



# ANTIQUA HISTORIA

Martiani, apud Marcum Ciprianum

MM. IX.

*Cum superiorum privilegio veniaque*

# SISTEMI CRITTOGRAFICI

I metodi crittografici si sono evoluti sino a tutto il XX secolo e, rispetto a quelli sviluppati empiricamente nei tempi antichi, sono divenuti sempre più complessi ed affidabili prima con l'introduzione delle macchine cifranti, poi con l'avvento della crittografia computerizzata (vedi storia della crittografia).

La tecnica si fonda principalmente sull'utilizzo separato o congiunto di due operazioni fondamentali: la trasposizione e la sostituzione, tramite le quali sono stati messi in pratica i due principi generali della crittografia - la diffusione e la confusione - ottenendo la trasformazione del messaggio originale (testo chiaro) fino a renderlo oscuro (testo cifrato) a chi non conosce le regole del metodo adottato.

## CIFRARI A TRASPOSIZIONE

In questi cifrari le lettere del messaggio originale vengono rimescolate in modo altamente complesso tanto che il messaggio finale risulta, a prima vista, caotico. In pratica il testo cifrato non è altro che un gigantesco anagramma del testo chiaro e la chiave consiste nella conoscenza dei passi con cui ripristinare la successione originaria delle lettere. Questa semplice costruzione può essere complicata costruendo delle apposite griglie dove viene inserito il testo, applicando sistemi diversi di prelevamento delle lettere (per cui vanno lette, ad esempio, prima le colonne pari e poi quelle dispari) oppure con altro più irregolare in cui l'ordine nel quale vanno successivamente considerate le colonne è dato da una parola chiave che, di fatto, viene a costituire la chiave del cifrario.

Benché essi, storicamente, siano stati i primi ad essere usati, furono presto messi da parte: il loro segreto è infatti piuttosto debole, poiché si può scoprire con procedimenti ed induzioni relativamente semplici: i più famosi metodi utilizzati nell'antichità furono il cd. "passo del cavallo" ed i "quadrati magici".

## CIFRARI A SOSTITUZIONE

Contrariamente a quanto avviene nella trasposizione, in questi cifrari la posizione globale delle lettere non muta ma varia invece l'aspetto delle singole lettere: quelle originali, del testo chiaro,

vengono sostituite, in quello cifrato, da altre rappresentate secondo una determinata regola che, in tal modo, viene a costituire la chiave del cifrario che, può essere di due tipi: monoalfabetico o polialfabetico. Il più famoso tra i primi è il codice di Cesare mentre tra i secondi quello conosciuto impropriamente come il codice di De Vigenère ha avuto il maggior successo sino al primo ventennio del XX secolo.

- **CODICE DI CESARE**

Il metodo è basato sulla sostituzione di ogni lettera del testo chiaro con quella determinata dallo scorrimento ordinato di un prefissato numero di lettere dell'alfabeto a partire dalla "A" (quattro per quello di Cesare).

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
DEFGHIJKLMNOPQRSTUVWXYZABC

- **CODICE cosiddetto di DE VIGENÈRE**

Per cifrare il testo nascosto nella pergamena è stato usato un metodo del quale gli è stata erroneamente attribuita la paternità anche se tale sistema non è mai stato da lui ideato. Esso, invece, è una variante ricavata da quelli di altri studiosi dell'epoca, molto più semplice da risolvere rispetto ai metodi realmente sviluppati dal De Vigenère.

- **LEON BATTISTA ALBERTI**

Fu il primo a proporre l'uso di due o più alfabeti cifranti la cui sostituzione doveva avvenire durante la cifratura del testo, per confondere di più l'eventuale decrittatore. È questo il vantaggio decisivo concepito nel suo sistema; tuttavia, pur essendosi imbattuto nella più importante scoperta del millennio nel campo delle scritture segrete, non riuscì a trasformare la sua idea appena abbozzata in una tecnica ben definita. A completare l'opera provvide un gruppo di altri intellettuali di varia provenienza che misero a frutto la sua originaria intuizione.

- **JOHANNES TRITHEMIUS**

Introdusse l'uso della tabula recta, tabella formata da 25 alfabeti normali, ognuno scalato ordinatamente di una lettera a sinistra rispetto al precedente (il codice di Cesare corrisponde in questa all'alfabeto 3).

- **GIOVAN BATTISTA BELLASO**

Fece della tabula recta un uso più avanzato collegandolo ad una novità che consisteva nell'utilizzo di una frase chiave (detta verme) che veniva accodata a sé stessa, tante volte quanto era necessario per renderla lunga quanto il testo in chiaro. Si iniziava quindi a cifrare il testo chiaro prelevando il primo carattere della chiave per stabilire quale dovesse essere la riga della tabula recta da utilizzare. Quindi si ricercava nella tavola la riga il cui primo carattere fosse identico e si utilizzava tale riga come alfabeto per il primo carattere del testo in chiaro. In altre parole, la differenza rispetto al metodo di Trithèmius consisteva nel variare alfabeto in base ad una chiave invece che in maniera sequenziale.

- **GEROLAMO CARDANO**

Con l'intento di avere una chiave che variasse ad ogni messaggio, sempre utilizzando la tavola recta, ebbe l'idea di usare come chiave autocifrante il testo chiaro stesso, ripartendo dall'inizio ad ogni nuova parola da cifrare.

- **GIOVANNI BATTISTA PORTA**

Utilizza la chiave autocifrante, nella sua interezza e accodata sotto il testo chiaro, che viene applicata, però, ad una tavola di sua invenzione, diversa dalla tabula recta di Trithèmius.

- **CODICI di DE VIGENÈRE**

Dopo aver studiato i metodi degli autori sopra citati, De Vigenère costruì suoi cifrari tutti migliori e molto robusti.

Uno, infatti, utilizzava la tavola recta di Trithèmius e la chiave autocifrante del Cardano, nella forma particolare in cui la lettera iniziale era casuale e concordata e la parte aggiuntiva presa dal testo chiaro privato della lettera finale (e, in un'altra variante, dal testo cifrato). Il sistema appena illustrato introduce un nuovo concetto... errato! Il sistema della chiave autocifrante del Cardano contiene almeno due errori gravi:

- possono esserci due lettere derivanti dalla codifica. Questo succede normalmente anche con altri sistemi, ma in questo il destinatario non conosce la chiave rappresentata dal testo in chiaro... che, invece, deve essere ancora decrittato!;
- il destinatario, secondo quanto ora descritto, si trova nella stessa condizione di un crittoanalista, con l'unica agevolazione che è già a conoscenza del metodo usato in fase di cifratura, mentre il crittoanalista deve scoprire anche quello. Non è quindi un sistema comodo, né tanto meno veloce in fase di decrittazione.

Un secondo ancora, che è stato all'origine poi dell'errata attribuzione del metodo a lui stesso, utilizzava, invece, la tecnica di Giovan Battista Bellaso con la sola differenza che la chiave di cifratura era formata da lettere scelte a caso così come le corrispondenze verticali per la scelta dell'alfabeto. Infatti la sequenza letterale della prima riga orizzontale e della prima colonna verticale della tabula erano anch'esse formate da lettere dell'alfabeto scelte a caso mentre le rimanenti erano tratte da quella di Trithèmius.

Orbene, la prima trasformazione del messaggio nascosto nella pergamena, è stata fatta utilizzando la tavola recta di Trithèmius mentre la chiave è una parola breve (mortepee) scritta ripetutamente sotto al testo chiaro in modo che ad ogni sua lettera sia associata una lettera della chiave.

Per ottenere il testo cifrato il passo successivo da compiere è quello di cercare nella prima riga della tavola la lettera del chiaro e nella prima colonna quella della chiave: la lettera cifrante è quella che si trova all'intersezione della colonna con la riga. Quindi, in ultima analisi, il metodo qui adottato è quello del Bellaso.

#### • GLI SVILUPPI SUCCESSIVI

Diversamente dai codici ideati dal De Vigenère, solo quello attribuitogli per errore ebbe molta fortuna e divenne famoso. Era considerato così affidabile che fu soprannominato "le chiffre indéchiffrable" ed il metodo fu utilizzato in diversi paesi di tutto il mondo fino agli inizi del XX secolo, epoca in cui fu scoperto il modo per decodificarlo.

I codici veri ideati dal De Vigenère, dunque, passarono del tutto inosservati mentre quelli derivati dal metodo del Bellaso - si ripete, attribuito per errore al De Vigenère - furono addirittura riscoperti nei secoli successivi.

- **FRANCIS BEAUFORT**

Il sistema ideato da questo ammiraglio inglese (1774-1857) fu pubblicato, dopo la sua morte, dal fratello. Sembra che, in effetti, fosse stato inventato, verso il 1710, da Jean Sestri. Il metodo utilizza la tavola recta di Trithèmius, ma invece di aggiungere la chiave al testo chiaro, la sottrae.

- **JOSÉ DE BRONCKHORST, CONTE GRONSFELD**

Fu un militare e diplomatico belga che, verso il 1734, ideò un sistema che era un perfezionamento della cifra di Cesare alla quale, però, veniva applicata una chiave numerica, ed era anche una variante del codice di De Vigenère poiché, in effetti, utilizzava 10 alfabeti anziché i 26 della tabula recta di Trithèmius.

- **JOHN HALL BROCK THAITES**

Mentre, dunque, quasi tutti i crittoanalisti - dal XVII al XIX secolo - si erano rassegnati all'idea che il codice cd. di De Vigenère fosse inviolabile, lo scienziato inglese Charles **BABBAGE** decise di tentare l'avventura in seguito ad uno scambio epistolare con John Hall Brock Thaites. Questi si era illuso di aver inventato un nuovo sistema crittografico mentre, in realtà, altro non era che la cifratura già inventata del de Vigenère. Ignaro che la sua scoperta giungeva con qualche secolo di ritardo egli scrisse al Journal of the Society of Arts con il proposito di brevettarla.

Babbage scrisse a sua volta alla Società, obiettando che «la cifratura .. è tra le più antiche, ed è inclusa in quasi tutti i trattati». Thaites non si perse d'animo e sfidò Babbage a violare il suo sistema. Lo studioso inglese vi riuscì, probabilmente nel 1854, ma la scoperta passò del tutto inosservata perché egli non la pubblicò mai.

Perché Babbage rinunciò ad annunciare la sua vittoria su un sistema così famoso di crittoanalisi? In effetti, ciò potrebbe essere imputato alla sua cattiva abitudine di non pubblicare le sue scoperte o, forse, può essere un ulteriore esempio della sua scarsa perseveranza. Ma c'è anche un'altra possibile spiegazione. La scoperta avvenne subito dopo lo scoppio della guerra di Crimea ed essa dava all'esercito inglese un potenziale e significativo vantaggio sui russi. È senz'altro possibile che il controspionaggio inglese abbia pregato Babbage di non divulgare il suo lavoro, ciò gli avrebbe dato un vantaggio

di anni sui servizi segreti delle altre potenze che, tutte, utilizzavano la cifratura cd. di De Vigenère, ancora ritenuta inviolabile.

Nel frattempo, però, il metodo di decifrazione di Babbage era stato scoperto, in maniera indipendente, da Friedrich Wilhelm KASISKI, un ufficiale in pensione dell'esercito prussiano. A partire dal 1863 quando egli descrisse il suo procedimento, il metodo di decrittazione sopraddetto prese il nome di test di Kasiski ed il contributo di Babbage fu totalmente dimenticato per tanto tempo.

- **CODICE di VERNAM o di MAUBORGNE**

In effetti l'analisi fatta da Kasiski e da Babbage aveva posto in evidenza che la ripetizione della chiave utilizzata per cifrare il testo in chiaro costituiva il punto debole del metodo in quanto si potevano creare delle ripetizioni nel testo cifrato che ne consentivano la decodifica. I crittografi, quindi, avevano cominciato a compiere esperimenti con chiavi prive di qualunque struttura. Il risultato fu una cifratura assolutamente inviolabile.

Mentre, dunque, la Grande guerra volgeva al termine (1918) il maggiore Joseph O. Mauborgne, capo delle ricerche crittografiche dell'Esercito degli Stati Uniti - e in modo indipendente da questi, l'ingegnere della AT&T Gilbert Vernam, nel 1917- idearono il concetto di chiave casuale, cioè di una chiave formata non da una o più parole riconoscibili, ma da una serie di lettere che si succedono senza alcun ordine. Fu così introdotta la cifratura a blocco monouso (one-time pad).

È, però, da ricordare che i limiti pratici di questa sistema - in particolare l'utilizzo esclusivo (una sola volta) della chiave - ha fatto sì che l'invenzione di Mauborgne e Vernam non abbia quasi mai trovato impiego sul campo di battaglia ed il metodo rimase, quindi, pressoché teorico.

In effetti, l'impiego pratico di questo sistema è attestato in pochissimi casi. Tra questi, nelle comunicazioni tra il Primo Ministro inglese ed i componenti della squadra di Bletchley Park durante il progetto e l'utilizzo della macchina Enigma nel periodo della seconda Guerra mondiale, tra i due Presidenti dell'America e dell'URSS con il famoso "telefono rosso" e tra Che Guevara e Castro, per le operazioni militari.

È, dunque, evidente che per effettuare la penultima trasformazione del messaggio nella pergamena, è stato utilizzato il metodo di Vernam e, quindi, la sua redazione non può essere anteriore alla scoperta di tale sistema (1917): la chiave scelta, infatti, è lunga come il testo da cifrare e, anche se non è composta da lettere scelte in maniera casuale è, comunque, del tutto idonea allo scopo che si voleva raggiungere (decifrazione impossibile o, quantomeno molto difficile, con il metodo Kasiski) poiché si è utilizzata una sequenza pseudo-casuale di lettere (testo rovesciato della prima lapide della marchesa Marie de Negre d'Hautpoul) mentre, per le sostituzioni, è stata ripresa la solita tabula recta di Trithèmius.

Inoltre la scelta di un testo comprensibile per la chiave - e non di una sequenza di caratteri inintelligibili - è stata fatta con l'intento evidente di creare un collegamento tra i due documenti e, tramite il testo della lapide, dare così maggiore credibilità a quello - più recente - cifrato e nascosto nella pergamena.

## Bibliografia e Collegamenti

- C.Giustozzi, A.Monti, E.Zimuel, "Segreti, spie, codici cifrati", Apogeo, Milano 1999
- S.Singh, "Codici e segreti", Rizzoli, Milano 1999
- <http://www.riksoft.com/crivigen.htm>
- <http://www.jura.ch/lcp/cours/dm/codage/>
- <http://www.trincoll.edu/depts/cpsc/cryptography>
- <http://alpha01.dm.unito.it/personalpages/cerruti/studenti/De-Santis/crittografia.html>
- <http://www.securegroup.it/pki/sdc.htm>
- <http://www.hh.se/staff/smeraldi/publications/downloads/mscthesis/pg60-112.ps.gz>