Aoi

Marco Moraglio

Crittografia e crittoanalisi

Dietro le righe della storia, tra sviluppi tecnico–scientifici e conflitti

Prefazione di
Davide Arecco

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-2019-4

I edizione: novembre 2018

A mamma e papà,
semplicemente grazie

Il desiderio di svelare segreti è profondamente radicato nella natura umana; la promessa di partecipare a conoscenze negate ad altri eccita anche la mente meno curiosa. Qualcuno ha la fortuna di trovare un lavoro che consiste nella soluzione di misteri, ma la maggior parte di noi è spinta a soddisfare questo desiderio risolvendo enigmi artificiali ideati per il nostro divertimento. I romanzi polizieschi o i cruciverba sono rivolti alla maggioranza; la soluzione di codici segreti può essere l'occupazione di pochi.

John Chadwick, *The Decipherment of Linear B*

Indice

Ringraziamenti

Un lavoro come questo non sarebbe stato possibile senza l'aiuto di diverse persone ognuna fondamentale seppur con contributi diversi.

Desidero ringraziare, in primo luogo, il mio relatore, il professor Arecco sia per la disponibilità che mi ha concesso sia per il costante entusiasmo che mi trasmetteva ad ogni incontro oltre che, naturalmente, per la preziosa prefazione. Inoltre, devo rivolgere un sentito ringraziamento anche alla professoressa Maria Federica Petraccia per avermi aiutato nella realizzazione dell'intera "parte prima" di questo lavoro.

Un sincero ringraziamento lo devo rivolgere anche al Dott. Federico Burlando, "Burla" per gli amici, che ho interpellato diverse volte per farmi consigliare un titolo accattivante sfruttando le sue immense doti creative.

Non posso non ringraziare anche la dott.ssa Carla Palazzesi per avermi aiutato a realizzare la corretta impaginazione di questo libro.

Ringrazio di cuore la dott.ssa Elisa Gentile, la mia ragazza, che da oltre sette anni è al mio fianco in ogni "battaglia" e che forse più di tutti ho "annoiato" con la storia della crittografia fin dai tempi della tesina del liceo… A lei che è il mio "tutto" va un ringraziamento speciale per avermi fatto crescere sotto tanti punti di vista in tutti questi anni e per avermi sempre spronato ad andare avanti.

Infine, la mia più grande riconoscenza, va ai miei genitori (ai quali dedico questo mio elaborato) che fin da quando sono nato mi supportano e mi aiutano a cercare di realizzare ogni mio desiderio: è grazie a voi che oggi sono qui.

Tra le righe della storia

di Davide Arecco[1]

È con un grande piacere che mi accingo a introdurre questo splendido libro del dott. Marco Moraglio. Per più motivi. In primo luogo, l'autore è stato in assoluto uno dei miei migliori allievi di sempre, serio e appassionato nei riguardi sia della storia sia della ricerca storica. In secondo luogo, questo lavoro – che nasce dalla rielaborazione della sua Tesi di Laurea magistrale, discussa con me presso l'Ateneo ligure – è frutto di studio e indagini accuratissimi, condotti con mano sicura e con altresì una grande attenzione per la scrittura e la forma narrativa (perché fare storia è anche, non va dimenticato, saper raccontare). In terzo luogo, il libro che il lettore ha tra le mani è dedicato a un argomento – la crittografia e le scritture segrete – che, oltre ad essere di grande fascino, riveste una importanza certo non secondaria nel corso dei secoli, come il lettore potrà constatare.

Non a caso, la ricerca di Marco Moraglio è di fatti una ricostruzione storiografica del percorso fatto dalla crittografia, dalle sue origini, sino a oggi. Egli non si è concentrato solo su un autore, oppure un gruppo di autori, o solo sull'età moderna e contemporanea, alla quale di solito si pensa quando ci si rivolge a questo argomento. No. Ha saputo, correttamente e con un grande ordine metodologico, riscrivere una storia di lungo periodo, poco nota o affatto conosciuta, sempre affascinante.

Oggi i *codici*, si sa, vanno di moda. Basta scorrere le novità letterarie, in qualunque libreria, non sempre di qualità o spessore. Queste ultime due caratteristiche sono invece presenti nel libro di Marco Moraglio, autore di uno studio serissimo e molto circostanziato, che demitizza là dove necessario e passa al vaglio della storia scritture e tecniche, attraverso le epoche e i loro protagonisti maggiori.

In effetti, di un libro come questo si sentiva davvero la mancanza. Sulla crittografia, infatti, vi è pochissimo in circolazione e sovente il taglio è molto, troppo divulgativo (complice il successo di Dan Brown

[1] Professore di Storia della scienza e della tecnica nell'età dell'Illuminismo dell'Università di Genova.

e altri scrittori a lui affini). Il pubblico vuole e ama scoprire segreti, capire cosa è stato celato, come e perché. Grazie a questo libro, può finalmente farlo in maniera chiara ed esaustiva, fonti alla mano. Le competenze storiche e la perizia filologica di Marco Moraglio ci donano in altre parole un libro che pare essere il saggio definitivo sul tema. Un saggio a lungo atteso. E se non entro qui in ulteriori dettagli, è solo per non rovinare il piacere della lettura.

Introduzione

La storia vera è quella segreta

Ronald Syme

È da sempre nella natura dell'uomo la necessità di comunicare.

Il progresso e l'emergere di nuove forme di società hanno ampliato lo scambio comunicativo trovandosi di fronte alla crescente necessità di sicurezza. Le informazioni non solo devono essere distribuite, ma diventa fondamentale anche che potenziali nemici non siano in grado di comprendere il significato del messaggio.

Un ordine in battaglia, un trattato diplomatico, una corrispondenza privata tra aristocratici, sono esempi di informazioni che, se finite nelle mani sbagliate, possono compromettere l'esito di un conflitto o provocare la destabilizzazione politica di un regno.

Il pericolo dell'intercettazione del testo da parte degli avversari promosse lo sviluppo di messaggi crittati che facevano uso di tecniche di alterazione del testo destinate a renderlo comprensibile solo alle persone autorizzate.

Da queste esigenze sociali e politiche è nata la crittologia che può essere divisa in due vere e proprie scienze atte una alla protezione dell'informazione e l'altra alla relativa decodificazione: la crittografia e la crittoanalisi.

Il termine crittologia deriva dal greco ed è una parola formata dai termini *κρυπτός*, che significa "nascosto" e *λόγος*, che significa "parola, discorso, argomento" e quindi, più liberamente, "scienza".

La crittografia ha per oggetto ogni operazione concernente le scritture segrete e può essere definita come la scienza che si occupa della protezione dell'informazione; la crittoanalisi, invece, è una disciplina che ha per oggetto i metodi di ricostruzione del testo in chiaro partendo da un contenuto cifrato di cui si ignora la chiave.

Tra crittografia e crittoanalisi, quindi, è come se fosse nata una continua battaglia, una lotta infinita "a colpi di nuovi codici e continue decifrazioni" con lo scopo, da parte della prima, di creare un sistema indecifrabile e, della seconda, di risolvere e scoprire ogni segreto.

Si tratta di uno "scontro" che continua ancora oggi e che non riguarda più esclusivamente determinati individui come ad esempio diplomatici o speciali membri dei servizi di intelligence. Se, infatti genericamente fino alla Seconda Guerra Mondiale la crittologia era oggetto di interesse principalmente per le comunicazioni militari e diplomatiche, oggi, esistono grandi quantità di dati che noi tutti usiamo e che richiedono sicurezza e riservatezza quali, ad esempio, numeri di carte di credito, codici bancomat o, ancora, registrazioni legali e qualsiasi tipo di transazione che eseguiamo su internet, che viaggiano su canali pubblici (quindi teoricamente accessibili a tutti) e che necessitano, dunque, di essere protetti.

L'obiettivo di questo lavoro, è quello di creare una sorta di breve *storia della crittografia* andando ad analizzare i principali metodi che sono stati sviluppati e utilizzati nel corso dei secoli. Ho deciso quindi di concentrare la mia ricerca partendo dai sistemi, anche di *intelligence*, che sono nati all'alba della storia per arrivare a "gettare uno sguardo" su alcuni dei più importanti metodi utilizzati durante il secondo conflitto mondiale.