Storia della Crittografia

Codici Medievali

Michael Sideri 5A 2018/19

Alto Medioevo

In questo periodo la crittografia viene usata principalmente per celare nomi propri, spesso sostituendo una lettera con la successiva, come facevano già i Romani con il Codice di Cesare.
Verso l'anno mille compaiono i primi alfabeti cifranti o monografici. Essi sono usati particolarmente da parte delle repubbliche marinare e dalla corte papale di Roma e a partire dal XIV° secolo .
Un altro sistema è quello usato dall'Arcivescovo di Napoli, Pietro di Grazia, tra il 1363 e il 1365 in cui le vocali sono sostituite da semplici segni e le vocali scritte in chiaro funzionano da nulle; nelle ultime lettere il procedimento è applicato anche alle consonanti più frequenti (l,r,s,m,n), che a volte erano cifrate anche con altre lettere alfabetiche.

Tuttavia la prima cifra completa cioè dotata di segni arbitrari per ciascuna lettera, omofoni per le vocali , molte nulle e un nomenclatore, fu la lettera di Michele Steno tra Roma e Venezia scritta nel 1411.
In seguito viene ampliato il nomenclatore e, a parte la diversità dei segni cifranti, tutte le cifre italiane dei tre secoli successivi seguirono questo modello. Ne abbiamo esempi anche alla corte

Francese del XVII° secolo e perfino da parte dei nobili francesi in esilio nel 1793. Tale sistema fu in uso anche nella telegrafia segreta attorno alla seconda metà dell' '800

Eccezioni a questo canone si debbono al Cardinale Richelieu attorno al 1640 per consiglio di **Antonio Rossignol**; si tratta di repertori invertiti con gruppi cifranti variabili, con due documenti per cifrare e decifrare con omofoni per le singole lettere. Possiamo trovarne altri esempi nelle corrispondenze tra Luigi XIV° e il suo maresciallo alla fine del '600 . La loro corrispondenza, con 11.125 gruppi cifranti diversi, veniva considerata "sicura", ed infatti fu sempre cifrata con lo stesso repertorio, mentre era già stata violata nel 1689 da Wallis.
Altre cifre papali del XVI° secolo utilizzano un sistema assai diverso, ossia la cifratura con polifoni. La prima di queste cifre appare attorno al 1540; l'ultima nel 1585. Il nomenclatore di tali cifre è costituito da circa 300 voci, tutte cifrate con gruppi di tre cifre.

Il disco cifrante di L.B.Alberti

L.B.Alberti, nel suo *Trattato della cifra*, ha proposto una coppia di cerchi cifranti concentrici: uno esterno fisso con 24 caselle contenenti 20 lettere maiuscole (escluse le rare J K Y W Q H) ed i numeri 1 2 3 4 per il testo chiaro; ed uno interno mobile, con le 24 lettere latine minuscole (con U=V) per il testo cifrato: le 20 lettere maiuscole messe in ordine alfabetico: le 24 maiuscole in disordine. (questa è una norma fondamentale, trascurata da molti successori dell'Alberti, senza la quale si ha una semplice generalizzazione del codice di Cesare).Fissata una lettera maiuscola come indice (ad es. B) si deve spostare il disco mobile interno e scrivere, come prima lettera del crittogramma, la lettera maiuscola (nel nostro caso *j*) che corrisponde alla B; quindi cifrare alcune parole con la lista risultante. I numeri 1 2 3 4 servono da nulle. Quando si decide di cambiare la lista cifrante si scriverà la nuova lettera chiave in maiuscolo in modo da indicare chiaramente al corrispondente il cambio di lista. Ciò fatto, si porterà quella lettera ad affacciare l'indice B ed in questa nuova posizione si cifreranno altre parole secondo la nuova lista. Per aumentare la segretezza (le lettere maiuscole costituiscono un aiuto non solo per il corrispondente ma anche per il "nemico") l'Alberti suggerisce di usare uno dei quattro numeri per segnalare il cambio di alfabeto; la lettera minuscola corrispondente al numero sarà la nuova chiave; non vi sono quindi più lettere maiuscole e la cifra risulta così molto più sicura, e decisamente superiore a quelle che la seguirono nel tempo, e in particolare alla fin troppo famosa *Tavola di Vigénère.*

Si tratta in definitiva di una delle cifre polialfabetiche più sicure, che non ottenne il successo meritato anche per la decisione dell'Alberti di tenerla segreta. (il suo trattato fu pubblicato solo un secolo più tardi a Venezia insieme ad altri suoi "opuscoli morali" e passò quasi inosservato).

La crittografia di G.B. Porta

G.B.Porta (o Della Porta), nel 1563 pubblicò a Napoli un trattato di crittografia (*De Furtivis literarum notis - vulgo de ziferis*) molto vasto e di ottimo livello.
Tra le cifre proposte dal Porta è nota soprattutto la *tavola*, che non è certo la migliore tra quelle presenti nel trattato e che è perlopiù più debole di quelle del Bellaso e dell'Alberti.
La tavola del Porta è molto simile a quella di Bellaso, ma usa 11 alfabeti invece di 5 e introduce il cosiddetto verme letterale, poi generalmente adottato, e che ha il grave inconveniente di produrre un periodo di ciframento relativamente corto, perché comprendente solo tante lettere quante ne ha il verme nel quale le liste cifranti si susseguono tutte nello stesso ordine: particolarità su cui si basa la decrittazione del sistema, facilitata, in questo caso, dalla conoscenza degli alfabeti usati.
In realtà il Porta consiglia di usare 11 alfabeti involutori arbitrari, ma dà, come esempio la tavola con l'alfabeto base regolare: sotto questa sola forma la sua cifra è stata poi da tutti divulgata. Seguendo le indicazioni del Porta si scriverà la parola, o verme, lettera per lettera sotto ciascuna lettera del testo chiaro, ripetendola quante volte occorre: la cifratura si farà usando per ciascuna lettera del testo chiaro la lista individuata dalla corrispondente lettera chiave, come nella tavola del Bellaso.

Le cifre di G.B.Bellaso

G.B.Bellaso pubblicò nel 1553 un opuscolo, "Il vero modo di scrivere in cifra" contenente alcuni suoi cifrari polialfabetici.
L'idea è quella di ricavare diversi alfabeti (tutti disordinati) da una parola convenuta, versetto o motto.
Un esempio dell'autore: data la parola chiave sia IOVE, il primo alfabeto derivato(con V=U) è:

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

Il secondo si ottiene spostando circolarmente la seconda riga:

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

e così via fino ad ottenere cinque alfabeti; ognuno di questi sarà identificato da un gruppo di quattro lettere; p.es.:

I D V Q | I O A B C D F G H L
| V E M N P Q R S T X

O F E R | I O A B C D F G H L
| X V E M N P Q R S T

A G M S | I O A B C D F G H L
| T X V E M N P Q R S

B H N T | I O A B C D F G H L
| S T X V E M N P Q R

C L P X | I O A B C D F G H L
| R S T X V E M N P Q

A questo punto si deve convenire un altro motto, p.es OPTARE MELIORA; le lettere di quest'ultimo servono a selezionare l'alfabeto da usare.

Volendo allora cifrare la frase "Inviare truppe domani" si ha:

Verme	O	P	T
Chiaro	I N V I A R E	T R U P P E	D O M A N I
Cifrato	X C O X E G	A A I C H H	D M T D X F S

Le cifre del Bellaso sono più deboli di quella dell'Alberti perché usano pochi alfabeti ed il cambio di lista non è segreto.

Bibliografia

- http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-9900/crittografiaclassica/intro.htm
- http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-9900/crittografiaclassica/www.apogeonline.com/catalogo/allegati/483/doc/algoritmi/storia.htm
- http://www.crittologia.eu/critto/bellaso.htm