Nicola Gulmini **30 Gennaio 2019**

Corso di Storia della Tecnologia dell'Informazione

Il metodo crittografico di Maria Stuarda

Durante il corso della storia, sovrani e generali hanno dovuto evitare che i loro messaggi cadessero nelle mani del nemico. Da questa necessità si sono sviluppate le tecniche crittografiche: metodi di alterazione dei testi affinché il significato di questi sia colto solo da chi è autorizzato.
D'altra parte, il bisogno strategico di conoscere il contenuto delle corrispondenze avversarie, ha favorito l'evoluzione della crittoanalisi, che ha l'obiettivo di risalire a tale contenuto facendo breccia nel sistema utilizzato per renderlo inaccessibile.

La vera e propria battaglia tra crittografi e decrittatori ha prodotto importanti progressi scientifici. Ogni volta che una delle due parti si è trovata in vantaggio la risposta dalla controparte non ha tardato ad arrivare, ricorrendo a metodi sempre più variegati e sofisticati che affondano le radici in discipline come la matematica, la linguistica, la teoria dell'informazione fino alla fisica quantistica.

A seconda dell'epoca storica che si decide di prendere in considerazione, dai tempi dell'antico metodo della *scìtala lacedemone*, alla nota vicenda della macchina Enigma, ciò che è avvenuto è strettamente legato al tempismo e al genio di alcuni eclettici personaggi. Dei numerosi intrighi politici, uno dei più rappresentativi e drammatici è il processo di Maria di Scozia.

Maria Stuarda, nata il 9 settembre 1543, fu incoronata regina all'età di nove mesi.
La sua tenera età fece guadagnare alla Scozia un periodo di pace e la corte scozzese, per questioni strategiche, premette per il fidanzamento tra lei e Francesco, Delfino di Francia. A diciassette anni si sposarono e la Stuarda divenne regina di Francia.
Nel 1560, però, Francesco morì e Maria fu costretta a tornare in Scozia, dove trovò parte dei suoi sudditi convertiti al protestantesimo.

Nel 1565 si unì in matrimonio con Enrico Stewart, conte di Darnley, unione dalla quale nacque un erede. Darnley, però, era violento, e dopo una successione di comportamenti immorali fu strangolato. Non è chiaro se dietro il suo assassinio ci fosse la nobiltà scozzese o la stessa Stuarda.

Nell'estate del 1567 gli aristocratici protestanti costrinsero la cattolica Maria ad abdicare in favore del figlio, così, l'anno seguente, lei si vide costretta a fuggire verso sud, chiedendo ospitalità alla cugina Elisabetta I.

Elisabetta I era figlia del matrimonio tra Enrico VIII e la seconda moglie Anna Bolena, sposata dopo il divorzio da Caterina d'Aragona. Il divorzio fu una vera e propria sfida nei confronti del pontefice in carica, perciò i cattolici consideravano illecita la seconda unione di Enrico VIII e illegale l'incoronazione della figlia. Maria Stuarda, perciò, era vista come la vera regina, e questo le valse la prigionia, con la motivazione ufficiale del presunto coinvolgimento con l'assassinio del secondo marito.

Dopo diciotto anni di reclusione, la Stuarda ricevette delle lettere, recapitatele da Gilbert Gifford, un contrabbandiere che si prese la responsabilità di permettere la comunicazione con alcuni sostenitori all'esterno. Essi stavano progettando non solo di farla fuggire, ma anche di uccidere Elisabetta I e di organizzare una ribellione alla quale si sarebbe aggiunta un'invasione straniera.

Il tutto era orchestrato dal gentiluomo Anthony Babington che covava risentimento verso il potere protestante tale da spingerlo ad organizzare quella oggi conosciuta come *congiura di Babington*.

Per eludere i controlli, Babington e la regina escogitarono un sistema steganografico: occultavano i messaggi. Gifford portava le lettere ad un birraio locale, che le nascondeva all'interno di uno zipolo cavo, opportunamente protette da un involucro di pelle. Lo zipolo era utilizzato per chiudere una botte di birra, che veniva portata a Chartley Hall, castello nel quale risiedeva la Stuarda, dove un suo fidato servitore controllava i tappi e consegnava l'eventuale contenuto al destinatario. Il trucco funzionava anche nel senso inverso della corrispondenza.
In genere, la tecnica ha un punto debole: con una perquisizione più o meno attenta, risulta violabile. Per questo motivo fu adottato, in aggiunta, un sistema crittografico: non era solo il messaggio ad essere nascosto, ma anche il suo contenuto.

Il metodo impiegato era un po' più sofisticato della basilare cifratura monoalfabetica, perché ricorreva all'utilizzo di un nomenclatore: un modo di crittare che si basa su un alfabeto cifrante e di un piccolo numero di parole in codice. In particolare, il loro faceva uso di 23 simboli che prevedevano la sostituzione con le lettere in chiaro tranne *j*, *v* e *w*; 35 simboli che rappresentavano precise parole o frasi, come *da*, *c'è*, *quando*, *questo* e altri; un simbolo che indicava le doppie e quattro *nulle*, cioè lettere prive di significato che vengono ignorate da coloro che comunicano, ma che rende arduo il compito di un eventuale crittoanalista che prova a risalire al significato del messaggio, aumentandone la sicurezza.

La falla, in tutto il canale di comunicazione, aveva origine dal doppiogiochismo di Gifford. Egli, infatti, in occasione di ogni viaggio effettuava una deviazione presso Sir Francis Walsingham, segretario di stato e stretto collaboratore della regina Elisabetta I. Questi aveva accesso a tutta la corrispondenza segreta della Stuarda e, per decrittare i messaggi, si rivolse a Thomas Phelippes, miglior decrittatore d'Inghilterra e uno dei più abili crittoanalisti d'Europa che non faticò a risolvere il problema.

Il suo *modus operandi* consisteva nel contare i simboli e attribuire un significato momentaneo ai più frequenti. Se l'approccio scelto forniva risultati privi di senso, allora tentava variando alcune scelte di percorso. Così facendo riusciva a filtrare le nulle e le accantonava, poi risaliva al significato della maggior parte dei simboli, lasciandone pochi, che si comprendevano dal contesto, nonostante gli eventuali errori ortografici aggiunti di proposito per rendere difficile tale compito.

Questo strumento non era così nuovo, si tratta di un metodo chiamato *analisi delle frequenze*, che permette di eludere le cifrature, calcolando la frequenza dei simboli del testo e confrontandola con la frequenza delle lettere nella lingua utilizzata. La più antica descrizione del procedimento risale al IX secolo e si deve ad uno studioso arabo, al-Kindi, che rese obsoleti i metodi di cifratura come quelli utilizzati dalla Stuarda.

Walsingham attese di entrare in possesso di più informazioni, che arrivarono poco dopo, opportunamente tradotte da Phelippes.

Il senso di sicurezza e la fiducia, da parte dei corrispondenti, riposta nel metodo usato, furono il motivo per il quale Walsingham riuscì a risalire ai nomi dei cospiratori e agli intenti chiari delle parti. Il segretario, infatti, fece modificare il contenuto di una lettera per fare in modo che Babington fornisse tutte le informazioni che gli servivano, senza nutrire alcun sospetto.
Egli temporeggiò per poter dimostrare l'incontrovertibile colpevolezza della Stuarda, altrimenti la regina Elisabetta non avrebbe acconsentito a farla giustiziare. Infatti, una mossa politica pesante come l'uccisione del capo di un paese, avrebbe avuto non poche conseguenze. Elisabetta I, inoltre,

aveva parecchi nemici e il legame di parentela non trascurabile con la Stuarda contribuiva alla sua titubanza.

Successivamente, Walsingham riuscì a catturare e giustiziare Babington e i cospiratori che lo assecondavano, dopo averli costretti a confessare.

L'11 Agosto 1586, Maria di Scozia fu arrestata con l'accusa di aver partecipato ad un complotto contro la corona inglese: tradimento, per il quale l'imputato non può farsi assistere o convocare testimoni a propria discolpa. Durante il processo lei si dichiarò completamente estranea al coinvolgimento, ma le prove in possesso di Walsingham erano troppo solide ed ella fu giustiziata l'8 febbraio 1587.

RIFERIMENTI BIBLIOGRAFICI

Simon Singh, *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, Milano, BUR Rizzoli, 2016

Per l'introduzione:

Alessandro Languasco, Alessandro Zaccagnini, *Manuale di crittografia. Teoria, algoritmi e protocolli*, Milano, Hoepli, 2015