CRITTOGRAFIA

Book Series

2

CRITTOGRAFIA

Book Series

It is impossible to agree beforehand about things
of which one cannot be aware before they happen

— Polibyus (150 BC)

La collana raccoglie le opere scientifiche che riguardano e approfondiscono l'affascinante, enigmatico e complesso campo crittografico.
La Crittografia è una materia molto ampia, che comprende tanto la progettazione di algoritmi, quanto lo sviluppo di tecniche crittoanalitiche. L'intento è quello di raccogliere opere che presentino e analizzino sia gli aspetti più teorici, tra cui le basi matematiche, sia quelli più pratici, tra cui gli aspetti protocollari. In questa ottica, inoltre, è interessante e necessario fornire visibilità alle innovazioni più promettenti, come la crittografia *postquantum*, la tecnologia blockchain e la cifratura nel cloud.
La collana ospita volumi che trattano ogni ambito della Crittografia, interessando e raggiungendo trasversalmente differenti contesti scientifici e divulgativi: note di lezioni universitarie per favorire la comprensione e la diffusione di tale disciplina; atti di convegni specializzati, per incrementare la consapevolezza della comunità scientifica nazionale e internazionale; monografie, che comprendono anche tesi di laurea e di dottorato, per divulgare ricerche e sperimentazioni.

The book series collects cryptographic works with ample scope.
Cryptography is a wide discipline, encompassing algorithm design and the investigation of cryptanalytic techniques. The book series aims at presenting both theoretical aspects, in particular the mathematical bases, and practical aspects, e.g. protocols. Along this line, we want to highlight the most promising innovations, such as *postquantum* cryptography, blockchain technology and cloud encryption.
The book series hosts lecture notes, to help spreading the knowledge of this fascinating subject, as well as workshop proceedings, to help the Italian scientific community collaborate, as well as specialized monographs, including Master's theses and PHD theses.

Vai al contenuto multimediale

Luigi Pasini

Delle scritture in cifra usate dalla Repubblica di Venezia (1872)

a cura di
Paolo Bonavoglia

Presentazione di
Michele Elia, Massimiliano Sala

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

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

ISBN 978-88-255-1926-6

I edizione: febbraio 2019

Pasini an intelligent and likable young man, succeeded in solving about 5.000 lines …

David Kahn, *Codebreakers*

Indice

Presentazione

MICHELE ELIA[*], MASSIMILIANO SALA[**]

La crittografia veneziana occupa una posizione rilevante nella storia delle scritture segrete, e per secoli ha dominato lo scenario europeo (almeno quanto quella dello Stato Pontificio) per la valentia dei suoi crittoanalisti e l'efficienza dei suoi servizi segreti. Servizi d'informazione indispensabili per la gestione dei commerci della Serenissima nel teatro mediterraneo, ma che furono anche decisivi per la storia d'Europa come lucidamente descritto nel saggio *Lepanto, La battaglia dei tre imperi,* dello storico Alessandro Barbero. In questa monografia è giustificato chiaramente l'impiego della crittografia per convogliare informazioni vitali a Venezia da Costantinopoli, al tempo in cui una missiva impiegava settimane, quando non mesi, per arrivare attraverso territori pericolosi, se non ostili.

La poderosa organizzazione dei servizi di Venezia, la ricchezza, la rilevanza dei loro archivi e l'efficacia dei loro metodi sono descritte con dovizia nel libro dello storico Paolo Preto, *I servizi Segreti di Venezia*. E proprio Luigi Pasini, archivista all'Archivio di Stato di Venezia tra il 1855 e il 1885, si appassionò alla crittoanalisi dei molti messaggi che giacevano cifrati, ma non dischiusi, in archivio. Il Pasini raccolse i suoi primi successi di decifratore in un breve trattato, *Delle scritture in cifra usate nella Repubblica di Venezia*, opera che pubblicò nel 1872.

Questo interessante lavoro di crittoanalisi, riscoperto dal professor Paolo Bonavoglia, è riproposto in questa collana a cura e con un utile commento dello stesso Bonavoglia. La crittoanalisi non ha un gran

[*] MICHELE ELIA, Politecnico di Torino, Dipartimento di Elettronica e Telecomunicazioni.
[**] MASSIMILIANO SALA, Università degli Studi di Trento, Dipartimento di Matematica.

numero di testi di riferimento, anche i libri sulla crittografia preferiscono la parte costruttiva e i metodi matematici. Il lavoro di Pasini è sicuramente interessante in una prospettiva storica, tuttavia la crittoanalisi ha molti seguiti imprevedibili, e vecchie idee possono essere utili ad attaccare sistemi crittografici nuovi, quindi il pratico interesse per questo testo potrebbe rivaleggiare con il suo indiscusso interesse storico.

L'opera del Pasini non poteva trovare miglior curatore del professor Paolo Bonavoglia, nipote e allievo del Generale Luigi Sacco.

Prefazione

PAOLO BONAVOGLIA*

Sulla storia della crittografia veneziana dal Medio Evo alla fine della Serenissima Repubblica, non ci sono molte fonti; vi dedica alcuni cenni distribuiti su alcune pagine David Kahn nel suo monumentale *Codebreakers*[1]:

> Perhaps the most elaborate organization was Venice's. It fell under the immediate control of the Council of Ten, the powerful and mysterious body that ruled the republic largely through its powerful secret police. Venice owed her preeminence largely to Giovanni Soro, who was perhaps the West's first great cryptanalyst. Soro, appointed cipher secretary in 1506, enjoyed remarkable success in solving the ciphers of numerous principalities[2].

mentre in italiano, oltre all'opuscolo di Luigi Sacco[3] che ne tratta fra quelle di altri stati italiani, c'è solo il volumetto di Luigi Pasini[4] archivista all'Archivio di Stato di Venezia tra il 1855 e il 1885, che viene ora ripubblicato; recentemente c'è solo il capitolo sulle cifre venezia-

* Paolo Bonavoglia, già docente di matematica al Liceo Foscarini di Venezia; dal marzo 2018 presidente della sezione Mathesis di Venezia.

[1] KAHN, *Codebreakers*,1967–1996, probabilmente la più completa opera di storia della crittografia della letteratura mondiale.

[2] Forse l'organizzazione più sofisticata era quella di Venezia. Era sotto il diretto controllo del Consiglio dei Dieci, il potente e misterioso organismo che dominava la repubblica per lo più con la sua potente polizia segreta. Venezia dovette la sua preminenza in gran parte a Giovanni Soro, che fu forse il primo grande crittoanalista dell'Occidente. Soro, nominato segretario per le lettere nel 1506, ottenne straordinari successi nel risolvere i codici di numerosi principati.

[3] SACCO, *Un primato italiano: la crittografia nei secoli XV e XVI* 1958.

[4] PASINI, *Delle scritture in cifra usate nella Repubblica di Venezia* 1872.

ne nel libro di Paolo Preto[5], più orientato agli aspetti storici che a quelli prettamente crittografici.

L'archivio veneziano contiene migliaia di documenti della storia della Repubblica di Venezia, ed è la principale fonte intorno alle cifre veneziane. Vi sono conservate lettere ducali, dispacci di ambasciatori, comandanti militari, governatori, e una significativa parte di questi sono scritti in cifra; non ci sono per la verità grandi enigmi irrisolti, della maggior parte dei molti messaggi c'è la *deciferazione* ufficiale da parte della cancelleria del Doge. Di alcuni c'è il testo chiaro trascritto negli atti segreti del Senato. Inoltre, nel fondo del Consiglio dei Dieci[6] sono custodite centinaia di *chiavi di cifra*.

Ma ci sono eccezioni: per alcuni periodi e per alcuni dispacci mancano le *deciferazioni* ufficiali della cancelleria.

Nella seconda metà dell'Ottocento Luigi Pasini, archivista all'Archivio di Stato di Venezia tra il 1855 e il 1885[7], anno della sua morte; a partire dal 1865 cominciò ad interessarsi dei numerosi dispacci cifrati irrisolti, soprattutto nel periodo a metà Cinquecento, dopo il 1554, e in quei trent'anni riuscì in una rimarchevole impresa crittografica, decrittandone un gran numero, circa 5.000 linee secondo Kahn.

Pasini si occupò soprattutto delle cifre del XVI secolo, nel decennio dopo il 1554 periodo per il quale mancano i testi decifrati e le chiavi di cifra, forse a causa di un incendio. Nel 1868 si occupò dei dispacci dell'ambasciatore veneziano in Inghilterra Giovanni Michiel, che nello stesso periodo erano stati decrittati dall'inglese Paul Friedmann; ne nacque una controversia su chi avesse per primo trovato la chiave; Friedmann che aveva ottenuto dall'archivio di Venezia le copie dei testi cifrati accusò Pasini di essersi vantato di meriti non propri, Pasini replicò con un opuscolo[8] ammettendo la priorità di Friedmann ma rilevando un gran numero di errori e lacune nel testo decifrato e riassumendoli in una tabella comparata. Pasini aveva certo due

[5] PRETO, *I servizi segreti di Venezia*, 1994.

[6] ARCHIVIO DI STATO DI VENEZIA: *Cifre, chiavi e scontri di cifra con studi successivi di L. Pasini e G. Giomo, sec. XVI – sec. XVIII*.

[7] Della vita di Luigi Pasini ho trovato ben poco; solo Kahn nel suo *Codebreakers* (cap. "Ciphers in the past tense" p. 858) fornisce qualche cenno biografico.

[8] PASINI, *I dispacci di Giovanni Michiel, deciferati da Paolo Friedmann*, *rettificazioni ed aggiunte di Luigi Pasini* 1869.

grossi vantaggi su Friedmann, la migliore conoscenza della lingua italiana, e, in quanto archivista, la facilità di disporre di tutti i documenti in originale.

Questo sia pur parziale successo lo spinse ad appassionarsi sempre più di crittografia e a tentare l'attacco ad altri cifrari dei quali si era persa la chiave; riuscì a ricostruire il cifrario degli ambasciatori in Francia, in Spagna e a Costantinopoli, e in seguito anche quello della Germania[9].

Nel 1871 Pasini riassunse i suoi primi successi nel volumetto qui ripubblicato, nel quale spiegava come aveva fatto a decrittare i dispacci, ma con qualche grossa reticenza proprio sui punti chiave; singolare è poi la presenza di un capitolo intitolato "*Dimostrazione della cifra di duplice alfabeto*"[10] dedicata a una cifra che non ha nulla a che vedere con i codici usati dalla diplomazia veneziana; ma in questo Pasini sembra ricalcare quella che David Kahn[11] definì la schizofrenia della crittografia rinascimentale: da un lato gli ingegnosi cifrari proposti a livello teorico da L. B. Alberti, G.B. Bellaso, G.B. Porta, l'abate Tritemio e Blaise de Vigenère, dall'altra i cifrari usati dalle varie diplomazie europee, quasi tutti basati su cifrari completamente diversi, i *nomenclatori*.

Negli anni successivi Pasini continuò a decrittare un gran numero di dispacci cifrati, e dalle carte trovate all'Archivio di Stato di Venezia risulta che stava lavorando a una nuova opera in quattro libri, della quale non si trova traccia; probabilmente la morte prematura sopravvenuta nel 1885 gli impedì di completare questo progetto.

In questo volumetto viene ripubblicato il primo opuscolo del 1872, ormai quasi introvabile, aggiungendovi una memoria trovata tra le sue carte e una postfazione dove riferisco sulla mia indagine tesa a chiarire il metodo seguito da Pasini.

Alle note a piè di pagina ne ho aggiunta qualcuna riconoscibile dalla sigla finale (N.d.C.). Ho inoltre reimpaginato la lista cifrante del capitolo V che era spezzata in due e di difficile lettura.

[9] Può suonare strana la parola *Germania* per dispacci del XVI secolo quando ancora non esisteva uno stato nazionale tedesco; si tratta in effetti del *Sacro Romano Impero,* prevalentemente formato di stati di lingua tedesca. E l'Imperatore, tra i tanti titoli, aveva anche quello di *Rex Germaniae*.

[10] PORTA, *De Furtivis literarum notis,* 1563.

[11] KAHN, *Codebreakers* 1967–1996, chap. 4 "On the Origin of a Species".

Devo ringraziare Michela Dal Borgo, Monica Del Rio e Giovanni Caniato, archivisti all'Archivio di Stato di Venezia, per l'assistenza fornita alle mie ricerche e in particolare ai miei primi passi tra filze, buste e fondi dell'archivio.

Un ringraziamento anche alla casa editrice ed a Michele Elia e Massimiliano Sala per aver inserito il libro nella collana *Crittografia* e per la bella presentazione del libro.

PARTE I

DELLE SCRITTURE IN CIFRA USATE DALLA REPUBBLICA DI VENEZIA

LUIGI PASINI*

* Luigi Pasini (1835 – 1885), archivista presso l'Archivio di Stato di Venezia tra il 1865 e il 1885.

Capitolo I

Introduzione

Scopo della presente pubblicazione è di dar un saggio di quanto intorno alle *scritture occulte nella Diplomazia Veneziana* si conserva nell'Archivio Generale di Venezia; di far conoscere i più valenti *cifristi*, le principali disposizioni che regolarono ne' tempi questo importante amminicolo dell'arte di Stato nel Governo Aristocratico di Venezia; e di offrire, in tal guisa, una breve notizia di quella scrittura, delle sue specie, e delle sue vicende.

Nel 1870 si eseguì nell'Archivio Generale il riordino delle *chiavi*, o *scontri di cifra*, e di altre carte relative a questa materia che giacevano confuse in una delle stanze dove si trova l'archivio degli Inquisitori di Stato. Queste chiavi, che ascendono ad oltre 400, con alcuni trattati, studi, teorie ed altro, sono disposte in ordine cronologico, e divise secondo la loro specie in otto grandi buste. Ne venne compilato un catalogo in cui sono indicati il numero progressivo, l'epoca, l'esponente della chiave, chi ne faceva uso, il numero delle pezze, il numero della busta, e nella finca delle *osservazioni* alcuni decreti che approvavano o vietavano per ragioni di secretezza, l'uso di una chiave.