



ANTIQUA HISTORIA

Martiani, apud Marcum Ciprianum

MM. IX.

Cum superiorum privilegio veniaque

STORIA DELLA CRITTOGRAFIA

Un breve excursus sulla storia della crittografia in Francia ci permetterà di capire quali fossero le potenziali conoscenze e le tecniche di crittografia che l'abate Bigou poteva avere a sua disposizione dato che egli è stato indicato come l'estensore materiale delle pergamene.

Sin dal 790 d.C., era conosciuto un sistema che si sa essere stato utilizzato da CARLO MAGNO, anche se qualche dubbio rimane sull'uso che può averne fatto il famoso sovrano francese in quanto è altrettanto noto come costui abbia imparato a leggere ed a scrivere solo a cinquant'anni. In un'epoca in cui l'analfabetismo imperversava - anche tra i personaggi di alto rango - la scrittura era già, di per sé, un mezzo riservato di comunicazione alle sole persone colte e, in particolare, ai membri più elevati della gerarchia della Chiesa che, infatti, proibì l'uso dei messaggi cifrati nei quali intravedeva l'opera del demonio. I dignitari di corte, invece, riservarono l'uso della cifra per i loro compiti di funzionari dello stato e fecero ampiamente uso di sistemi già noti nell'antichità.

In effetti, il metodo impiegato al tempo di Carlo Magno, era assai semplice in quanto si trattava di un cifrario a sostituzione, derivato dal codice di Cesare, complicato con artifici particolari come l'uso di punti o segni convenzionali per le vocali, di lettere diverse da quelle normalmente usate per la scrittura corrente, prese anche da lingue straniere, ed altro ancora.

In quella stessa epoca, poi, in cui era anche difficile esternare liberamente il proprio pensiero, soprattutto in tema religioso - c'era il rischio di finire sul rogo - gli scrittori presero le loro precauzioni ed utilizzarono la crittografia per nascondere i loro nomi per negare o rivendicare la paternità dei loro scritti; prese così piede, tra gli eruditi, la tecnica dell'anagramma (ad esempio François Rabelais = Alcofribas Nasier), mentre i ladri ed i briganti, per essere capiti solo dai loro compari, inventarono un linguaggio particolare, l'argot (dialetto parigino).

Venne, poi, l'idea di seguire una strada simile, ai fini diplomatici, con l'uso di linguaggi convenzionali o "jargons": nei crittogrammi i nomi dei personaggi importanti erano designati in modo convenzionale, tratti da un elenco detto "nomendatore" o "repertorio". Questo tipo di linguaggio restò in voga sino al XVII secolo: ad esempio per l'ambasciatore di Francia a Roma, nel 1622, Roma = il giardino, il Papa = la rosa ed i Cardinali della Curia erano designati con nomi di fiori.

È, dunque, dagli scritti diplomatici che prende avvio la crittografia, già fiorente nel corso del XIV secolo presso la Curia romana, a Venezia e, in seguito, nelle più grandi città italiane come Firenze,

Milano e Napoli, dove furono istituite delle ambasciate permanenti e, per proteggere la corrispondenza, fu creata la funzione, ben remunerata, di "segretario-crittologo". In effetti, chi occupava questo incarico, beneficiava di un rapporto speciale e di una confidenza tutta particolare con il proprio signore dal quale dipendeva strettamente fino ad essere impietosamente giustiziato se questi si fosse convinto del suo tradimento. Era, il crittologo, incaricato di ideare nuovi sistemi, di cifrare messaggi e, ovviamente, di cercare di scoprire i segreti di tutte le cifrature, intercettate (o comprate) alle altre potenze, soprattutto di quelle nemiche.

Con l'invenzione della stampa la crittologia assunse una veste decisamente più scientifica, l'impiego dei sistemi di cifratura s'impose e divenne generale nelle relazioni diplomatiche ed al più alto livello del comando militare.

In Francia non mancarono personaggi di grande fama per la loro grande esperienza in questa disciplina. Già durante il regno di Luigi XII, il re aveva avuto modo di conoscere il sistema di cifratura che gli Sforza avevano fatto sviluppare dal loro crittografo, Cicco Simonetta, così come al servizio della Serenissima c'era Giovanni Soro, alla Curia romana, l'Alberti e l'Argenti, a Napoli, Giovanni Battista Porta.

Ecco alcuni nomi di francesi illustri nell'arte crittografica:

PHILIBERT BABOU

Signore del castello della Bourdaisière, vicino Tours, a sud-est del paese di Montlouis sur Loire. Nel XIV secolo, sul luogo, esisteva già una fortezza che apparteneva a Jean le Meingre detto "Boucicault". Nel XV secolo, dopo numerosi cambiamenti, il castello divenne proprietà di Nicolas Gaudin, tesoriere della regina di Francia. Il 28 aprile 1510, Philibert Babou sposò Marie Gaudin e, divenuto signore della Bourdaisière (1520), fece ricostruire completamente il castello - alle cui spese contribuì lo stesso re di Francia - conservando solo la vecchia torre medievale dell'angolo nord-ovest.

Valetto di camera del re di Francia Luigi XII, poi crittografo di Francesco I ed Enrico II, era abilissimo nel decrittare i messaggi intercettati in qualsiasi lingua essi fossero scritti. Tesoriere del re, sovrintendente generale alle Finanze (1527) prese il posto di Jacques de Beaune, barone de

Semblancay e sindaco di Tours, accusato di malversazione dalla regina madre, Luisa di Savoia che lo fece condannare a morte.

Babou fu grandemente ricompensato e non è certo se tanta regale munificenza fosse dovuta solo alla remunerazione dei suoi servigi per i numerosi incarichi a corte o piuttosto anche per l'intraprendenza della sua sposa - donna bellissima - che era diventata l'amante di re Francesco (la Belle Babou) e poi del suo più grande rivale, evidentemente non solo in guerra, l'imperatore Carlo V. Nella chiesa di Saint Denis, ad Amboise, c'è un monumento marmoreo della Scuola di Tours, raffigurante una "deposizione di Cristo", che proviene dalla vecchia cappella della Bourdaisière. Secondo la tradizione Philibert Babou vi sarebbe rappresentato nella persona di Giuseppe d'Arimatea, Marie Gaudin in quello della Vergine e le loro tre figlie in quella delle Sante Donne.

Il punto dolens del metodo di sostituzione classico, come il metodo di Cesare e di Trithèmius, era quello di non sfuggire all'analisi delle frequenze e la soluzione trovata fu quella di rimpiazzare una lettera non già con un simbolo unico ma con altro, scelto a caso, all'interno di un gruppo di simboli proporzionali alla frequenza della lettera da cifrare. Questo tipo di sostituzione è chiamata "omofonica".

Il metodo inventato da Babou (1558) ne è un esempio evidente anche se non tiene conto solo delle frequenze d'apparizione delle lettere nella lingua francese. Infatti, per meglio confondere i crittoanalisti egli inserì anche delle lettere nulle, dei simboli speciali per i bigrammi ed un piccolo nomenclatore.

FRANÇOIS VIÈTE

Nato a Fontenay le Comte, capitale del Bas Poitou, fece i suoi studi di diritto all'Università di Poitiers, dove prese la laurea in legge assumendo l'incarico di avvocato del re presso il locale Tribunale. Divenne segretario e biografo del conte arcivescovo Jean de Parthenay e precettore della di lui figlia, Catherine. Visse prima al Parc Soubise (Herbiers en Vendée), poi si recò a Lione, al seguito del suo signore (1564), dove incontrò il re di Francia, Carlo IX.

Dopo la morte di Jean de Parthenay, nel 1568 seguì Antoinette d'Aubeterre e prese dimora a La Rochelle, capitale del partito ugonotto, dove incontrò i capi dei protestanti Condé, Coligny, Jeanne d'Albret ed il suo figlio Henri de Navarre che, in seguito, sarebbe asceso al trono di Francia (Enrico IV).

Nel 1571 divenne avvocato al parlamento di Parigi e nel 1579 dette alle stampe il suo Canon Mathématique. Alla morte del padre gli successe nella signoria della Bigotière e nel 1574 venne nominato consigliere al parlamento di Bretagna. Nel 1580 venne nominato dal re Enrico III, Maître des Requêtes ordinaire de l'Hôtel du Roi dal cui incarico venne allontanato, sino al 1589, a causa delle sue idee protestanti, per le pressioni esercitate sul re dai duchi di Guisa e di Nemours, capi cattolici della Santa Lega. Fu costretto, quindi, a ritirarsi nel Poitou dove si dedicò ai propri lavori matematici ed alla preparazione della sua opera maggiore: l'Art analytique.

Con l'ascesa al trono di Francia di Enrico IV riprese il suo incarico a vita di Maître des Requêtes e di consigliere del re (anche privato) e della corte reale installata a Tours. Nel 1597 venne nominato commissario per la Généralité du Poitou e, nel tempo libero, continuò a dedicarsi ai suoi lavori matematici. Nel 1600 pubblicò un proprio rapporto sul vero calendario gregoriano che fu condannato dalla Curia romana ed il fatto lo trascinò in una lunga polemica con il matematico padre gesuita Clavius, ufficialmente incaricato dal Papa (1582) della riforma del calendario. Morì a Parigi il 23.2.1630.

In Francia François Viète, rinnovatore dell'Algebra, esercitava il proprio sapere ed i suoi talenti sui messaggi cifrati della corte di Spagna e di Venezia per conto del suo re Enrico IV: «*Durant les troubles derniers j'ai découvert au Roy le plus fidèlement que j'ai pu les cahiers d'Espagne et d'Italie écrits en chiffres, où il a vu presque toujours ce qui s'est attenté au préjudice de son service et du bien de son Etat*». Viète veniva regolarmente incaricato della decifrazione delle lettere in codice e vi riuscì così bene che ricevette il titolo di decifratore ed interprete reale...ed una richiesta di condanna al Papa come negromante. Essendosi, infatti, un giorno vantato imprudentemente con dei cortigiani, dopo un buon pranzo, di saper leggere tutti i messaggi cifrati della cancelleria spagnola, l'ambasciatore di Venezia, presente all'intrattenimento, lo fece sapere al re di Spagna. Filippo II lo accusò di stregoneria perché riteneva invulnerabili le tecniche usate dai suoi crittografi che usavano un cifrario composto da più di 500 caratteri.

La lettera di Moreo al re di Spagna - primo messaggio segreto che gli fu dato da decrittare - è del 28.10.1589 ed anche se fu completamente decifrato e reso pubblico il 28.3.1590, il grande matematico francese non impiegava più di 2 o 3 giorni per decifrare i messaggi che gli venivano consegnati da Enrico IV. I segreti dell'arte, Viète li ha rivelati in un scritto redatto poco tempo prima della sua morte ("La manière de découvrir les Chiffres d'Espagne et d'Italie pour le bien du service

du Roy et de l'Etat de la France"). La memoria, indirizzata a Sully, contiene i principi che sono poi stati posti alla base della decrittazione: identificare i diversi tipi di cifra, utilizzare tutti gli indizi utili presenti nel contesto del messaggio, fare un'analisi fondata sugli studi di frequenza dei differenti segni e delle loro associazioni.

BLAISE DE VIGENÈRE

Nacque a Saint Pourçain e si preparò culturalmente a Parigi dove venne introdotto, dopo i suoi studi, a corte. La sua cultura enciclopedica, unita ad un meditato ed attento lavoro, gli permise di occuparsi oltre che in modo esteso e intenso della cultura ebraica, dell'esegesi biblica, ma anche di traduzioni che spaziavano dal greco al latino all'italiano. Si possono ricordare le traduzioni da Platone, Livio, Cicerone e tanti altri, persino dal Tasso. Primo segretario del duca di Nevers, uomo segnato dal destino, di una cultura notevolissima, è rimasto famoso soprattutto per il "Traité des Chiffres ou Secrets Manieres d'ecrire" (1586) e ancor più per il "Tractatus de Igne et Sale" (1608), può considerarsi uno dei massimi testi d'alchimia operativa.

La vita di Blaise fu affastellata da angosce dell'epoca e da personali drammi. Pare morisse in modo tragico (1596), un'agonia sofferta che sembra si determinasse per un cancro alla bocca, come ricordano documenti dell'epoca, per cui, nonostante tutti i rimedi di medici e chirurghi, morì soffocato. Vigenère prese confidenza con gli scritti degli studiosi suoi contemporanei a 26 anni, quando fu inviato a Roma per due anni in missione diplomatica. Ma a 39 anni egli giudicò di aver messo da parte abbastanza denaro per voltare le spalle alla diplomazia e dedicarsi esclusivamente agli studi. Solo allora riprese in esame, con maggiore attenzione, le idee di Alberti, Trithemius e Porta, ricavandone una tecnica crittografica nuova, coerente e di grande potenza.

ANTOINE ROSSIGNOL

I miglioramenti della tipica cifratura monoalfabetica, dei quali l'introduzione degli omofoni è un esempio, permisero di realizzare scritture segrete abbastanza sicure ma di più facile gestione, sia per il mittente sia per il destinatario, rispetto alla cifratura polialfabetica.

Una delle più resistenti cifrature monoalfabetiche della nuova generazione fu la "Grande Chiffre" di Luigi XIV. Questa era usata per crittare la corrispondenza riservata del re e rendere

inaccessibili ai potenziali avversari i suoi piani, i suoi intrighi e le sue mosse politiche. Un messaggio crittato con questo sistema riguardava una delle personalità più misteriose della storia francese, la Maschera di Ferro, ma la forza della Gran Cifra rese incomprensibile ed inutilizzabile il suo contenuto per circa duecento anni. La Gran Cifra fu inventata da una equipe familiare di crittografi, padre e figlio: Antoine e Bonaventure Rossignol. Durante la guerra contro i protestanti, il principe di Condé aveva posto l'assedio a Réalmont. La città resisteva con tutte le forze e le truppe francesi rischiavano di essere decimate dalle malattie. Condé dovette decidere se attaccare subito o se togliere l'assedio ed aveva già deciso per la ritirata, quando fu fatto prigioniero un soldato, al servizio degli Ugonotti, che aveva tentato di passare le linee nemiche. All'uomo fu trovato addosso un documento contenente una poesia così brutta che fu chiaro a tutti che nascondeva un messaggio segreto. Lo stato maggiore di Condé si mise all'opera per la decifrazione ma, ben presto, si rese conto di non riuscire nell'impresa. Fu in quel momento disperato che un ufficiale si ricordò di conoscere un gentiluomo di campagna della zona, studioso appassionato di matematica e di crittografia.

Antoine Rossignol riuscì (1626), nella stessa giornata in cui gli fu consegnato, a decifrare il messaggio. Nel testo c'erano importanti indicazioni sulla reale condizione degli Ugonotti nella città assediata, poiché scarseggiavano le munizioni e nello scritto si paventava la resa della città se non fosse stata inviata subito una spedizione in suo soccorso. Condé restituì a tarda sera il documento, con la decifrazione del messaggio segreto nascosto nella poesia, agli assediati di Réalmont e la mattina seguente la città si arrese. I Rossignol furono ammessi a corte con incarichi di rilievo, prima al servizio di Luigi XIII poi del suo successore il Re Sole che fu così colpito da tanta abilità che fece spostare i loro uffici accanto ai suoi appartamenti, in modo che potessero svolgere un ruolo di primo piano nell'elaborazione della politica diplomatica francese.

Il maggior merito dei Rossignol fu intuire la possibilità di un sistema crittografico molto più resistente di quelli utilizzati in precedenza. In effetti il metodo da loro ideato fu così forte da sventare tutti i tentativi dei crittoanalisti stranieri di impadronirsi dei segreti francesi.

Il cifrario dei Rossignol rimase in uso sino alla fine del 1700 durante il regno di Luigi XIV ed impiegato da LOUVOIS e CATINAT, che istituirono un servizio permanente di decrittazione - divenuto famoso come "Cabinet noire" (Camera nera) e già esistente durante il regno di Enrico IV - da loro riorganizzato e reso più efficiente. Resterà, per lunghissimo tempo, il servizio, primo fra tutti quelli d'Europa, e sarà completato durante il regno di Luigi XV (il "Segreto del Re") che

riuscirà a violare il servizio di cifra impiegato a Vienna per cui riceverà, regolarmente, copie dei messaggi decifrati due volte alla settimana. I codici di Rossignol - la Grande Chiffre riservata al re ed ai suoi stretti collaboratori, e la Petite Chiffre, utilizzata dai subalterni della corte reale - sono di un tipo particolare cd. "disordinato", in quanto le parole in successione alfabetica del "repertorio o nomenclatore" (ad esempio: affare, azione, attacco, altro, avviso, ecc.) venivano fatte corrispondere non già ad una successione numerica ordinata (ad esempio: 135, 136, 137, 138, 139, ecc.) ma a dei numeri a caso.

I successori di Rossignol non furono all'altezza del loro predecessore e, purtroppo, dopo la sua morte, i suoi codici non furono più usati ed i particolari del loro funzionamento furono dimenticati. Ciò rese illeggibili numerosi documenti conservati negli archivi francesi. Il servizio di cifratura francese, infine, scomparve per due motivi: l'attività fu orientata maggiormente verso il servizio di spionaggio mentre l'azione disinvolta delle cd. "Camere nere" europee - che leggeva tutta la posta che partiva ed arrivava dalle corti reali - indusse gli ambasciatori ad evitare l'impiego della posta reale ed a ricorrere sistematicamente alla valigia diplomatica, molto più lenta ma più sicura. Il "Cabinet noir", poi, venne soppresso durante la Rivoluzione: il 10.8.1790 la Costituente dichiarò l'inviolabilità della corrispondenza, principio che verrà affermato con una legge del 1850.

La crittologia francese entrò, quindi, in lento declino e ne è testimonianza, per esempio, il fatto che, nel 1796, gli emigranti francesi realisti e controrivoluzionari comunicavano con i loro partigiani in Francia impiegando un sistema che altro non era che un semplice cifrario di Cesare, completato di un piccolo nomenclatore di facile decrittazione. La situazione non migliorò affatto durante il Direttorio o l'Impero. Infatti, all'epoca della campagna d'Italia, Napoleone BONAPARTE utilizzava anch'egli un semplice cifrario a sostituzione del tipo di quello di Cesare e, talvolta tutte le lettere non venivano cifrate e comparivano in chiaro nel messaggio.

Con l'avvento dell'Impero, Napoleone dispose l'utilizzo di una Grande Chiffre e di una Petit Chiffre - che nulla avevano a che vedere con quelle del Rossignol - delle quali, però, venne fatto poco e cattivo uso. Soprattutto la Petit Chiffre non fu mai cambiata durante tutta la campagna di Russia e i servizi dello zar Alessandro I la decifravano con tutta facilità. La debolezza dei cifrari usati in seguito è testimoniata da un fatto importante: nel 1832 la duchessa de BERRY tentò di sollevare la Vandea per togliere il trono a Luigi Filippo e restaurare la dinastia dei Borboni in Francia: il progetto

falli perché la polizia intercettò e decifrò con facilità una lettera inviata dalla duchessa ad un suo agente a Parigi.

Il risveglio dell'arte crittografica in Francia avvenne intorno alla fine del 1800 con la lotta agli anarchici, dei quali furono decifrati alcuni messaggi poi presentati al processo di Ravachol (1892). Il cifrario di Rossignol fu ricostruito, nel 1893, dal generale Bazeries; la decifrazione del famoso telegramma Panizzardi, collegato all'affare Dreyfus, è del 1894, mentre nel 1899 furono decifrati i messaggi del duca d'Orleans e del partito realista che avevano complottato per rovesciare la Repubblica.

Bibliografia e Collegamenti

- S.Singh, "Codici e segreti", Rizzoli, Milano 1999
- AA.VV., "L'art du secret", Dossier Pour la Science no 36, juillet/octobre 2002