Tale frequenza delle singole lettere nella lingua, possedendo un testo di messaggio cifrato abbastanza lungo, si ripresenta nel messaggio stesso così come era per la lingua. I simboli più frequenti sono le vocali a, e, i, o ed è altamente probabile che la frequenza propria si conservi. Di fatto è possibile "indovinare" il messaggio codificato con un codice monoalfabetico.

b) Il segreto del codice deve risiedere solo in un meccanismo facilmente mutabile e questo segreto deve essere facilmente trasportabile.

c) Occorre trovare una metodologia che permetta di mutare l'alfabeto per codificare, in maniera da rompere le statistiche.

Nel Rinascimento così troviamo un cambiamento radicale, nascono i primi codici segreti che non fanno uso di un solo alfabeto cifrante, ma di molti alfabeti cifranti. Tali codici si chiamano codici polialfabetici.

Nuovi sistemi di cifratura furono ideati oltre che da Leon Battista Alberti, sul cui codice torneremo più avanti, da Giovan Battista Della Porta, celebre multiingegno napoletano (1540-1615), inventore anche della camera oscura, da Gerolamo Cardano (1501-1576), proprio lui: il medico-mago, quello dell'equazione di terzo grado, che, durante la sua sfortunata esistenza, trattò anche di argomenti crittografici di interesse notevole. Fuori d'Italia troviamo il

tedesco Tritemio (Johannes da Trittenheim, 1462-1516), ed infine il francese Blaise de Vigenere (1522-1596) che "fece il grande passo" e raccogliendo le eredità di tutti coloro che l'avevano preceduto realizzò un codice che doveva resistere ad attacchi dei più grandi genii del tempo per più di 300 anni.

L'esame dell'opera di questi Matematici, ma anche personaggi in altri campi, costituisce la migliore analisi dello sviluppo della Scienza dell'Informazione del XV e XVI Secolo.

Leon Battista Alberti nasce a Genova in una data non sicura tra il 1404 e il 1407. Proveniente da famiglia di abili commercianti a livello internazionale si dedica profondamente allo studio. Si addottora a Bologna nel 1428 ed entra al servizio del Cardinal Albergati ai cui servizi era pure Enea Silvio Piccolomini futuro Papa Pio II, lo segue a Roma ove nel 1432 viene assunto come abbreviatore Apostolico da Papa Eugenio IV (Papa dal 1431 al 1447). La situazione dei Papi ed antipapi del tempo è complessa come appare dalla tabella che segue:

PAPI	ANTIPAPI
URBANO VI 1378 - 1389	CLEMENTE VII 1378 - 1394
BONIFACIO IX 1389 - 1404	BENEDETTO XIII (Pietro De Luna) 1394 - 1414 deposto
	ALTRI ANTIPAPI
INNOCENZO VII (Cosimo Migliorati da Sulmona) 1404 - 1406	ALESSANDRO V 1409 - 1410 (muore avvelenato)
GREGORIO XII 1406 - 1417 (abdica)	GIOVANNI XXIII (Cardinale Cassa) 1410 - 1414 deposto

Il Concilio di Costanza, promosso da Sigismondo Malatesta da Rimini inizia nel 1414 e finisce nel 1418, mette fine allo Scisma d'Occidente. Gregorio XII abdica e i rimanenti due Antipapi Benedetto XIII e Giovanni XXIII sono deposti dal Concilio. Il Concilio elegge il Cardinale Colonna che prende il nome di Martino V, nel 1417.

MARTINO V	(1417-1431)	
EUGENIO IV	(1431-1447)	
NICCOLO V	(1447-1455)	
CALLISTO III	(1455-1458)	(Alfonso Borgia)
PIO II	(1458-1464)	(Enea Silvio Piccolomini)
PAOLO II	(1464-1471)	

In questa ripresa dopo lo Scisma Leon Battista Alberti entra alla Corte Papale e rimane al servizio di vari Papi quali Nicolo V Di Sarzana, Callisto III (Alfonso Borgia), Pio II (E. S. Piccolomini) ed infine Paolo II che lo licenzia dal lavoro presso il Vaticano. Il codice (crittografico) di Alberti fu elaborato, sotto Papa Piccolomini, su commissione del segretario pontificio Leonardo Dato, intorno al 1466.

Dopo il licenziamento come abbreviatore l'Alberti si dedica ai suoi lavori di Architettura. Muore a Roma nel 1472. Nel "Trattato di pittura" formula i concetti fondamentali della geometria descrittiva e può essere considerato il padre della Prospettiva. Tra le sue opere architettoniche ricordiamo il Tempio Malatestiano a Rimini, Palazzo Rucellai e la facciata di S.Maria Novella a Firenze e infine S.Andrea a Mantova.

ANALISI E CRITTOANALISI DELLA MACCHINA DI ALBERTI

Il codice crittografico di Alberti fu elaborato, sotto Papa Piccolomini e su richiesta di Leonardo Dato, segretario pontificio, intorno al 1466.

Esso era una macchina di legno mediante costituita da due cerchi concentrici. Nel disco più esterno appare l'alfabeto in chiaro formato da 24 caselle 20 delle quali contenenti lettere (mancano

per ragioni di sicurezza crittografica, le lettere che si presentano con minore frequenza, cioè h, j, k, q, w, x, y) e le rimanenti quattro contenenti i numeri 1, 2, 3, 4. Il disco interno contiene una permutazione di altre 23 lettere (mancano le lettere J e W ed U=V) formanti l'alfabeto cifrante. Esso può ruotare rispetto al primo disco.

Possiamo simularlo utilizzando, per ragioni tipografiche, un modello equivalente costituito da due striscie delle quali la prima fissa e la seconda mobile:

a b c d e f g i l m n o p r s t u v z 1 2 3 4 - chiaro
A B C D E F G H I K L M N O P Q R S T U X Y Z - cifrato

Il segreto del codice consiste nel fissare una permutazione del secondo alfabeto concordata tra trasmettitore e ricevitore e quindi una coppia di lettere che "azzera" la macchina.

B A C H I K L D E F G M N O T U P Q R S X Z Y - permutazione

(a, F) coppia di azzeramento

La macchina simulata dalla doppia striscia è pronta a lavorare secondo lo schema che segue:

a b c d e f g i l m n o p r s t u v z 1 2 3 4 - chiaro
F G M N O T U P Q R S X Z Y B A C H I K L D E - cifrato

Si prenda il messaggio : "romaeunagrandemetropoliurbana....." e lo si copi inserendo di tanto in tanto dei numeri di cambio di alfebeto nel modo casuale che segue:

rom1ae3unagr2andeme1tropoliur4bana.....

Seguendo il rapporto chiaro - cifrato iniziamo a codificare:

a b c d e f g i l m n o p r s t u v z 1 2 3 4 - chiaro
F G M N O T U P Q R S X Z Y B A C H I K L D E - cifrato

rom1aeunagr2andeme1tropoliur4bana..... testo chiaro
YXRK testo cifrato

Arrivati ad 1 si codifica 1 come se fosse una lettera però si sposta la lettera F di azzeramento sotto il numero 1 in modo da cambiare alfabeto:

a b c d e f g i l m n o p r s t u v z 1 2 3 4 - chiaro
O T U P Q R S X Z Y B A C H I K L D E E G M N - cifrato

e si continua a crittografare con il nuovo alfabeto:

rom1aeunagr2andeme1tropoliur4bana.....	testo chiaro
YXRKOQLBOSHG	testo cifrato

Al nuovo cambio di alfabeto corrisponde un secondo spostamento che consiste nel portare o (che corrisponde all'azzeramento a) verso destra fino al numero 2.

a b c d e f g i l m n o p r s t u v z 1 2 3 4	- chiaro
P Q R S X Z Y B A C H I K L D E F G M N O T U	- cifrato

e si continua a crittografare con il nuovo alfabeto:

rom1aeunagr2andeme1tropo1iur4bana.....	- chiaro
YXRKOQLBOSHGPHSXCXN	- testo cifrato

Si deve ancora cambiare alfabeto portando P sotto 1 verso destra e continuando a codificare, ma il procedimento è chiaro. La decodifica avviene a rovescio disponendo della macchina azzerata.

a b c d e f g i l m n o p r s t u v z 1 2 3 4	- chiaro
F G M N O T U P Q R S X Z Y B A C H I K L D E	- cifrato

e del messaggio da decodificare

YXRKOQLBOSHGPHSXCXN	testo cifrato
roml	decodifica fino al primo numero!

Si porta allora F sotto 1 e si continua:

a b c d e f g i l m n o p r s t u v z 1 2 3 4	- chiaro
O T U P Q R S X Z Y B A C H I K L D E F G M N	- cifrato

YXRKOQLBOSHGPHSXCXN	testo cifrato
roml aeunagr2	seguito della decodifica!

È ormai ben chiaro il meccanismo della macchina di Alberti e il nostro discorso volge al termine.

Quando è robusto il codice di Alberti è facile da dire! Se ci mettiamo nell'ipotesi che il "nemico" ovvero l'utente non autorizzato conosca la permutazione dell'alfabeto cifrante il codice appare di una debolezza estrema perché occorrono soltanto i 23 tentativi con le coppie azzeranti:

(a, A), (a, B), ..., (a, F), ..., (a, Z)

per scoprire che la coppia (a,F) ha un significato!

Se è segreta anche la permutazione iniziale i tentativi da fare sono:

24! 24

che è un grande numero. Tuttavia nasce la difficoltà del comunicarsi la permutazione, con accordi di vario tipo. Per una sovracifratura il codice di Alberti è praticamente un ottimo rinforzo.

Eravamo nella metà del 1400 ed un genio ha prodotto ed ideato tre grandi idee nuove:

la statistica

(scoprendo le frequeze di lettere in una lingua)

i codici polialfabetici

(che erano l'idea vincente ancora oggi valida);
è il caso di concludere:

il GENIO ha prodotto!

BIBLIOGRAFIA

[1] L.B.ALBERTI, *Opuscoli morali* (VI - La cifra), pubblicato postumo da Cosimo Bartoli, Venezia, 1568. (Archivi Vaticani).

[2] E.AMBRISI-F.EUGENI, *Il problema della protezione della informazione,I: cenni storici e metodi statistici per la decrittazione*, Ratio Math. 1 (1990), 15-37.

[3] L.BERARDI, *Algebra e Teoria dei Codici correttori*, Edz.F.Angeli, 1994.

[4] A.BEUTELSPACHER-F.EUGENI, *Geometrie Finite e crittosistemi: stato dell'arte e problematiche*, Atti del II Simposio Nazionale su : "Stato e prospettive della ricerca crittografica in Italia" a cura della Fondazione Bordoni, Roma, 1989.

[5] C.B.BOYER, *Storia della Matematica*, Mondadori Editore, 1987.

[6] G.CARDANO,*De subtilitate*, Basilea, 1547.(Vaticano-Apostolica)

[7] B.DE VIGENERE, *Traicte des ciffres ou secretes manieres d'escrire*, Parigi, 1586, (Roma - Biblioteca Nazionale).

[8] F.EUGENI-B.K.DASS, *How to share secrets: the idea of threshold games*, Journal of Information & Optimization Sciences, 12 (1991),451-458.

[9] R.L.MEYER, *Teoria della Comunicazione e struttura urbana*, Il Saggiatore, Edz. Mondadori,Milano, 1969.

[10] G.B. PORTA, *De Furtivis Literarum notis*, Napoli, 1563, (Roma - Biblioteca Nazionale)

[11] G.TRITEMIO, *Steganografia*, (traduzione dall'orginale latino di F.Benedetti e A.Dupré), Nardini Editore, Firenze, 1982