DE CIFRIS KOINE
Book Series
Volume III

ERUDITORUM ACTA 2024

DE CIFRIS KOINE
Series Editorial Board

DE CIFRIS KOINE
Book Series

De Cifris Koine è una collana editoriale curata da De Cifris Press, marchio dell'associazione nazionale De Componendis Cifris dedicata allo studio e alla divulgazione della crittografia e delle discipline correlate.

Questa collana rappresenta un punto di riferimento per la comunità crittografica italiana, offrendo una panoramica delle ricerche e delle innovazioni nel campo. Attraverso la pubblicazione degli atti di conferenze e workshop, De Cifris Koine fornisce non solo approfondimenti scientifici, ma anche contributi divulgativi, mettendo in luce i progressi e le attività dei principali esponenti in questo ambito.

La serie abbraccia un ampio spettro di argomenti, estendendosi oltre la crittografia stessa per includere le sue molteplici applicazioni e intersezioni con altre discipline. Tra queste, si annoverano la teoria dei codici, vari rami della matematica come l'algebra, la teoria dei numeri e la geometria, l'informatica con un focus particolare sulla cybersecurity e sull'informatica teorica, nonché l'ingegneria elettrica, le telecomunicazioni, la storia e gli aspetti legali legati alla crittografia.

Gli articoli pubblicati in questa collana sono accettati in tre lingue: italiano, inglese e francese.

La periodicità della pubblicazione è trimestrale.

De Cifris Koine is a book series published by De Cifris Press, publishing house of the national association De Componendis Cifris, whose activities focus on cryptography and related topics. De Cifris Koine volumes form the voice of the Italian cryptographic community, as they collect communications from both scientific and educational events and summaries of papers of its members and of their activities. In particular, De Cifris Koine hosts conference and workshop proceedings, including short abstracts.

Topics covered in De Cifris Koine volumes relate to cryptography and its applications to and connections with other disciplines, as for example coding theory, maths (mainly algebra, number theory and geometry), computer science (mainly cyber security and theoretical computer science), electronic engineering, telecommunication engineering, history of cryptography and law.
Accepted articles are either in Italian, English or French.
Volumes are published quarterly.

La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

Cette collection est une référence importante pour la communauté cryptographique italienne, offrant une vue d'ensemble de la recherche et des innovations dans ce domaine. Grâce à la publication d'actes de conférences et de groupes de travail (workshops), la De Cifris Koine fournit non seulement des contributions scientifiques académiques, mais aussi des contributions à destination du grand public, mettant en lumière les progrès et les activités des principaux acteurs et des principales actrices du domaine.

Les articles de cette collection couvrent un large éventail de sujets allant de la cryptographie à ses nombreuses applications et intersections avec d'autres disciplines. On y retrouve notamment la théorie des codes, diverses branches des mathématiques telles que l'algèbre, la théorie des nombres et la géométrie, l'informatique, avec un accent sur la sécurité informatique et l'informatique théorique, ainsi que le génie électrique, les télécommunications et les aspects juridiques de la cryptographie. Les articles soumis à la De Cifris Koine sont acceptés en italien, anglais et français. La fréquence de publication est trimestrielle.

ERUDITORUM ACTA 2024

Edited by:

– *Antonino Alì*,
Università di Trento, Italy.
– *Massimiliano Sala*,
Università di Trento, Italy.

Pubblicazione trimestrale di proprietà dell'associazione nazionale di crittografia
De Componendis Cifris

Autorizzazione del Tribunale di Milano in data 23 - 02 - 2024
Num. R.G. 1315/2024 Num. Reg. Stampa 22
ISSN 3034-9796 - ISBN 979-12-81863-02-6

Editore: De Componendis Cifris APS.
Marchio Editoriale: De Cifris Press.
Direttore responsabile: Massimiliano Sala
Redazione: Antonino Alì, Nadir Murru
Luogo di pubblicazione: Via Gianfranco Zuretti 34 - 20125 Milano
e-mail: editorial@decifris.it
Stampa in proprio
Numero 3 - Pubblicato il 01 - 09 - 2024

PREFACE

Questo volume, raccogliendo i contributi presentati durante il nostro convegno *"De Cifris Eruditorum 2024"*, offre un'analisi multidisciplinare della crittografia, tracciando il suo percorso storico ed esplorando, da un punto di vista giuridico, le sue attuali applicazioni e implicazioni.
I tre interventi storici toccano sia l'età classica, sia il Medio Evo, sia il Rinascimento. I due contributi giuridici si concentrano sulla cyber security e sul delicato equilibrio tra il rispetto dei diritti fondamentali e la necessità di sicurezza.

This volume contains all talks given at our conference *"De Cifris Eruditorum 2024"*. It offers a multidisciplinary approach to cryptography, starting from its historical evolution and arriving at exploring its current applications from a legal point of view.
The three historical talks touch on the cryptographic evolution in the classical age, in the Middle Ages and in the Renaissance.
The two talks by legal experts focus on cyber security and the difficult balance between fundamental rights and security needs.

Ce volume, rassemblant les contributions présentées lors de notre conférence *"De Cifris Eruditorum 2024"*, offre une analyse multidisciplinaire de la cryptographie, retraçant son parcours historique et explorant, d'un point de vue juridique, ses applications et implications actuelles.
Les trois interventions historiques couvrent l'âge classique, le Moyen Âge et la Renaissance. Les deux contributions juridiques se concentrent sur la cyber sécurité et sur le délicat équilibre entre le respect des droits fondamentaux et la nécessité de sécurité.

Massimiliano Sala & Antonino Alì
Editor in Chief & Managing Editor
De Cifris Koine

Indice

Introduzione a Eruditorum ACTA 2024 2
Antonino Alì and Massimiliano Sala

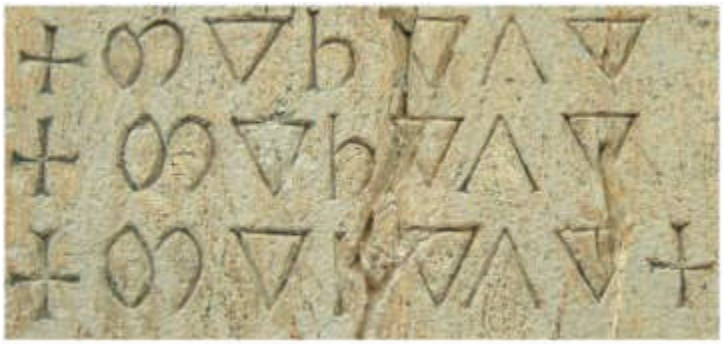
Franceschi - Partenio, una disputa crittografica nel Rinascimento 5
Paolo Bonavoglia

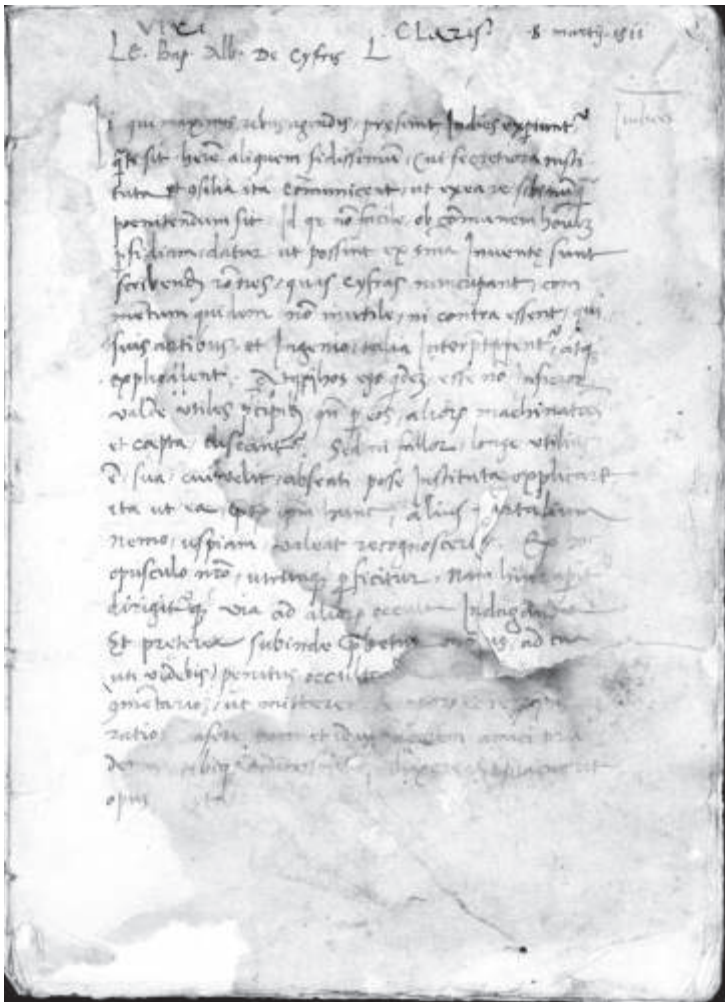
Scrivere per nascondere, leggere per scoprire. Le origini della crittografia 24
Marco Moraglio

Epigrafi cifrate nelle chiese antiche 35
Cosimo Palma

Il nuovo framework giuridico cyber dell'Italia. La crittografia come strumento di cybersicurezza e per l'autonomia strategica nazionale 52
Marcello Albergoni

Human Rights Implications of Encryption Backdoors 59
Antonino Alì





Introduzione a Eruditorum ACTA 2024

Antonino Alì and Massimiliano Sala

Università di Trento

Questo volume offre un'analisi multidisciplinare della crittografia, tracciando il suo percorso storico e esplorando, da un punto di vista giuridico, le sue attuali applicazioni e implicazioni. Raccogliendo i contributi presentati durante il convegno *"De Cifris Eruditorum 2024"*, tenutosi il 15 marzo 2024 presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento, questa raccolta illumina le molteplici sfaccettature di una disciplina che si situa all'intersezione tra matematica, storia, diritto e tecnologia.

La crittografia, arte e scienza della comunicazione segreta, ha giocato un ruolo fondamentale nella storia umana, influenzando l'esito di guerre, rivoluzioni e intrighi politici. Oggi, nell'era digitale, la sua importanza è cresciuta esponenzialmente, divenendo cruciale per la protezione dei dati personali, la sicurezza delle transazioni finanziarie e la tutela delle comunicazioni sensibili. Questo volume si propone di esplorare la ricca storia della crittografia e le sue implicazioni contemporanee attraverso una serie di saggi che spaziano dall'antichità ai giorni nostri.

Nel cuore del Rinascimento veneziano si consumò una disputa crittografica di notevole importanza, minuziosamente ricostruita da Paolo Bonavoglia. La contesa tra Franceschi e Partenio, due figure chiave della crittografia della Serenissima, non fu solo un confronto tra personalità, ma incarnò la tensione tra approcci innovativi e metodi tradizionali. Questo saggio ci trasporta nelle sale del potere della Repubblica di Venezia, rivelando come le questioni di sicurezza e segretezza fossero al centro delle preoccupazioni politiche dell'epoca. L'autore offre uno sguardo approfondito sulle tecniche crittografiche impiegate, illustrando come l'evoluzione di questi metodi riflettesse i cambiamenti politici e tecnologici del tempo.

Spostandoci ancora più indietro nel tempo, Marco Moraglio ci conduce alle origini della crittografia. La sua esplorazione delle prime tecniche di cifratura utilizzate nel mondo antico svela le ingegnose strategie adoperate per proteggere le comunicazioni. Dai messaggi nascosti degli antichi greci alle cifre utilizzate dagli imperatori romani, senza trascurare quanto accadesse nel Vicino Oriente, questo contributo getta luce sulle origini di un'arte che ha plasmato il corso della storia. Moraglio non si limita a descrivere le tecniche, ma le contestualizza all'interno delle società che le hanno prodotte, offrendo così una prospettiva più ampia sulla funzione della segretezza nelle civiltà antiche.

De Cifris Koine – Eruditorum ACTA 2024 https://doi.org/10.69091/koine/vol-3-I01

La crittografia non è solo una questione del passato, come dimostra l'intrigante caso di un'epigrafe cifrata nella Chiesa di Santa Maria la Nova a Napoli. Cosimo Palma affronta questo enigma, che ha resistito per secoli ai tentativi di decodifica e decrittazione, con un approccio innovativo. Affiancando tecniche avanzate di linguistica computazionale a un'attenta analisi storica, il saggio offre nuove prospettive su questo affascinante mistero, evidenziando come le moderne tecnologie possano gettare nuova luce sui segreti del passato ogni qualvolta si rimane attenti e rispettosi verso il relativo contesto socio-culturale. Il lavoro di Palma dimostra come la crittografia possa essere un ponte tra passato e presente, unendo metodi tradizionali e tecnologie all'avanguardia nella ricerca storica.

Nel contesto contemporaneo, è ineluttabile analizzare il ruolo della crittografia anche nella cybersicurezza nazionale. Marcello Albergoni presenta un'analisi approfondita del nuovo quadro giuridico italiano in materia, rivelando come questa antica arte sia diventata uno strumento fondamentale per la sicurezza informatica e l'autonomia strategica del paese. Il saggio esplora le complesse interazioni tra politica, tecnologia e sicurezza nazionale, delineando le sfide e le opportunità che si presentano nell'era digitale. Albergoni mette in luce come la legislazione debba costantemente adattarsi per stare al passo con i rapidi sviluppi tecnologici, sollevando importanti questioni sulla governance della sicurezza informatica.

Infine, il volume affronta una delle questioni più controverse legate alla crittografia moderna: l'introduzione di "backdoor" nei sistemi di cifratura. Antonino Alì, che è anche uno dei curatori di questo volume, esplora le profonde implicazioni sui diritti umani di tali pratiche, mettendo in luce l'acuta tensione tra le esigenze di sicurezza nazionale e la tutela della privacy individuale. Attraverso un'analisi giuridica e etica, il saggio solleva interrogativi cruciali sul futuro della privacy nell'era della sorveglianza digitale. Alì esamina casi giurisprudenziali recenti e dibattiti politici in corso, offrendo una panoramica dettagliata delle sfide etiche e legali che la società deve affrontare nel bilanciare sicurezza e libertà individuali.

Questa raccolta di saggi offre quindi una panoramica ricca e variegata sulla crittografia, evidenziandone la rilevanza storica, le applicazioni contemporanee e le sfide etiche e giuridiche che solleva. L'approccio interdisciplinare adottato riflette la natura poliedrica di una disciplina che continua a evolversi e a influenzare profondamente il nostro mondo digitalizzato, anche se il suo agire è spesso celato ai più. Ogni contributo, pur mantenendo la sua specificità, si inserisce in un dialogo più ampio sulla natura della segretezza, della sicurezza e della privacy nella società.

Ci auguriamo che questo volume possa non solo informare, ma anche stimolare ulteriori riflessioni e dibattiti sull'importanza della crittografia nel plasmare il nostro passato, presente e futuro digitale. In un'epoca in cui la protezione dei dati e la sicurezza delle comunicazioni sono diventate questioni di primaria importanza, comprendere la storia e le implicazioni della crittografia è essenziale per navigare le complesse sfide del mondo contemporaneo. Questo libro si propone come un punto di partenza per esplorare queste tematiche, invitando il lettore a considerare il ruolo cruciale che la crittografia ha giocato e continuerà a giocare nella nostra società.

Antonino Alì
Massimiliano Sala

Franceschi - Partenio, una disputa crittografica nel Rinascimento

Paolo Bonavoglia

De Cifris
paolo.l.bonavoglia@gmail.com

Sommario Recenti ricerche hanno portato alla luce una disputa fra Franceschi e Partenio, i due massimi compositori di cifre della Venezia cinquecentesca, il cui esito ebbe profonde conseguenze sull'evoluzione della crittografia della Repubblica di Venezia.

Keywords: Venezia · storia della crittografia · Rinascimento

Introduzione

La letteratura sulla crittografia veneziana è molto scarsa e per lo più basata su fonti secondarie. Tra i pochi testi basati su fonti primarie, in massima parte l'Archivio di Stato di Venezia[1], uno dei più grandi d'Europa, vanno citati l'opuscolo del 1872 di Luigi Pasini ([6] e la recente edizione [7]) l'archivista che a fine Ottocento riordinò il materiale crittografico dell'archivio veneziano, quello del 1902 di Aloys Meister [5, p.16] il più valido dal punto di vista crittografico, e nel 1994 il capitolo 13 del libro sui servizi segreti di Venezia di Paolo Preto [8], poco interessato alla tecnica crittografica ma ricchissimo di riferimenti ai materiali d'archivio. Ultimissimo un articolo di Ioanna Iordanou [3], anche questo centrato sull'*intelligence*.

Tale scarsità è per lo più attribuita alla difficoltà di raggiungere e soggiornare a lungo nel centro storico veneziano. Un problema che non sussiste per i residenti, come chi scrive, che dal febbraio 2018 sta conducendo una ricerca estesa sulla storia della crittografia veneziana. Superate le restrizioni del periodo della pandemia, è ripresa dal 2022, ed ha portato nuova luce su personaggi ed episodi dei quali si sapeva poco o nulla[2]. Questo articolo è dedicato a due personaggi e ad episodi dei quali finora si conoscevano a malapena nomi e cognomi.

De Cifris Koine – Eruditorum ACTA 2024 –https://doi.org/10.69091/koine/vol-3-E01

[1] In seguito abbreviato in ASVe; sito web: https://www.archiviodistatovenezia.it/it/

[2] Le risultanze di tale ricerca sono state pubblicate in [2].

CX - Il consiglio di dieci

Il Consiglio di Dieci (Cons^o di X o CX) era il tribunale della Serenissima Repubblica che si occupava della sicurezza, dello spionaggio e quindi anche della crittografia. Nominava, previa prova di ammissione, i segretari deputati alle cifre (*Ziffre*), incaricati di cifrare e decifrare i dispacci diplomatici e militari; alcuni poi progettavano cifre e decrittavano dispacci cifrati alieni intercettati.

Era formato di dieci membri effettivi eletti dal Maggior Consiglio, ai quali si aggiungevano di diritto il Doge e i sei consiglieri ducali, portando il totale a 17[3].

Crittografia e crittanalisi

Nel seguito userò spesso queste due parole, che per la verità sono molto posteriori al Cinquecento. Un esempio per chiarirne il significato:

- *Crittografia*: Alice deve inviare un messaggio segreto **M** a Bob; questo, usando una serie di regole segrete concordate con Bob e chiamate K (**cifrario** o **chiave**), trasforma M in una sequenza C di segni che appare caotica, priva di senso. Bob, disponendo di K, può decifrarla. Viceversa, una spia Eva che non conosce la chiave K non può decifrare C e nemmeno capire di cosa si tratta. Questa è l'arte di *scrivere in cifra* e di progettare metodi di cifratura sicuri.
- *Crittoanalisi*: Eva sa che la crittografia non è perfetta e passa il cifrato C a Bruno, un esperto crittanalista che, usando metodi matematici o statistici, riesce a **decrittare** C, cioè a recuperare il messaggio originale senza conoscere K.

Crittografia e crittoanalisi sono spesso descritte come una continua rincorsa tra chi progetta cifre più sicure e chi cerca il modo di forzarle.

Cifre mono-alfabetiche

Uno dei metodi di cifra più popolari consiste nel sostituire ogni lettera del testo da inviare, detto testo chiaro, con un segno cifrante che può essere un'altra lettera, un numero, un segno speciale, geometrico o di fantasia.

Il più semplice è quello di Cesare[4], descritto da Svetonio nelle *Vite dei 12 Cesari* [12], che consiste semplicemente nel sostituire ogni lettera del testo chiaro con quella che lo segue di tre posti nell'ordine alfabetico: è riassunto nella seguente tabellina.

lettera chiara	ABCDEFGHILMNOPQRSTVX
lettera cifrante	DEFGHILMNOPQRSTVXABC

[3] Come i posti ancora visibili nella sala di riunione all'interno del Palazzo Ducale. Gli scranni furono razziati dalle truppe francesi nel 1797.

[4] Non il più antico, che dovrebbe essere l'Atbash menzionato dalla Bibbia.

Svetonio non dice cosa sostituire alle ultime tre lettere **T V X**; di solito si intendono, come in un'aritmetica modulare, le prime tre lettere A B C.
L'alfabeto solitamente è spostato di 3 posizioni, ma in generale è possibile spostarlo di n posizioni. Qual è quindi il numero dei possibili cifrari di Cesare? Questi sono 20 usando l'alfabeto latino antico, uno per ogni possibile spostamento. Più correttamente, sono $20 - 1 = 19$, scartando il caso banale $n = 20$ dove il cifrato è uguale al testo chiaro. Insomma, bastano al massimo 19 tentativi per trovare quello giusto: il cifrario di Cesare è debolissimo. Molto meglio usare un alfabeto disordinato:

lettera chiara ABCDEFGHILMNOPQRSTVX
lettera cifrante HILOPQXABCMDERSTVFGN

infatti in questo caso gli alfabeti possibili sono

$$N = 20 \times 19 \times 18 \cdots = 20! = 2.432.902.008.176.640.000$$

Numero astronomico, quindi indecifrabile!?

L'analisi delle frequenze

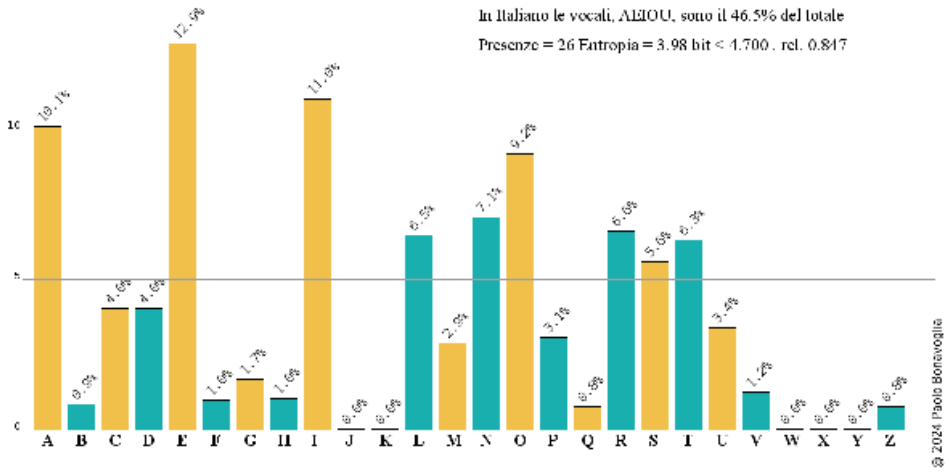
In effetti le cifre monoalfabetiche si possono forzare con l'analisi delle frequenze, una tecnica definita già dal matematico arabo Ibrahim Al Kindi[5], vissuto a Baghdad nel periodo aureo del Califfato, studiata intorno all'800 d.C. e riscoperta in Europa[6] verso il Trecento in alcuni stati italiani, forse anche alla Corte Imperiale del Sacro Romano Impero.

Possiamo costruire una sorta di "impronta digitale" della lingua facendo il conteggio delle singole lettere su un *corpus*, un insieme di testi di almeno 10000 lettere. Si otterrà un istogramma simile a quelli nelle figure 1c (italiano) e 1d (inglese). In generale, ogni testo avrà una distribuzione di frequenze simile a quella di un corpus nella stessa lingua.

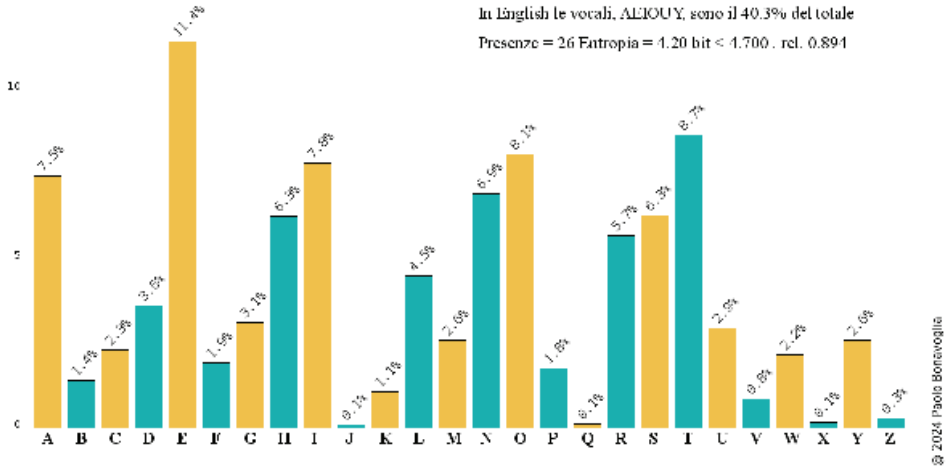
Beninteso, simile, non identica. Può capitare che in un testo italiano, tanto più se breve, la lettera più frequente sia la **A** o la **I** invece della **E**. Ma non capiterà mai che la lettera più frequente sia la **B** o la **V** o altre lettere rare, a meno che non si tratti di un testo artificiosamente messo insieme con questo scopo. Una frequenza molto più costante è quella della somma delle vocali, che in italiano anche per testi brevi non dovrebbe allontanarsi molto dal 46.5%, e in inglese dal 40%.

[5] Su Al Kindi e sulla crittografia araba riferimenti d'obbligo sono il Codebreakers di David Kahn [4] e l'articolo su Cryptologia [1]

[6] Non vi sono prove che i primi crittanalisti in Europa conoscessero l'opera d Al Kindi: questa è per ora solo un'ipotesi.



(c) Frequenze della lingua italiana.



(d) Frequenze della lingua inglese.

Figura 1: I diagrammi provengono dal mio sito `http://www.crittologia.eu`, pagina `http://www.crittologia.eu/critto/php/frequenze_lingua.phtml`

L'utilità di questi diagrammi per decrittare un testo cifrato per sostituzione (mono-alfabetica) è immediata: confrontando le frequenze ordinate del cifrato e della lingua presunta si può fare una prima buona ipotesi sulla sostituzione utilizzata, verificabile assegnando segni a lettere e poi scambiandole. Non sarà difficile ricuperare il testo originale dopo qualche tentativo.

Il nomenclatore

Le cifre monoalfabetiche sono ancor più vulnerabili quando sono visibili gli spazi che le separano, e spesso possono essere decrittate anche senza fare conti di frequenza, con regole empiriche come quelle di Cicco Simonetta[7]. Sono in buona parte utili solo se il cifrato è a parole disgiunte, e sfruttano per esempio il fatto che in italiano la lettera finale di quasi tutte le parole è una vocale, ecc. ecc.

Tra la fine del Trecento e l'inizio del Quattrocento compaiono i primi espedienti per rendere più sicure le cifre:

- Scrivere le parole tutte attaccate in modo che non se ne vedano l'inizio e la fine;
- usare qualche segno cifrante come *parola nulla*, nel senso che non significa nulla ed è solo un fattore di disturbo;
- usare segni cifranti diversi, detti *omofoni*, per la stessa lettera chiara soprattutto per le più frequenti, prime tra tutte le vocali; se distribuiti a caso possono spianare la distribuzione delle frequenze, confondendola;
- usare lo stesso segno cifrante, detto *polifono*, per lettere diverse; in questo modo la decifra non è più univoca e va fatta scegliendo la sola che abbia senso; può essere molto efficace ma va usato con molta accortezza;
- cifrare per gruppi di lettere, per esempio sillabe (*sillabari*), o parole intere (*dizionari*).

Soprattutto usando l'ultima regola, la stessa parola può cifarsi in diversi modi. Supponiamo di avere un dizionario per parole intere, un sillabario per sillabe ed un alfabeto per lettere singole.
Il dizionario prevede 173 per 'VENEZIANI', che è già la parola cifrata.
Il sillabario prevede: 735 per NI, 435 per VE, 341 per NE, 427 per ZI. L'alfabeto prevede 111 per A, quindi VENEZIANI diventa così: 435 341 427 111 735.
Ovviamente servirà accordarsi su quale metodo usare!

Un cifrario che comprende un po' di tutto, un alfabeto con o senza omofoni e nulle, un sillabario e un dizionario si chiama *nomenclatore* e occupa un foglio di carta o due, uno per cifrare, uno per decifrare. Quando richiede molti fogli o un libretto presero il nome di *codici*.

[7] Le regole sono riportate in latino nel libro del Meister [5] e tradotte in italiano da Luigi Sacco alla fine di [10]

Cifre polialfabetiche

Un'alternativa ai nomenclatori per rendere più sicure le cifre è quella delle cifre polialfabetiche, nelle quali si cifra ancora lettera per lettera, niente sillabari, niente dizionari, ma usando una parola segreta come chiave. La stessa lettera del testo chiaro può essere cifrata con cifre diverse a seconda della chiave, da questo il nome di *polialfabetiche*.

La prima cifra di questo tipo, pubblicata nel 1518, è la *tabula recta* (tavola quadrata) dell'abate Tritemio, mentre la prima ad usare una parola segreta come chiave è quella di G.B. Bellaso del 1553; la più nota è quella del de Vigenère del 1587, che unì le due precedenti nella cosiddetta *tavola di Vigenère*[8].

Più antica di tutte era quella descritta da Leon Battista Alberti alla fine del suo trattatello di cifre *De Cyfris* (o *De Cifris*), scritto tra il 1466 e il 1474 e pubblicato in una traduzione italiana solo nel 1578, che passò inosservata.

Figura 2: Il disco cifrante di Alberti nel De Cifris

Il *De Cifris* è noto soprattutto per il celebre disco cifrante descritto nel suo trattato, che può essere usato in almeno due modi[9]:

- **semplice**, ovvero monoalfabetico: si fissa il disco mobile in una posizione concordata come quella in figura 2; la **A** si cifra con *m*, la **L** con c, e quindi **ALBERTI** si cifra con *mcokpgh*;
- **difficile** ,ovvero polialfabetico: si ruota di tanto in tanto il disco interno, quindi cambiando alfabeto; occorre ovviamente segnalare il cambio, per esempio scrivendo in maiuscolo la lettera che sta ora sotto la convenuta A.

[8] Maggiori dettagli su de Vigenère in [11]

[9] Per maggiori dettagli sul funzionamento vedi `http://www.crittologia.eu/critto/alberti.phtml`.

Le cifre polialfabetiche non furono in verità quasi mai usate dalle cancellerie europee, perché come osservava Agostino Amadi nel suo trattato, i principi badano al sodo e non è accettabile che un segno cifrante possa stare per diverse lettere chiare, infatti basta che il segretario salti una lettera della chiave e tutto il resto del cifrato diventa indecifrabile. Inoltre l'uso di queste cifre è molto più lento dei nomenclatori.

L. B. Alberti, padre della crittanalisi?

Si legge spesso che l'opera di Alberti rimase sconosciuta per secoli e che non ebbe alcuna influenza sulla storia della crittografia. Ma esistevano diversi manoscritti all'epoca, e lui stesso aveva raccomandato che fossero letti solo da principi e da professionisti nella materia.

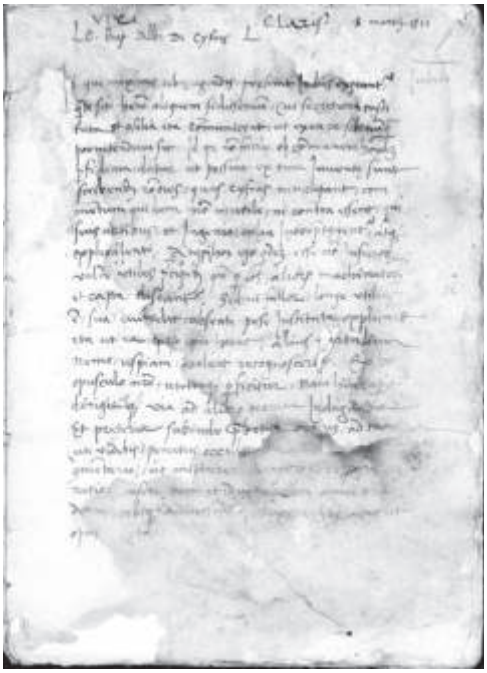


Figura 3: Prima pagina del De Cyfris custodito all'Archivio di Stato di Venezia; file *Consiglio-di-Dieci-Chiavi-di-Cifra-b-041-n-01_ 0001_ 001-r.jpg*.

Prima di parlare del suo disco, Alberti scrive una lunga analisi delle caratteristiche delle lingue latina e italiana, a partire dalle frequenze delle varie lettere e

dei gruppi di lettere, come strumento utile a decrittare cifre alfabetiche. Questa introduzione è per lo più ignorata dai tanti autori che hanno trattato del Decifris, con almeno due importanti eccezioni: David Kahn nel suo *Codebreakers*, e prima di lui Luigi Sacco, che era un crittanalista, nel suo opuscolo *Un primato italiano: la Crittografia nei secoli XV e XVI* [10] e nella terza edizione del suo *Manuale di Crittografia* [9].

Ma ora dalle ricerche negli archivi veneziani risulta che il *De Cifris* era ben noto a Giovanni Soro e ai suoi successori a Venezia, dove disponevano di una copia. Nei numerosi trattati sulle cifre presenti in archivio, Alberti viene spesso menzionato, in particolare in un trattatello anonimo che dice che Alberti fu il primo a "scrivere in modo confuso dell'arte del levar le cifre" [10] e in una lettera di Alvise Borghi (altro grande crittanalista).

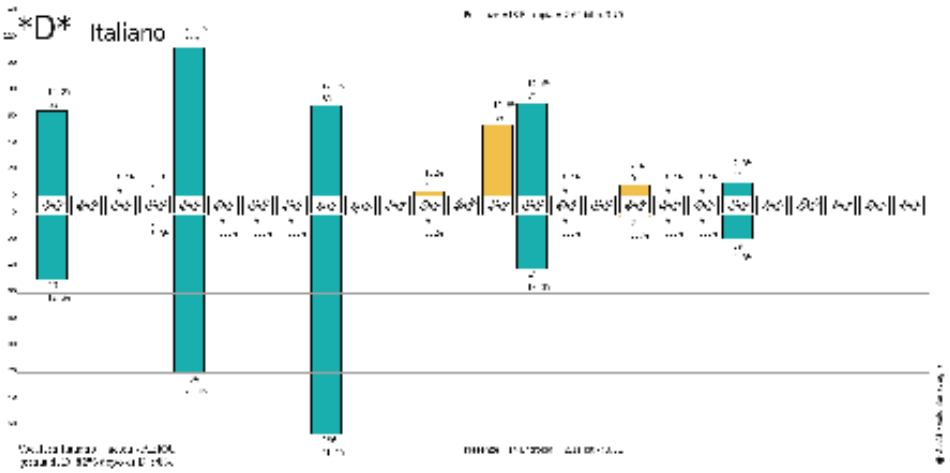
Il "modo confuso dell'arte del levar le cifre"? In effetti Alberti non usa numeri, tabelle o diagrammi, ma le idee generali sono abbastanza chiare. Nelle pagine introduttive, troviamo un'analisi delle varie lettere dell'alfabeto, della loro frequenza e della frequenza delle lettere vicine, che equivale a un'analisi delle frequenze dei digrammi, ma nessun dato numerico, nessuna tabella, nessun diagramma dei dati. E nei trattati veneziani troviamo dati espressi in forma relativa, per esempio 23 su 200 (non c'era il segno di percentuale), tabelle, schemi e diagrammi delle frequenze.

Digrammi, trigrammi n-grammi

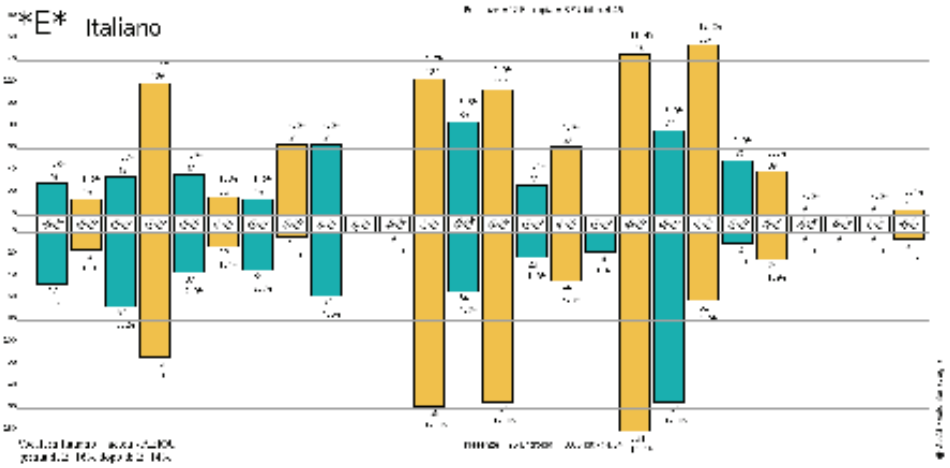
Non si trovano però in questi trattati diagrammi di frequenza dei digrammi, solo tabelle descrittive lettera per lettera; oggi la cosa si può fare facilmente ed è utile per capirne visivamente l'importanza.

L'analisi delle frequenze dei digrammi è uno strumento ancora più potente di quello delle singole lettere, infatti come appare evidente dai due diagrammi, quello della E in figura 4b e quello della D in figura 4a, c'è una significativa differenza tra vocali e consonanti. Le vocali sono socievoli, vanno d'accordo con tutte, molto meno le consonanti; la **D** è un caso estremo, va d'accordo solo con le vocali e con **L**, **N**, **R** che sono le consonanti più socievoli, più di tutte la **R** che alcuni considerano una semiconsonante.
Senza entrare in dettagli, è intuibile che questi digrammi ci permettono di valutare quanto sia buona una data ipotesi, ancor meglio se si considerano gli n-grammi con $n = 3, 4 \ldots$ Il metodo permette di forzare anche le cifre con omofoni, ed era probabilmente questa l'arma segreta dei veneziani dopo il 1510, quando si vantavano di essere capaci di forzare qualsiasi cifra allora in uso.

[10] Appare curioso il fatto che questi trattati non spendano una sola parola sul disco cifrante, nonostante qualche disco in cartoncino sia presente in archivio. Curioso ma coerente con quanto diceva Amadi in proposito.



(a) Frequenze della lingua italiana.



(b) Frequenze dei digrammi con la lettera E, in italiano; come ogni vocale è molto socievole, va d'accordo con tutte.

Figura 4: Frequenze dei digrammi delle due lettere D ed E nella lingua italiana.

1572 - Franceschi entra in scena

Hieronimo di Franceschi[11] (Venezia, 1540-1600), segretario della Cancelleria Ducale e poi del Senato, fu il grande sostenitore del cifrario polialfabetico che chiamava *ziffra uera* e accanito avversario dei vecchi cifrari, i nomenclatori, dove ogni segno ha una decifratura unica ed è quindi in teoria *trazibile*, decrittabile[12]. Franceschi argomentava che se Venezia disponeva di professionisti capaci di decrittare ogni cifra era verosimile che anche gli altri principi ne disponessero, da qui la necessità di adottare nuove cifre più sicure.

Nel settembre 1572 Franceschi presentò al CX una *cifra vera* a suo dire assolutamente sicura, che fu approvata un anno dopo. Nell'archivio veneziano si trovano diversi esempi di questa cifra che permettono di ricostruirne in dettaglio il funzionamento; la cifra detta del *falso scontro* consisteva nel convertire ogni lettera del testo chiaro in un numero di due cifre, e sommarvi ordinatamente i numeri di una chiave consistente di una sequenza di numeri casuali lunga come il messaggio; per decifrare si farà la sottrazione invece dell'addizione.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
4	16	14	10	1	17	15	18	2	11	13	6	3	12	19	7	9	8	5	20

Chiaramente si tratta di una cifra polialfabetica. In sostanza un Vernam *ante litteram*, che però fu poco apprezzato da Gianfrancesco Marin, grande crittanalista veneziano che la considerava lenta e macchinosa.

La cifra delle caselle

Nel 1577 entra in uso la *cifra delle caselle*, revisione della precedente, probabile frutto di un compromesso con il Marin. Le principali novità erano:

1. per cifrare si sottrae la chiave dalla cifra, per decifrare si somma;
2. la cifra piccola ha due omofoni per ogni lettera nell'intervallo $1 \ldots 39$, che differiscono sempre di 20: ad esempio la **A** si cifra con 16 o 36 e solo la **H** ha un unico omofono, 20;
3. la cifra piccola ha ora, oltre all'alfabeto con cifre tra 0 e 39, un piccolo dizionario di 60 parole con cifre comprese tra 40 e 99;

[11] Nelle sue numerose lettere e suppliche al CX si presenta sempre così: *"Io, Hieronimo di Franeschi ... "*. Solo nel 1599, il suo ultimo anno, appare la forma italianizzata *"Io, Girolamo di Franceschi ... "*. Ho preferito mantenere la forma da lui usata.

[12] Questo, che per Amadi era un pregio, diventa un grave difetto per Franceschi!

4. la chiave è ora una sequenza di numeri casuali compresi tra 0 e 19 e scritti su una grata, foglio di carta spessa con finestrelle (o caselle), con tre numeri della chiave scritti sopra; vi sono 26 righe di 8 colonne ciascuna per un totale di $3 \times 26 \times 8 = 624$ numeri.

All'occhio del matematico risulta evidente che si tratta di un'aritmetica modulo 20 realizzata alla buona; i segretari sceglieranno tra i due omofoni quello che evita di andare sottozero. Il dizionario poi aggiunge ben poco alla sicurezza della cifra, che poggia sulla casualità della chiave sulla grata e sulla sua rigorosa custodia. Considerata l'avversione del Franceschi per i nomenclatori, potrebbe trattarsi di una concessione al Marin.

Erano previste solo quattro grate per le più importanti ambasciate veneziane: 1) la grata presso l'imperatore a Vienna o Praga, denominata *Germania*, in figura 5; 2) presso il re di Francia a Parigi e il duca di Savoia a Torino; 3) presso il re di Spagna a Madrid; 4) presso il sultano a Costantinopoli. Altre si trovavano presso le diverse isole sotto amministrazione veneziana.

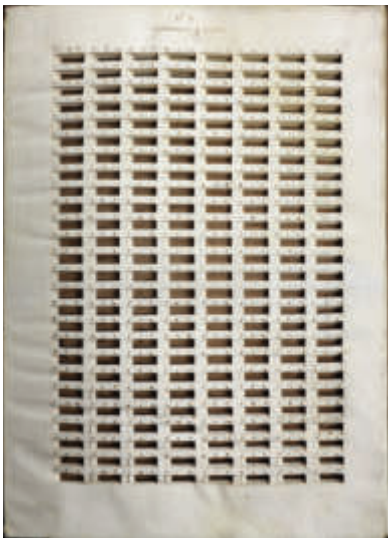


Figura 5: La grata "Germania" usata come chiave per le comunicazioni con l'imperatore. *ASVe CX Cifre, chiavi e scontri di cifra. busta 4, fasc.8, c.1.*

La cifra piccola per convertir lettere in numeri è questa:

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
16	13	1	15	2	24	19	20	28	14	27	17	18	10	29	12	25	11	23	26
36	33	21	35	22	4	39		8	34	7	37	38	30	9	32	5	31	3	6

Vediamo ora come cifrare un messaggio con le caselle, e prendiamo la prima riga di quello di Sigismondo Cavalli ambasciatore presso l'imperatore a Vienna, del 9 novembre 1577, che così cominciava:

«Da buona parte intendo che lo Imperatore scrisse sabato una lettera di sua mano al arciduca Matias sopra doi ponti principali [..]. »

Per cifrare questo testo il segretario a Vienna pone un foglio bianco sotto la grata, legge la prima lettera del messaggio, che è **D** e che ha per cifra 15; sottrae il numero della grata sopra la casella, 2, ottenendo $15 - 2 = 13$ e scrive 13 nella casella; poi cifra la seconda lettera **a** ottenendo $16 - 8 = 8$, e così via, ricordando che stiamo operando in un'aritmetica modulare con modulo 20.

d	a	b	u	o	n	a	p	a	r	t	e	i	n	t	e	n	d	o	che	l	o	Imp.re	s
15 -	16 -	13 -	23 -	18 -	17 -	16 -	10 -	16 -	12 -	11 -	2 -	28 -	17 -	11 -	2 -	17 -	15 -	18 -	69 -	14 -	18 -	87 -	25 -
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
13	8	10	21	12	7	16	7	9	8	10	12	26	10	6	0	13	14	15	62	12	14	86	17

Una volta rimossa la grata, il dispaccio cifrato è pronto ad essere spedito a Venezia, dove il segretario addetto alla decifra pone il cifrato appena ricevuto sotto la grata, a registro, e ora deve solo sommare il numero soprastante per ricuperare il testo chiaro come schematizzato nella seguente tabella:

13+	8+	10+	1+	12+	7+	16+	7+	9+	8+	10+	12+	6+	10+	6+	0+	13+	14+	15+	62+	12+	14+	86+	17+
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
15	16	13	3	18	17	16	10	16	12	11	22	8	17	11	2	17	15	18	69	14	18	87	25
d	a	b	u	o	n	a	p	a	r	t	e	i	n	t	e	n	d	o	che	l	o	imperatore	s

La cifra delle caselle rimase in uso per più di un decennio, ma scontrandosi continuamente con la scarsa simpatia dei segretari, sempre più infastiditi dal dover fare tanti calcoli per cifrare. Negli anni Ottanta di quel secolo si trovano molte lamentele in proposito, e di converso abbiamo le lettere del Franceschi che lamentava lo scarso uso che si faceva della sua cifra: solo in Francia e in Savoia veniva usata regolarmente.

In questo clima sembra inserirsi a pennello l'entrata in scena di Pietro Partenio.

1590 - Il notaio Pietro Partenio

Pietro Partenio (1538-1620) era titolare di un affermato studio notarile, più volte membro del collegio notarile di Venezia, dilettante di cifre, che nel 1590, a 52 anni si presentò al CX con una lunga lettera, nella quale proponeva nuove cifre, per lo più nomenclatori. Nel 1593 furono approvate dal CX che le raccolse in un elegante codice pergamenaceo, tutt'ora a disposizione degli studiosi dell'archivio veneziano[13], e garantì al Partenio un vitalizio.

Nonostante tutto, queste cifre non entrarono subito in uso ed il Franceschi non gradiva la concorrenza di un dilettante; il conflitto tra i due, oltre che uno scontro tra caratteri, era soprattutto uno scontro tra due concezioni diverse della crittografia, tra il nomenclatore e il polialfabetico.

La cifra 5 del Partenio: un nomenclatore sovracifrato

L'occasione per adottare una cifra del Partenio si presentò nel 1595, quando Giovanni Mocenigo, tornato da Parigi dove era ambasciatore presso Enrico IV, riferì al CX un fatto inquietante[14]: che anni prima a Tours, dove aveva la sua sede alla fine delle guerre di religione, era andato da lui monsieur Viete[15], persona molto intendente di cifre, che gli offrì una serie di lettere del re di Spagna per Venezia, da lui decrittate e piuttosto allarmanti. Mocenigo aveva allora chiesto a Viète se fosse capace di decrittare anche le cifre veneziane, e avuta una risposta vagamente positiva, alla domanda «ma anche quella delle caselle?» aveva risposto con un enigmatico «In quella bisogna far salti». Viète aveva poi promesso prove di tutto questo, ma non si era più fatto vedere. Nonostante la vaghezza di queste vanterie del Viète, nel dubbio il CX decise di sospendere immediatamente la cifra delle caselle come cifra di massima sicurezza e di sostituirla con la cifra 5 del Partenio, subito inviata al nuovo ambasciatore in Francia, Pietro Duodo. Il provvedimento non ebbe in realtà molto peso; il Duodo la usò in tre dispacci soltanto tra luglio e agosto 1595, poi non se ne trova più traccia nei dispacci da Parigi, che continuano a usare il nomenclatore. Verosimilmente il segretario non aveva gradito...

Lo scontro di cifra effettivamente usato, in figura 6, era una versione ridotta del nomenclatore del 1593, con il numero di cifre ridotto da 1000 a 500. La novità di questa cifra, rispetto ai nomenclatori allora in uso, stava nella presenza di un sistema di **sovracifratura**, tecnica che sarebbe divenuta di uso comune solo nel XIX secolo, allo scopo di garantire la sicurezza delle comunicazioni, anche nel caso lo scontro di cifra fosse caduto in mano al nemico, evento non infrequente nella storia delle cifre. La tabellina di sovracifra usata dall'ambasciata in Francia è la seguente:

[13] *ASVe CCX Raccordi n.1*
[14] Si trova in *ASVe CX Deliberazioni segrete f. 27 c. 174*
[15] Francois Viète, matematico e notissimo algebrista, fu anche un valente crittanalista

Figura 6: La cifra 5 del Partenio nella versione 1595. *ASVe CX Cifre, chiavi e scontri di cifra. busta 2, fasc,23*

0	1	2	3	4	5	6	7	8	9
p	c	e	u	f	s	z	m	i	q
h	t	r	b	l	d	a	n	o	g

Il segretario trova la cifra nel nomenclatore, per esempio quella della parola 'SIGNOR' è 489; ognuna delle cifre decimali va ora sostituita da una lettera scelta tra le due sottostanti nella tabellina; quindi 4 può sostituirsi con f o l, 8 con i oppure o, 9 con q o g. Ovviamente il nemico venuto in possesso del nomenclatore non potrà decifrare alcun messaggio, non conoscendo la tabellina di sovracifra.

Estate 1596 - Franceschi forza la cifra 5

Franceschi non aveva digerito la sostituzione della sua cifra con quella del Partenio; si mise alla ricerca di un punto debole, e nel luglio del 1596 si presentò a ìl CX sostenendo che il Partenio sbagliava quando affermava che la cifra n.5 era indecifrabile anche da chi fosse in possesso del nomenclatore. Per dimostrarlo lanciò una sfida chiedendo che il CX nominasse un segretario che (usando una diversa tabellina) cifrasse un breve testo e glielo consegnasse; Franceschi lo avrebbe decifrato in pochi giorni. Così fece, come riferisce la delibera del CX che è riportata tal quale qui sotto:

«[. . .] uenne il Franceschi pochi giorni da poi insieme col fed[elissi]mo Piero Amai[16]. giouene deputato alle zifre, et allieuo di esso Franceschi, et presentò scritto il senso della zifra data cauata il qual senso confrontato col primo originale si trouò esser l'istesso di parola in parola.»

Il Comino aveva usato questa chiave

0	1	2	3	4	5	6	7	8	9
e	d	b	o	s	l	t	f	h	g
n	m	z	p	a	r	c	u	q	i

per produrre il cifrato che, accanto alla soluzione di Franceschi e Amai, è mostrato in figura 7.

Figura 7: Il cifrato prodotto dal Comino e la chiave e il testo decrittato da Franceschi e Amai. *ASVe CX Cifre, chiavi e scontri di cifra. Busta 6 misc. Fasc. Franceschi*

[16] Si tratta del figlio di Agostino Amadi autore del più noto trattato alle cifre veneziano. Il Cognome varia spesso da Amadi a Amai, problema frequenti in tempi nei quali i documenti erano [quasi] sempre scritti a amano

Il CX convocò d'urgenza il Partenio per dire le sue ragioni in proposito. Secondo quanto si legge nelle carte d'archivio la sua difesa apparve debole e confusa, basandosi solo sul fatto che la sua cifra 5 originale del 1593, era stata dimezzata da mille a cinquecento segni cifranti. Poco convinto da questa difesa, che peraltro confermava che la cifra adottata era *trazibile*, inviò immediatamente un dispaccio al bailo di Costantinopoli invitandolo a non usare più la cifra del Partenio, ma a usare piuttosto per le comunicazioni più riservate la cifra delle caselle.

Settembre 1596 – virulenta reazione del Partenio

Pochi giorni dopo arriva la reazione del Partenio, una lunghissima lettera, nella quale sostiene che lui per avvertimento intendeva non solo la tabellina ma anche le istruzioni d'uso della medesima, che il Comino non conosceva bene la cifra e aggiunge:

«[...] che la proua da loro et tra loro fatta è nulla et un ordimento fabricato dal sudo Franc^{i} per leuarmi l'honore, la riputatione et la gratia del mio Principe [...]» Partenio conclude riconoscendo che la cifra delle caselle è fortissima, ma sottoposta al rischio del furto e finiva paragonandola, per il fatto di cifrare lettera per lettera, alla cifra del Tritemio vecchia ormai di 90 anni. Letta questa lettera il CX si spaccò in due opposte fazioni, e come già fatto in passato decise di affidarsi a una commissione di 5 nobili. Furono eletti:

- Leonardo Donà, il futuro doge protagonista di un famoso scontro con il papato e patrocinatore di Galileo e del suo cannocchiale.
- Giacomo Foscarini
- Niccolò Gussoni
- Paolo Peruta
- Giacomo Soranzo

La commissione se la prese comoda tanto che dopo 18 mesi, nel febbraio 1598 (1597 more veneto), il CX prese atto che la delibera del 16 set 1596 non era stata eseguita, sollecitando i cinque a concludere qualcosa al più presto.

La sfida finale tra Franceschi e Partenio finisce nel nulla

Recentissimo è il ritrovamento di due minute della relazione finale della commissione, dalla quale si apprende che per concludere i lavori aveva deciso di organizzare una prova per confrontare le due cifre in termini di sicurezza, velocità e facilità d'uso; dovevano partecipare in persona Partenio e Franceschi e due aiutanti di loro fiducia, Pinardo e Pietro Amai. Una breve descrizione su quella prova la troviamo alla fine della relazione, riportata tal quale nell'ortografia dell'epoca:

> «[...] ma quando si uenne all'atto della proua, l'Amai si escusò di non uoler uenir a questa concorrenza, atteso che la casella gli era stata diuersificata in modo che non sapendo lui ben summare et sottrarre non gli bastaua l'animo di scriuerla per quel tramite, Onde non perdere l'occasione si continuerà con il Franceschi, che è il principale scriuesse lui la sua propria, et il Pinardi che è lo alieuo scriuesse quella del Parthenio, così essendosene contentato esso Pinardti, e hauendo dato a tutte doi le parti l'istessa cosa da scriuere, trouiamo per esperienza di molta [importantia?], et che pregiudicheria troppo al publico seruitio che per le difficoltà della ziffra douessero trattenersi lungamente, non essendo alcuno che non conosca quanto [giudi..uoli] la [lentezza] o la perdita di un auiso; et però quanto alla facilità diremo che quella del [Franceschi] adoperarsi più facilmente dell'altra, Eseguendo noi sottoscritti la commissione [...].»

1600 - Exit Franceschi

Ma la relazione dei 5 nobili non fu mai consegnata. Motivo più probabile la morte del Franceschi, che dovette avvenire nella prima metà del 1600 dato che nel giugno 1600 il CX deliberò una sanatoria dei debiti che i due nipoti avevano ereditato dal nonno. Per parte sua Partenio scompare per cinque anni, per tornare in scena all'inizio del 1606 quando dona al CX altre 5 cifre e si offre di tenere un corso per giovani aspiranti cifristi, tra i quali il giovanissimo Ottavian Medici, che considera quasi come suo figliolo (Partenio era scapolo e non aveva figli).

1621 - Un'altra commissione di nobili liquida elegantemente Partenio

Dalla relazione finale, aprile 1621, dei tre nobili incaricati dal CX nel 1619 di riformare le cifre veneziane leggiamo:

> «[...] Più uolte siamo stati insieme con essaminatione dili[gentissi]ma sopra una gran uarietà de scontri, che ci sono stati presentati et dalli secretari ziffristi e dal già Pietro Parthenio peritissimo in tal professione; di questo soggetto potemo con la [nostra?] solita sincerità dire a Vostra Serenità di hauer ueduto, mentre egli uiueua inuentioni molto spiritose, di pari sicurtà, et degne di comendatione ma bilanciati questi requisiti con qualche difficoltà nel uso et tardità nel trazer et scriuer, quando alla giornata occorre che che quasi a tempi presenti risorge la multiplicità da ogni parte habbiamo giudicato per queste sole cause di non poter determinare la loro essercitatione.»

Pietro Partenio peraltro era già morto nel 1620, alla bella età di 82 anni.

1621 - Ottavian Medici seppellisce Franceschi e Partenio

Alla fine la commissione dei tre nobili approvò come nuova cifra corrente quella di Ottavian Medici e G.B. Lionello, con la quale vengono definitivamente abbandonati sia i cifrari polilalfabetici di Franceschi sia i nomenclatori sovracifrati del Partenio. Medici puntò su un nomenclatore semplice con segni di 3 cifre decimali, rinforzati dalla raccomandazione di scriverle tutte di seguito e con un gran numero di nulle, come si può osservare nel seguente estratto dal cifrario completo, troppo vasto per essere riportato per intero.

Alfabeto

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
156	157	158	159	256	175	258	259	356	357	176	276	376	457	458	177	277	377	477	559
174	274	374	474	574	257	275	375	475	575	358	359	456	476	576	459	556	557	558	577

Nulle

86	87	88	89	96	97	98	99	100	101	102	103	104	105	106	114	123	132	141	150	180
214	223	232	241	250	314	323	332	341	350	414	423	432	441	450	514	523	532	541	550	

Sillabario

ba	be	bi	bo	bu	bra	bre	bri	bro	bru	ca	ce	ci	co	cu	cra	cre	cri	cro	cru	da	de	di	do	du
115	116	117	118	119	215	216	217	218	219	315	316	317	318	319	415	416	417	418	419	515	516	517	518	519
dra	dre	dri	dro	dru	fa	fe	fi	fo	fu	fra	fre	fri	fro	fru	ga	ge	gi	go	gu	gna	gne	gni	gno	gnu
124	125	126	127	128	224	225	226	227	228	324	325	326	327	328	424	425	426	427	428	524	525	526	527	528

. . . e così via fino a za ze zi zo zu

Il cifrario appare già a prima vista un po' troppo regolare per essere sicuro, ma in mancanza di documentazioni è impossibile dire se sia stato forzato dalle "camere nere" (*black chamber*) che andavano formandosi a Vienna, Parigi, Londra. . . Dal punto di vista dei segretari addetti alla cifra fu invece un successo: la scrittura continua incontrò qualche difficoltà ma divenne la norma, e così l'uso del sillabario come cifra di base; molto meno le nulle, ancora una volta ignorate quasi del tutto.

Medici rimase alla guida del servizio cifra fino alla metà del secolo, quando si ritirò avendo ottenuto la nobiltà per la sua famiglia, unico *cifrista* ad aver ottenuto un tale onore. La fortuna delle sue cifre gli sopravvisse a lungo, in pratica fino alla caduta delle Repubblica nel 1797. Le sue cifre furono riciclate tali e quali, come quella del 1621, che ricompare nei dispacci diplomatici verso il 1680, oppure con piccole modifiche come quella del 1630 che riappare un secolo dopo con le cifre semplicemente incrementate di 10. Una cifra del 1714 che resta in uso per mezzo secolo: la decadenza della crittografia veneziana non potrebbe essere meglio esemplificata.

Conclusioni

Franceschi e Partenio furono due geniali progettisti di cifre probabilmente troppo in anticipo sui tempi: si intende anche che erano troppo complicate e lente da usare. La cifra delle caselle restò in uso per diversi anni, ma per parti sempre più limitate; scarsa fortuna, ma comunque sempre meglio della cifra 5 del Partenio abbandonata nel giro di due settimane.

Ebbe invece fortuna la controriforma del Medici con la sua cifra che, come abbiamo appena visto, seppure ingegnosa nel tentativo di rinforzare i nomenclatori senza usare sovracifre o polialfabetiche, degenerò per un secolo e mezzo in una sorta di copia e incolla delle sue cifre, più nessun segno di inventiva o di innovazione... In definitiva, questa disputa tra Franceschi e Partenio aveva portato a una duplice sconfitta e all'inizio della decadenza della crittografia veneziana.

Resterebbero due questioni aperte: "Era fondato il timore di entrambi che i nomenclatori veneziani fossero decrittati nelle varie capitali europee?", "E lo era anche per le cifre del Medici?"...

Nota riproduzione documenti d'archivio
L'uso di fotoriproduzioni di documenti conservati dall'Archivio di Stato di Venezia è stato concesso con suo Nulla Osta dal protocollo `ASVe 3269/2024`.

Riferimenti bibliografici

1. Ibrahim A. Al-Kadit. Origins Of Cryptology: The Arab Contributions. *Cryptologia*, 16(2):97–126, 1992.
2. Paolo Bonavoglia. *La crittografia della Repubblica di Venezia*. Crittografia. Aracne, Roma, 2023.
3. Ioanna Iordanou. *Venice's secret service*. Oxford University Press, Oxford, 2019.
4. David Kahn. *The codebreakers; The Story of Secret Writing*. Scribner, New York, 1996. 10th Printing.
5. Aloys Meister. *Die Anfänge der modernen diplomatischen Geheimschrift*. Ferdinand Schöningh, Paderbord, 1902.
6. Luigi Pasini. *Delle scritture in cifra usate nella Repubblica di Venezia*. Tipografia Naratovich, Venezia, 1872.
7. Luigi Pasini. Delle scritture in cifra usate nella Repubblica di Venezia (1872). In Paolo Bonavoglia, editor, *Crittografia*. Aracne, Roma, 2019.
8. Paolo Preto. *I servizi segreti di Venezia*. Edizioni EST, Milano, 1999.
9. Luigi Sacco. *Manuale di Crittografia, III edizione*. Ist. Poligrafico dello Stato, Roma, 1947.
10. Luigi Sacco. *Un primato italiano: la Crittografia nei secoli XV e XVI*. Istituto Storico e di Cultura dell'Arma del Genio, Roma, 1958.
11. Maurice Sarazin. *Blaise de Vigenère, Bourbonnais: introduction à la vie et à l'œuvre d'un écrivain de la Renaissance*. Editions des Cahiers Bourbonnais, 1997.
12. Caius Suetonius Tranquillus. *Suetonius Collectio. De vita Caesarum (Latin Edition)*. Independently published, 2020.

Scrivere per nascondere, leggere per scoprire. Le origini della crittografia

Marco Moraglio

Università degli Studi dell'Insubria
marcomoraglio92@gmail.com

Sommario L'obiettivo di questo intervento è quello di analizzare la nascita della crittografia per poi indagare i principali sistemi utilizzati nel mondo classico. Infine, ci concentreremo su un argomento poco noto carico di mistero, sviluppandolo sempre da un punto di vista prettamente storico

Keywords: Storia della crittografia.

Da sempre l'uomo ha avuto la necessità di comunicare. Con il progredire e l'ampliarsi delle società è notevolmente aumentato anche lo scambio comunicativo trovandosi così di fronte alla crescente necessità di sicurezza. Ben presto, quindi, le informazioni non dovevano più essere solo distribuite ma diventava anche fondamentale che potenziali nemici non fossero in grado di comprendere il significato del messaggio. Da queste esigenze sono nate la steganografia, la crittografia e, di conseguenza, la crittoanalisi. In particolare, tra queste ultime c'è stato, fin da subito, un vero e proprio conflitto che si protrae fino ai giorni nostri: da una parte, infatti, i crittografi cercano di realizzare un cifrario che sia invincibile mentre, dall'altra, i crittanalisti si trovano davanti al difficile compito di provare a rompere i diversi sistemi di cifratura.

L'obiettivo di questo lavoro è quello di ripercorrere gli esordi della storia della crittografia andandosi a concentrare in particolar modo sugli eventi principali che hanno caratterizzato questo percorso fino alla caduta dell'Impero Romano d'Occidente. Questo breve articolo è diviso in tre sezioni:

- Gli esordi: *intelligence* e crittografia nell'Antico Vicino Oriente
- Il mondo greco
- Il mondo romano

De Cifris Koine – Eruditorum ACTA 2024 –https://doi.org/10.69091/koine/vol-3-E02

Intelligence e crittografia nell'Antico Vicino Oriente

Volendo cercare l'antenata più stretta della crittografia dobbiamo senza dubbio andare a studiare l'attività di spionaggio. Quest'ultima, intendendo il lavoro dei servizi segreti anche come semplice ricerca e selezione delle informazioni, ha origini antichissime. I vari potentati che nacquero nella cosiddetta *mezzaluna fertile* all'alba della storia, infatti, molto spesso erano impegnati in una serie di guerre. Il compito delle prime spie, quindi, era quello di ricercare e riportare informazioni inerenti le condizioni sociali, economiche e politiche del nemico che si voleva combattere.

Domenico Vecchioni[1] affermava che *"gli imperi che hanno perfezionato i propri servizi segreti sono durati più a lungo degli altri"* e la storia dei primi israeliti sembra confermare la sua asserzione. L'Antico Testamento[2] è infatti ricchissimo di episodi nei quali emerge una vera attività spionistica e, addirittura, l'utilizzo di un codice cifrato. Seguendo cronologicamente la trattazione testamentaria il primo esempio di utilizzo di intelligence lo incontriamo quando Mosè manda la sua squadra a cercare informazioni sulla Terra Promessa, dimostrandosi un abile leader militare oltre che una ottima guida politica.

> Mosè dunque li mandò ad esplorare il paese di Canaan e disse loro: «Salite attraverso il Negheb; poi salirete alla regione montana ed osserverete che paese sia, che popolo l'abiti, se forte o debole, se poco o molto numeroso; come sia la regione che esso abita, se buona o cattiva, e come siano le città dove abita, se siano accampamenti o luoghi fortificati; come sia il terreno, se fertile o sterile, se vi siano alberi o no. Siate coraggiosi e portate frutti del paese.[3]

Sicuramente si tratta di uno spionaggio estremamente particolare nel quale le capacità tecniche tipiche di un buon agente segreto sono subordinate a una necessità valutativa del territorio. La figura della spia emerge anche in altri passi del testo biblico; uno dei più celebri riguarda la conquista di Gerico. Si racconta infatti di Raab, una locandiera della città, che si trova ad ospitare due spie inviate da Giosuè il quale aveva l'obiettivo di completare la conquista della Terra Promessa; per raggiungere lo scopo, quest'ultimo, aveva inviato due agenti al fine di reperire il maggior numero possibile di informazioni. La notizia, però, era arrivata anche al re di Gerico che aveva ordinato a Raab di allontanare i due uomini. La donna si dimostrò tuttavia un'ottima doppiogiochista riuscendo a mandare "fuori strada" i soldati del re di Gerico e proteggendo così le spie di Giosuè.

[1] Diplomatico e scrittore italiano.

[2] Per tutto l'articolo, a meno che non sia diversamente indicato, per le citazioni bibliche si farà riferimento a *La Sacra Bibbia*, versione ufficiale CEI, edizione a cura della Unione Editori e Librai Cattolici Italiani (UELCI), Cooperativa Promozione Culturale, Roma 2004 [2].

[3] [2], Nm 13, 17-20.

Per la storia della crittografia, comunque, l'Antico Testamento non è importante solo per i racconti dei primi agenti segreti, ma soprattutto perché troviamo l'applicazione del primo codice monoalfabetico mai utilizzato: il *cifrario Atbash*. I codici monoalfabetici sono cifrari a sostituzione molto semplici ma che sono stati efficaci fino al "calcolo delle frequenze" di Al-Kindi nel IX secolo[4]. Sempre nell'Antico Testamento e, più precisamente nel libro di Geremia, leggiamo:
«Il re di **Sesach** berrà dopo di essi».
La parola **Sesach** è un termine crittato, il vero nome della città è infatti nascosto.

I codici monoalfabetici prevedono la sostituzione di ogni lettera con un altro carattere secondo una tabella prestabilita. In particolare, il cifrario Atbash nasconde la prima lettera con l'ultima, la seconda con la penultima e così via. Il nome stesso del sistema crittografico deriva dalla sua attuazione. "Atbash", infatti, è composto dalla prima lettera dell'alfabeto ebraico *alef*, dall'ultima lettera *taw*, dalla seconda *beth* e, dalla penultima, *shin*: da queste quattro lettere proviene il nome del codice (A – T – B – SH). Il metodo più semplice per risolvere un cifrario Atbash consiste nell'utilizzo di una tabella di cifratura, in questo caso una semplice lista involutoria. Sapendo, in sostanza, che questo tipo di codice crittografico prevede l'inversione dell'alfabeto, sarà sufficiente scrivere su due righe i due alfabeti (il primo "normale" ed il secondo cifrato) e a quel punto fare un semplice lavoro di ricerca.

Al fine di decrittare il termine nascosto, partendo da ogni lettera all'interno della seconda sequenza, dovremo cercare la sua corrispettiva nell'alfabeto originale.

alfabeto chiaro	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
alfabeto cifrato	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Figura 1: Alfabeto chiaro e cifrato in Ebraico.

Quindi, dalla parola **ששכ** (formata dalle lettere *shin shin* e *kaf*) si ottiene il termine **בבל** formato dalle lettere *bet bet* e *lamed*): la città **Sesach** occultata da Geremia è dunque **Babele**.

[4] Molto probabilmente furono motivi religiosi inerenti l'analisi testuale del Corano a condurre gli arabi all'invenzione della "tecnica dell'analisi delle frequenze". Ai fini della nostra ricerca è fondamentale il fatto che l'esame dei testi non si arrestò alle singole parole, ma giunse alle singole lettere: fu a questo punto che gli studiosi si accorsero che vocali e consonanti comparivano con frequenza molto variabile. Non è certo chi, per primo, abbia capito che l'analisi delle frequenze rendeva possibile decifrare un crittogramma; ad ogni modo appare certo che la più antica descrizione del procedimento si debba allo studioso del IX secolo Abu Yusuf ibn Ishaq al-Kindi.

Sistemi informativi, naturalmente, erano presenti anche all'interno di altri potentati dell'epoca. All'interno di questo articolo mi sembra doveroso citare, almeno, i servizi dell'antico Egitto e quelli dell'antica Persia.

L'Egitto, concentrò e sviluppò maggiormente la presenza di agenti nelle aree di pericolo per il regno che si trovavano a est verso la Palestina e la Mesopotamia (territori spesso aggrediti dagli Ittiti), e a sud nei territori della Nubia, da sempre instabili. Esistevano tre sezioni diverse dei servizi segreti egizi che svolgevano compiti di ricerca e protezione in ambiti differenti: la prima ricercava informazioni di carattere economico (ad esempio l'ubicazione di miniere d'oro), la seconda era riservata alla protezione fisica del faraone e, la terza, aveva lo scopo di investigare riguardo a notizie politiche e geografiche. La sezione che si occupava della difesa del monarca, era denominata "Occhi e orecchie del re" e faceva rapporto direttamente al primo ministro. Questo corpo speciale è passato alla storia per essere riuscito a sventare alcune minacce contro i faraoni, tra le quali possiamo ricordare la "Congiura del Grande Harem", che fu organizzata da alcune donne del palazzo ai danni di Ramses III ma scoperta e fermata in tempo.

Per quanto riguarda la Persia bisogna anzitutto ricordare che gli Achemenidi diedero vita a un impero decentralizzato attraverso la divisione in regioni, le satrapie, che erano dotate di grandissima autonomia e che venivano amministrate da un governatore regionale, il satrapo. Questi ultimi erano dunque figure estremamente importanti all'interno dell'impero e, generalmente, si trattava di individui fidati nominati direttamente dal re, anche se proprio la loro rilevanza all'interno delle dinamiche politiche rendeva necessario un controllo costante del loro operato. Per avere questo continuo monitoraggio era indispensabile, quindi, un lavoro di spionaggio che agisse nelle satrapie. Le informazioni, una volta raccolte, venivano inviate rapidamente alla capitale grazie ad un efficientissimo sistema di strade e poste.

I servizi segreti persiani possono essere analizzati grazie a due capolavori della letteratura greca: la *Ciropedia* di Senofonte ([8]) e le *Storie* di Erodoto ([4]). In particolare, per quanto concerne la prima opera è Senofonte a fornirci numerosi dettagli riguardo l'*intelligence* persiana:

> Inoltre abbiamo appurato che Ciro guadagnò a sé i funzionari detti Occhi e Orecchie del Re non altrimenti che con premi e onorificenze, e in effetti colmando di doni quanti gli portassero informazioni utili indusse molti ad ascoltare e a osservare cose che, se riferite al sovrano, potevano giovargli. Di qui l'opinione corrente secondo cui il Gran Re ha molti Occhi e molte Orecchie. Comunque sia, è sbagliato credere che il sovrano scelga un solo individuo come Suo occhio: un singolo potrebbe vedere o udire ben poco, e del resto prescrivere a una sola persona di tenere gli occhi aperti equivarrebbe a invitare chiunque altro a tenerli chiusi, e in più tutti saprebbero di

> doversi guardare da colui che è noto come l'Occhio del Re. In realtà le cose non stanno in questi termini e il sovrano presta ascolto a chiunque dichiara di aver udito o di aver visto qualcosa che meriti la sua attenzione. Così si attribuiscono al Re molti Occhi e molte Orecchie, e dappertutto si teme di dire, come se egli fosse in ascolto, parole ostili al sovrano, e si teme, come se egli fosse presente, di compiere azioni che possano nuocergli. Ecco perché nessuno avrebbe osato confidare ad altri qualcosa di spiacevole sul conto di Ciro, anzi ognuno si comportava come se fosse costantemente a contatto con gli Occhi e con le Orecchie del suo Re. Io non so trovare altra ragione di questa generale disposizione verso di lui che nel suo desiderio di ricambiare piccoli servigi con grandi doni [5].

Il mondo greco

Fino a questo momento abbiamo analizzato i sistemi di spionaggio dell'antichità e il codice Atbash presente nella Bibbia. Tuttavia, oltre alla crittografia, esiste un'altra tecnica per proteggere i messaggi: si tratta della steganografia, termine che deriva dal greco dove στεγανός significa "coperto" e γραφία "scrittura".

La differenza sostanziale tra le due tecniche risiede nel fatto che la crittografia si prefigge di nascondere il contenuto del testo, la steganografia, invece, cerca di occultare direttamente il messaggio. Per questo motivo, steganografia e crittografia, pur essendo discipline indipendenti l'una dall'altra, possono essere usate contemporaneamente per garantire maggiore sicurezza al messaggio.

Per descrivere alcuni esempi, la fonte principale a cui si deve fare riferimento è senza dubbio Erodoto con il suo capolavoro, le *Storie* ([4]).

Il primo aneddoto riportato dallo storico greco, narra di Arpago, un nobile appartenente al popolo dei Medi che, volendo vendicare un torto subito, decide di agire da doppiogiochista in favore dei Persiani. Il confine tra le due regioni, tuttavia, è estremamente sorvegliato e pertanto è costretto a escogitare un capolavoro di steganografia [5, p. 79] per riuscire a far pervenire al re persiano Ciro il suo messaggio:

> E infine, non avendo altro mezzo perché le strade erano sorvegliate, escogitò, per comunicare il suo disegno a Ciro, che viveva in Persia, uno stratagemma. Preparò una lepre, ne aprì il ventre e, lasciandole la pelliccia intatta così come si trovava, le mise dentro una lettera dove aveva descritto il suo piano. Cucì il ventre della lepre e diede al domestico più fedele delle reti come se fosse un cacciatore, incaricandolo di raccomandare oralmente a Ciro, nel consegnargli la lepre, di tagliarla con le proprie mani e senza testimoni[6].

[5] Senofonte, Ciropedia, viii 2.10 ss [8].
[6] Erodoto, Storie, i 123.3 ss [4]

Nell'opera di Erodoto troviamo anche altri esempi di steganografia ma il più famoso di questi è il celeberrimo caso dello "schiavo tatuato":

> Infatti Istieo, che voleva mandare ad Aristagora il segno della rivolta, e che, essendo le vie sorvegliate, non disponeva di nessun altro mezzo sicuro, aveva raso la testa del suo schiavo più fedele, ne aveva trapunto il capo, e aveva atteso che vi ricrescessero i capelli; e appena gli erano cresciuti lo aveva mandato a Mileto, con quest'unico incarico: che, giunto a Mileto, dicesse ad Aristagora di radergli i capelli e di gettare uno sguardo sulla sua testa; e recavano i caratteri incisi, come ho già detto, un messaggio di rivolta [7].

Per quanto riguarda la crittografia invece, le più antiche notizie riguardo l'origine, sono quelle sulla scitala lacedemonica che Plutarco ritiene probabilmente in uso sin dai tempi di Licurgo[8] ma più sicuramente usata ai tempi di Lisandro[9]. Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio; sulla fettuccia si scriveva per righe o colonne parallele, lettera per lettera, il testo segreto. Senza un secondo bastone delle stesse misure del primo, il messaggio risultava incomprensibile.

Tra il 390 e il 360 a.C. Enea Tattico[10], generale della lega arcadica, scrive il primo trattato di cifrari. Grazie a Polibio [7, x 44] sappiamo che il trattato giunto a noi, in realtà, non è altro che una sezione di una più ampia opera di carattere militare intitolata τὰ περὶ τῶν στρατηγικῶν ὑπομνήματα [11].

Nel xxxi capitolo, intitolato *Sui messaggi segreti*, Enea riporta un elenco di quindici metodi (ai quali si devono aggiungere cinque varianti) per trasmettere segretamente un messaggio. Tuttavia, di questi, solo due possono essere considerati sistemi crittografici mentre gli altri tredici sono esempi di steganografia.

Il primo, di facile decrittazione, prevedeva l'utilizzo di "puntini" da inserire nella parola al posto delle vocali [11, xxxi 30], l'altro, invece, è più interessante ed è diventato celebre come "disco di Enea".

> Spiegherò adesso il mezzo di trasmissione più segreto, ma anche più laborioso: quello senza scrittura. Ecco di cosa si tratta. Su un astragalo di una certa grandezza, pratica 24 fori, 6 per ciascuna faccia: i fori rappresentano le lettere dell'alfabeto. Tieni bene a mente, a partire dalla faccia in cui si trova al primo posto l'alfa, anche le lettere che seguono via via su ciascuna faccia. Quindi, quando vuoi formare una parola per mezzo di questi fori, vi inserirai un filo. Così, per esempio, se vuoi comporre la parola «Aineian», seguendo questo metodo, inserirai il filo iniziando dalla faccia dell'astragalo

[7] Erodoto, Storie, v 35.3 [4]

[8] Principale legislatore di Sparta, vissuto tra il ix e l'viii secolo a.C.

[9] Vissuto dal 440 al 395 a.C., Lisandro, fu un militare spartano che servì la sua città nell'ultima fase della guerra del Peloponneso e all'inizio della guerra di Corinto nella quale trovò la morte.

[10] Secondo alcuni studiosi sarebbe da identificare con Enea di Stimfalo.

> dove si trova l'alfa, salterai le lettere successive fino ad arrivare alla faccia dove c'è lo iota ed inserirai di nuovo il filo; trascurate le successive lettere, arriverai dove c'è il ni e lo inserirai; [...] alla fine, risulterà un gomitolo di filo avvolto intorno all'astragalo: chi leggerà il messaggio dovrà trascrivere su una tavoletta le lettere indicate dai fori. Il filo verrà sbrogliato in senso inverso a quello in cui è stato avvolto [11, xxxi 16–19].

Una svolta fondamentale nella storia della crittografia la incontriamo con Polibio. Quest'ultimo, infatti, nelle sue Storie, afferma di aver contribuito a progettare un sistema completamente innovativo, che è ormai comunemente conosciuto come "scacchiera di Polibio" [7, X 45, 6-12].

	1	2	3	4	5
1	α	β	γ	δ	ε
2	ζ	η	θ	ι	κ
3	λ	μ	ν	ξ	o
4	π	ρ	σ	τ	υ
5	φ	χ	ψ	ω	

In realtà, questo più che un sistema di cifratura è un metodo di telecomunicazione, ma è importante sottolineare che per la prima volta si introducono due numeri per indicare una lettera (per esempio η=22, φ=51...).

Il mondo romano

In un certo senso, non è sbagliato affermare che le prime spie romane di cui si ha certezza siano delle... oche!

Attirati dalla ricchezza delle terre meridionali, all'inizio del iv secolo, i Galli superarono le Alpi e, dopo aver sconfitto l'esercito romano presso il fiume Allia[11], riuscirono a entrare e a saccheggiare Roma [3, p. 89]. Solo il Campidoglio rimase incolume [7, II 18, 2] e i Galli, preferendo evitare uno scontro campale, decisero di infiltrarsi durante la notte senza farsi notare. Tuttavia, le oche sacre del Campidoglio si accorsero della loro presenza e iniziarono a starnazzare svegliando così il console Marco Manlio che, a questo punto, riuscì a respingere i nemici [5, p. 119].

Leggendo questo aneddoto sorge spontaneamente un quesito: perché la grande potenza, Roma, non adotta sin da subito un importante sistema di *intelligence* dato che, come abbiamo visto, se ne erano già sviluppati vari tipi, in diverse regioni? La risposta va sicuramente ricercata nel *mos maiorum* e nel concetto di *bellum iustum*

[11] Il fiume Allia è un affluente del Tevere.

sempre ricercato da Roma che, infatti, sembrò sempre disapprovare l'uso di insidie ed inganni, preferendo ogni volta lo scontro a "viso aperto" [6, p. 65].

Però come sostiene Brizzi [1] «la guerra annibalica rese l'Urbe consapevole della necessità di sviluppare una rete informativa efficiente, creando quindi una vera e propria frattura tra i propri valori morali e la ragion di stato».

Alla vigilia della seconda guerra punica (218-202 a.C.) i Cartaginesi potevano vantare, grazie al costante sviluppo dei loro sistemi di spionaggio, una rete informativa nettamente superiore agli *exploratores* romani e, inoltre, trovarono in Annibale il perfetto comandante che riuscì a sfruttare pienamente le potenzialità delle sue strutture di *intelligence*. Nel corso della guerra l'inesperienza dei Romani in fatto di spionaggio si manifestò diverse volte. Un esempio eclatante fu la battaglia del lago Trasimeno: il luogo si prestava perfettamente per un'imboscata ed Annibale aveva già mandato in avanscoperta alcuni ricognitori al fine di redigere una mappatura completa del territorio per organizzare un poderoso attacco; il controspionaggio romano non fiutò il pericolo e la battaglia segnò una nettissima sconfitta per l'esercito romano.

La situazione cambiò completamente quando la gestione dello scontro fu affidata a Scipione; egli, fu infatti il primo a comprendere la necessità di reperire informazioni ed usare stratagemmi. La stessa mentalità romana, da sempre avversa a tali tecniche, di fronte al serio pericolo della sconfitta si modificò rapidamente. A partire dal 204 a.C. la guerra fu portata in Africa e Scipione iniziò ad usare in maniera massiccia le spie. L'esempio più importante di questa nuova scelta tattica si ritrova senza dubbio con l'invio di una ambasceria presso Siface[12] composta non solo da diplomatici ma anche da centurioni che, tuttavia, vennero travestiti da schiavi. Questi ultimi avevano il compito di aggirarsi nell'accampamento con lo scopo di analizzare l'esercito nemico, di individuare il posizionamento delle torrette d'avvistamento pericolose e di memorizzare qualsiasi altro elemento potesse risultare utile [5, p. 135].

Un'importante conseguenza di questa guerra fu la paura. I Romani furono presi da una sorta di psicosi dell'aggressione e, sebbene in seguito alla vittoria su Cartagine non avessero più veri rivali, il popolo e il Senato iniziarono a considerare preoccupante qualsiasi movimento si verificasse all'orizzonte. Questo sentimento spinse Roma al militarismo e, più importante per la nostra trattazione, a un uso sempre maggiore di spie. Per quanto concerne i servizi di informazione militare, si vennero a creare principalmente cinque tipi di spie nel corso del tempo: si tratta dei *frumentarii*, degli *stationarii*, degli *speculatores*, dei *beneficiarii* e degli *agentes in rebus*.

[12] Siface era il re della Numidia.

Inoltre, anche a Roma si inizia a utilizzare la crittografia. I cifrari fondamentali sviluppatisi nella più grande potenza dell'antichità furono principalmente due ad opera di Giulio Cesare e di Ottaviano Augusto. Il primo è un cifrario a sostituzione monoalfabetica con "chiave" 3. Questo significa che nel sistema crittografico a lui attribuito, ogni lettera viene fatta slittare tramite uno spostamento di tre posizioni. La fonte che ci parla di questo sistema crittografico è Svetonio che, nella *Vita dei Cesari* descrive la tecnica adottata da Cesare per proteggere i suoi messaggi:

> Restano anche alcune lettere a Cicerone, altre agli amici su questioni private; in queste, se doveva trasmettere qualche cosa riservatamente, la scriveva in cifra, cioè modificando l'ordine delle lettere in modo tale non ne potesse venir fuori nessuna parola di senso compiuto: se uno vuole esaminarle e decifrarle, metta la quarta lettera dell'alfabeto, cioè la D, al posto della A, e così le altre lettere[13].

Schematizzando dunque il sistema di Cesare, otteniamo la seguente tabella:

alfabeto chiaro	A	B	C	D	E	F	G	H	I/J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
alfabeto cifrato	D	E	F	G	H	I/J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C

Figura 2: Il cifrario a sostituzione monoalfabetica di Cesare, nella variante con uno spostamento in "chiave 3".

In questo caso, il famoso messaggio di Cesare *veni vidi vici*, dopo la crittazione, diventerebbe *"zhqm zmgm zmfm"*.

v	e	n	i		v	i	d	i		v	i	c	i
z	h	q	m		z	m	g	m		z	m	f	m

Sempre Svetonio ci spiega il codice di Augusto che prevedeva semplicemente uno spostamento in "chiave 1" in quanto ogni lettera veniva sostituita da quella immediatamente successiva.

v	e	n	i		v	i	d	i		v	i	c	i
x	f	o	k		x	k	g	k		x	k	d	k

[13] Svetonio, Vita dei Cesari, trad. it. di F. Casorati, Newton, Roma 2015, i 56 [10].

Infine, vorrei parlare di un enigma interessante scoperto durante gli scavi eseguiti a Pompei nel 1936. Tra i numerosi graffiti riportati alla luce, uno attirò l'attenzione di molti studiosi: si trattava di un rompicapo in lingua latina (fig. 3), già ritrovato in altri territori, costituito da venticinque lettere disposte su cinque righe in forma di quadrato. Il crittogramma è stato trovato anche in una versione "rovesciata"

(fig. 4) rispetto a quella appena rappresentata, tuttavia, anche in questo caso, si viene a creare un palindromo perfetto. Il "quadrato magico", è dunque formato da quattro A, quattro E, quattro O, quattro R, quattro T, due P, due S e una N.

R	O	T	A	S
O	P	E	R	A
T	E	N	E	T
A	R	E	P	O
S	A	T	O	R

Figura 3: Il crittogramma.

S	A	T	O	R
A	R	E	P	O
T	E	N	E	T
O	P	E	R	A
R	O	T	A	S

Figura 4: La forma "rovesciata".

Due studiosi, Sigurd Agrell e Felix Grosser, senza essere a conoscenza l'uno del lavoro dell'altro, iniziarono a studiare il rompicapo da un punto di vista crittografico, arrivando alla medesima, sensazionale, soluzione. All'interno del Quadrato si nasconde un anagramma e, più precisamente un doppio *pater noster* che, a causa della presenza di un'unica N, può essere trascritto solo in forma di croce con ai lati due A e due O che simboleggiano l'*alfa* e l'*omega* citata nell'Apocalisse [9, p. 195].

A

P

A

T

E

R

A P A T E R N O S T E R O

O

S

T

E

R

O

Riferimenti bibliografici

1. G. Brizzi. *I sistemi informativi dei romani. Principi e realtà nell'età della conquista oltremare (218-168 a.C.)*. Franz Steiner Verlag, Wiesbaden, 1982.
2. CEI, editor. *La Sacra Bibbia, (versione ufficiale CEI)*. Unione Editori e Librai Cattolici Italiani (UELCI), Roma, 2004.
3. G. Clemente. *Guida alla storia romana*. Oscar Mondadori, Milano, 2008.
4. Erodoto. *Storie*. Newton Compton, Roma, 2008.
5. S. Musco. *Storia dello spionaggio antico. Teoria e strategie di intelligence dagli albori alla caduta dell'Impero romano*. Aracne editrice, Roma, 2014.
6. M.F. Petraccia. *In rebus agere. Il mestiere di spia nell'antica Roma*. Pàtron Editore, Bologna, 2012.
7. Polibio. *Storie*. Newton Compton, Roma, 1998.
8. Senofonte. *Ciropedia*. BUR, Milano, 2013.
9. A. Socci. *La guerra contro Gesù*. BUR, Milano, 2012.
10. Svetonio. *Vita dei Cesari*. Newton Compton, Roma, 2015.
11. Enea Tattico. *La difesa di una città assediata (Poliorketika)*. ETS Editrice, Pisa, 1990.

Epigrafi cifrate nelle chiese antiche

Cosimo Palma

Università di Pisa - Universitá di Napoli "L'Orientale", Italia
cosimo.palma@phd.unipi.it

Sommario In numerosi luoghi di culto si rinvengono iscrizioni misteriose, molte delle quali tutt'ora incomprensibili. Tra queste spicca un'epigrafe situata nella Cappella Turbolo della chiesa napoletana di Santa Maria La Nova, su cui si dilungherà questo contributo. L'iscrizione è stata analizzata mediante procedure scritte in *Python* in combinazione con il software di decrittazione *AZdecrypt*, mostrando caratteristiche linguistiche che convergono inequivocabilmente verso l'ipotesi che il suo testo in chiaro sia cifrato mediante sostituzione monoalfabetica su una lingua naturale, possibilmente insieme a tecniche di trasposizione e polialfabetismo. Un'analisi preliminare degli n-grammi dei caratteri e sulle combinazioni vocali-consonanti estratti dai corpora non è ancora riuscita a individuare alcuna lingua candidata per il testo in chiaro.

Introduzione

Iscrizioni misteriose hanno sempre affascinato sia studiosi che profani, in quanto artefatti paradossali che oscillano tra il mostrare e il nascondere. Questa contraddizione solleva interessanti questioni di natura filosofica ed epistemologica sulla natura della conoscenza e della comunicazione. Nel corso della storia, numerosi esempi di epigrafi cifrate hanno catturato l'attenzione del pubblico. Tra questi, spiccano tre casi particolarmente intriganti: i Colossi di Memnone a Tebe, le iscrizioni nei Duomi di Barga, Lucca e Pisa, e l'epigrafe nella Chiesa di Santa Maria la Nova a Napoli.

I colossi di Memnone I Colossi di Memnone, imponenti statue poste a guardia della tomba del faraone Amenhotep III a Tebe, sono noti non solo per la loro maestosità, ma anche per i suoni misteriosi che emettono all'alba, fenomeno attribuito dalla leggenda al richiamo di Memnone, figlio di Eos, la dea dell'aurora. Sui piedi di queste statue sono incise numerose iscrizioni, di cui due particolarmente enigmatiche [20]. Il metodo di cifratura utilizzato, scoperto dal filologo Bataille [3], si basa su un sistema numerico ispirato alla cabala ebraica, applicato all'alfabeto greco: l'*ipopsefia*.

De Cifris Koine – Eruditorum ACTA 2024 –https://doi.org/10.69091/koine/vol-3-E03

(a) (b)

Figura 1: (a) Viste anteriore e laterale delle gambe del colosso di Memnone (Fonte: *Wikimedia*). Sulla destra, dettaglio della parte esteriore del piede sinistro (adattato da [20]).

Come nella *gematria* rabbinica, si associa a ogni lettera dell'alfabeto greco un valore numerico, che va da 1 a 900. Con la strategia di crittografia più comune, ogni segno si traduce in quello risultante dalla differenza tra l'ordine numerico immediatamente superiore e il valore numerico stesso. Ad esempio, se Ψ equivale a 700, dovrebbe essere letto come 1000 meno 700, quindi 300, il valore della lettera τ. Secondo questo calcolo, tutti i glifi corrispondenti a numeri con un 5, come 50 e 500, non cambiano [1].

I Duomi di Barga, Lucca e Pisa Le iscrizioni nei Duomi toscani presentano un caso diverso, dove la brevità del testo rende impossibile un vero attacco crittografico. L'epigrafista Margherita Guarducci [7] ha proposto un'interpretazione basata sulla simbologia cristiana, identificando le lettere **MHL** come abbreviazione di "Michael", ripetuta tre volte in onore della Santissima Trinità [illegible].

La Chiesa di Santa Maria la Nova a Napoli Infine, l'epigrafe nella Chiesa di Santa Maria la Nova a Napoli rappresenta una sfida ancora più complessa. A differenza degli esempi precedenti, si tratta di un testo più esteso e articolato, che richiede un'analisi approfondita e multidisciplinare per svelare il suo significato nascosto.

All'interno della Cappella Turbolo di Santa Maria la Nova (Napoli, Italia) si trovano due epigrafi. Quella sul lato sinistro dell'osservatore contiene una dichiarazione di indulgenza di Papa Gregorio XIII relativa alle messe in essa celebrate, in

[1] Nonostante la sua rilevanza, non si è ritenuto opportuno includere questo approccio nello studio sull'iscrizione cifrata della Cappella Turbolo, in quanto rientra comunque nell'ambito di una sostituzione monoalfabetica. Eventualmente, essa potrebbe essere facilmente indagata per verificare se sia stata applicata seguendo i principi isopsefici.

dedicazione alla signora Turbolo, la nobildonna Giovanna De Rosa. Sul lato destro è posta un'epigrafe scritta in un alfabeto sconosciuto[2].

(a) Complesso Monumentale Santa Maria La Nova

(b) Cappella Turbolo

Figura 2: Sulla sinistra, vista della navata centrale della Chiesa di Santa Maria La Nova. A destra, vista frontale della Cappella Turbolo. L'iscrizione presa in esame in questo lavoro è situata sulla parte destra (Fonte: *Wikimedia*).

Questa caratteristica immediatamente riconoscibile non ci permette di capire che ci troviamo di fronte a un testo cifrato: come spesso accade in questi casi, l'unica prova decisiva che stiamo affrontando un crittogramma sarebbe scoprirne la decrittazione, o almeno qualsiasi altro elemento esterno che possa indicarci senza ulteriori dubbi che si tratti di un crittogramma.

Lavori correlati

Da alcuni articoli di giornale emerge che sono stati intrapresi seri tentativi di decrittazione, anche se le pubblicazioni scientifiche correlate sembrano impossibili da rinvenire. Gli unici due lavori pubblicati che menzionano esplicitamente l'iscrizione della cappella Turbolo sono focalizzati sulle caratteristiche artistiche e architettoniche dell'intera chiesa [19] o su un insieme specifico di eventi storici e genealogie aristocratiche esposti per verificare l'affidabilità della teoria secondo cui nella tomba posta all'esterno, dall'altro lato del muro della epigrafe stessa, sarebbe sepolto

[2] L'iscrizione è costituita da circa seicento glifi, contro i millesettecentocinquanta dell'indulgenza papale. Oltre alle ovvie ragioni di spazio, l'inserimento dell'intera fotografia sarebbe stato superfluo a causa delle numerose cancellazioni ed erosioni presenti principalmente nelle aree superiore e inferiore. Si rimanda alla sezione "Rassegna degli alfabeti storici e dei cifrari coevi" 4 per ulteriori dettagli sull'argomento.

(a) Dettaglio epigrafe crittata (b) Araldo della Famiglia Ferrillo

Figura 3: Sulla sinistra, un'istantanea dell'epigrafe cifrata della Cappella Turbolo nella Chiesa napoletana di Santa Maria La Nova ai raggi ultravioletti (per gentile concessione dell'associazione culturale 'Oltre il chiostro', ente gestore del complesso monumentale). A destra, particolare della Tomba Ferrillo, situata al di lá del muro cui l'epigrafe esaminata è affissa. Secondo alcuni, luogo di sepoltura di Vlad III di Valacchia (popolarmente conosciuto come Dracula (Fonte: *Wikimedia*).

il conte Vlad III di Valacchia [14], popolarmente conosciuto come il conte Dracula. Nel primo lavoro l'autore, il colto e generalmente stimato padre Rocco, afferma che l'iscrizione sia la traduzione in greco dell'iscrizione latina adiacente. Eppure, anche un profano riconoscerebbe facilmente che la prima epigrafe è troppo lunga rispetto alla seconda, che a sua volta mostra molti glifi non appartenenti all'alfabeto greco. Tale incongruenza, la cui menzione non vuole detrarre nulla al defunto autore, suscita sincera sorpresa, e meriterebbe ulteriori approfondimenti. Nel secondo testo correlato, vengono avanzate tre congetture sulle origini dell'iscrizione, tra le quali si riporta solo la più rilevante: l'iscrizione non sarebbe altro che una tavola usata dai monaci francescani per scopi didattici.

La chiesa era infatti considerata, alla fine del XVI secolo, uno dei poli universitari più fiorenti del Sud Italia, dove, tra le altre cose, si insegnavano anche lingue orientali e calligrafia. La stessa autrice riporta che una datazione al radiocarbonio eseguita sull'epigrafe la colloca intorno al XVI-XVII secolo e che un tentativo preliminare di decrittazione, consistente nel sostituire ogni glifo con probabili fonemi correlati a glifi simili in altri alfabeti, non ha portato a risultati soddisfacenti. Non è raro trovare iscrizioni misteriose nelle chiese occidentali così come in quelle orientali, anche se in questi casi sono presenti per lo più sotto forma di tetragrammi [15], una lunghezza del testo che non può essere paragonata a quella ivi analizzata.

Un altro articolo (quasi omonimo al presente, peraltro menzionato in 4) formula per primo il dilemma epistemologico di un oggetto cifrato situato in bella vista [20]. Secondo l'autore, il potere magico o mistico attribuito alle lettere dell'alfabeto nella cultura orientale ed egizia spiega l'uso degli acrostici in contesti religiosi in Egitto. Inoltre, afferma che il codificatore potrebbe voler stuzzicare l'osservatore con un enigma, come un gioco intellettuale, e non con il vero scopo di nascondere un messaggio. Un ulteriore scenario, tanto sottile quanto importante, è il caso in cui qualcosa debba essere scritto per legge o imposizione, implicando implicitamente la sua comprensibilità, senza esprimerla, aprendo così la possibilità per l'incisore riluttante di eseguire una sorta di "giuramento di Isotta", per cui il requisito venga soddisfatto nella forma, ma non nella sostanza.

Formulazione del problema

Molte osservazioni superficiali, come il numero di caratteri diversi, nella stessa gamma degli alfabeti standard, sono sufficienti per supporre che l'epigrafe sia molto probabilmente la crittografia di un testo scritto in una lingua naturale. Tuttavia, il fatto stesso che l'artefatto sia situato in bella vista, ci permette di immaginare che qualunque informazione contenuta in esso non debba essere eccezionalmente segreta e richieda di essere rivelata da un gruppo di persone in possesso della chiave adatta o di una quantità sufficiente di tempo. Il denso conglomerato di storia e mistero in cui l'epigrafe è avviluppata induce innanzitutto a fare un passo indietro e decidere da quale angolazione debba essere affrontata la decrittazione. Lo stesso è indubbiamente, allo stesso tempo, una fonte di motivazione per intraprendere questa sfida.

Metodologia

A causa dell'abbondante letteratura disponibile per l'aspetto storico e della mancanza di un'analisi quantitativa seria dell'oggetto, si è deciso di concentrarsi solo sui compiti strettamente correlati alla decrittazione, nella speranza che gli indizi rilevati, una volta uniti a quelli provenienti da dominii diversi, possano infine portare a una soluzione olistica del rompicapo. I principali passaggi intrapresi per tentare la decrittazione dell'epigrafe sono:

- Revisione degli alfabeti storici e dei cifrari coevi;
- Analisi statistica sui singoli caratteri;
- Raccolta e pre-elaborazione dei *corpora* delle lingue candidate;
- Trasposizione dei glifi dell'epigrafe in caratteri latini;
- Analisi preliminare sull'alternanza di vocali e consonanti;
- Calcolo dell'Indice di Coincidenza per frammenti di testo estratti da ciascun corpus;

- Calcolo dell'Entropia dell'Informazione di Shannon per frammenti di testo estratti da ciascun corpus;
- Esecuzione del test di Friedman per ogni lingua candidata;
- Analisi statistica sugli N-grammi;
- Generazione di un file di N-grammi adatto per il software *AZdecrypt*;
- Copia della traslitterazione principale dell'epigrafe nella finestra di input del software;
- Esecuzione del risolutore per ogni modalità di decrittazione rilevante;
- Salvataggio e analisi dei file di output.

Nel seguito, verranno descritti in dettaglio solo i passaggi non banali tra quelli sopra elencati.

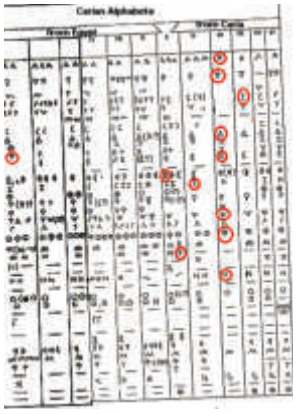
Rassegna degli alfabeti storici e dei cifrari coevi

Prima di immergersi nella procedura canonica di decrittazione, per la quale si è seguito il percorso tracciato in [11, 8] sulla base di [18], si è inizialmente intrapreso una revisione di tutti gli alfabeti esistenti, che ha sostanzialmente confermato la già menzionata gamma di alfabeti partecipanti alla composizione dell'epigrafe, come lo slavonico ecclesiastico, il greco, il latino e il copto [14]. In aggiunta a questi, l'alfabeto cario è risultato essere l'alfabeto che, singolarmente, contiene il maggior numero di glifi dell'iscrizione[3]. Non solo gli alfabeti esistenti, ma anche quelli inventati sono stati presi in debita considerazione[4], come elencati in [10, 5, 24, 23, 22, 13, 12, 21]. I lavori citati contengono anche lo stato dell'arte della scienza crittologica del XVI secolo, che all'epoca era ancora ai suoi albori. Se la datazione al radiocarbonio dell'iscrizione fosse considerata affidabile (il che è altamente probabile, poiché corrisponde alle date incise sulla tomba dei Turbolo), l'ipotesi di crittografie a sostituzione polialfabetica o omofonica non può essere ancora scartata con certezza (vedi sezione "Analisi statistica sui singoli caratteri" per una valutazione empirica di questa domanda), poiché esse sono nate proprio in quegli anni [5, 24]. L'indagine in questo dominio può essere considerata completa solo se viene preso in considerazione anche un altro insieme di simboli, cioè quelli che potrebbero essere mappati a concetti, invece che a caratteri alfabetici usuali, come nel caso dei segni alchemici.

Nonostante la notevole somiglianza con alcuni dei simboli presenti nell'epigrafe, non è stato possibile trovare un modo univoco per abbinarli a singoli caratteri. Ad esempio, prendere solo la lettera iniziale dell'elemento rappresentato risulterebbe in una pesante omofonia, che una volta trasposta praticamente non produrrebbe alcuna parola o frase significativa.

[3] Il cario è una lingua estinta parlata fino al primo secolo a.C. in *Caria*, una regione dell'Anatolia occidentale, e in Egitto [1].

[4] I due esempi più notevoli sono la *Lingua Chaldeorum* di Rodolfo IV Duca d'Austria, e la *Lingua Ignota* di Santa Ildegarda di Bingen, alla quale è persino collegato un glossario di oltre mille parole.



(a) Alfabeto Cario

Epigraph's glyph (EG)	Related Latin letter (CL)	EG	CL
A	A	O	O
B	B	Π	P
C	C	Q	Q
D	D	R	R
E	E	S	S
F	F	T	T
G	G	U	U
H	H	V	V
I	I	W	W
L	L	X	X
M	M	Y	Y
N	N	Z	Z

(b) Glifi mappati a caratteri latini

(c) Tavola dei simboli alchemici

Tavola 1: Sulla sinistra, tavola diacronica dell'alfabeto cario. I glifi che assomigliano a quelli dell'epigrafe sono cerchiati in rosso. Al centro, mappatura dei glifi presenti nell'iscrizione cifrata verso alfabeto latino, per permettere l'analisi computazionale del testo. A destra, la tavola dei simboli alchemici di Basilio Valentino, del 1666 (Fonte: *Wikimedia*).

.

Analisi statistica sui singoli caratteri

L'epigrafe ha chiaramente subito gravi cancellazioni, soprattutto nella parte inferiore: l'intero testo a nostra disposizione non è quindi adatto per un'analisi statistica soddisfacente, che di solito offre i migliori risultati quando eseguita su campioni più ampi. Tuttavia, l'attacco manuale preliminare non ha avuto successo, portando così a un attacco assistito dal computer [16]. Il primo passo verso la decrittazione è stato stabilire una mappatura arbitraria dei glifi in lettere latine per produrre un documento leggibile dal computer. Successivamente, un gruppo di lingue candidate è stato selezionato secondo vari fattori, come il loro prestigio nel periodo a cui appartiene l'iscrizione, nonché la loro diversità[5], e raccolto online, principalmente attraverso il database di corpora online HistCorp [9][6].

[5] Considerare diverse famiglie linguistiche accelera consapevolmente il processo di identificazione della lingua del testo in chiaro, in modo tale che la soluzione si possa trovare in maniera graduale, procedendo dal ceppo, alla famiglia, al ramo, fino al dialetto.

[6] Il corpus per il lussemburghese antico è stato ottenuto manualmente, mediante la scansione di una copia del *Codex Mariendalensis*

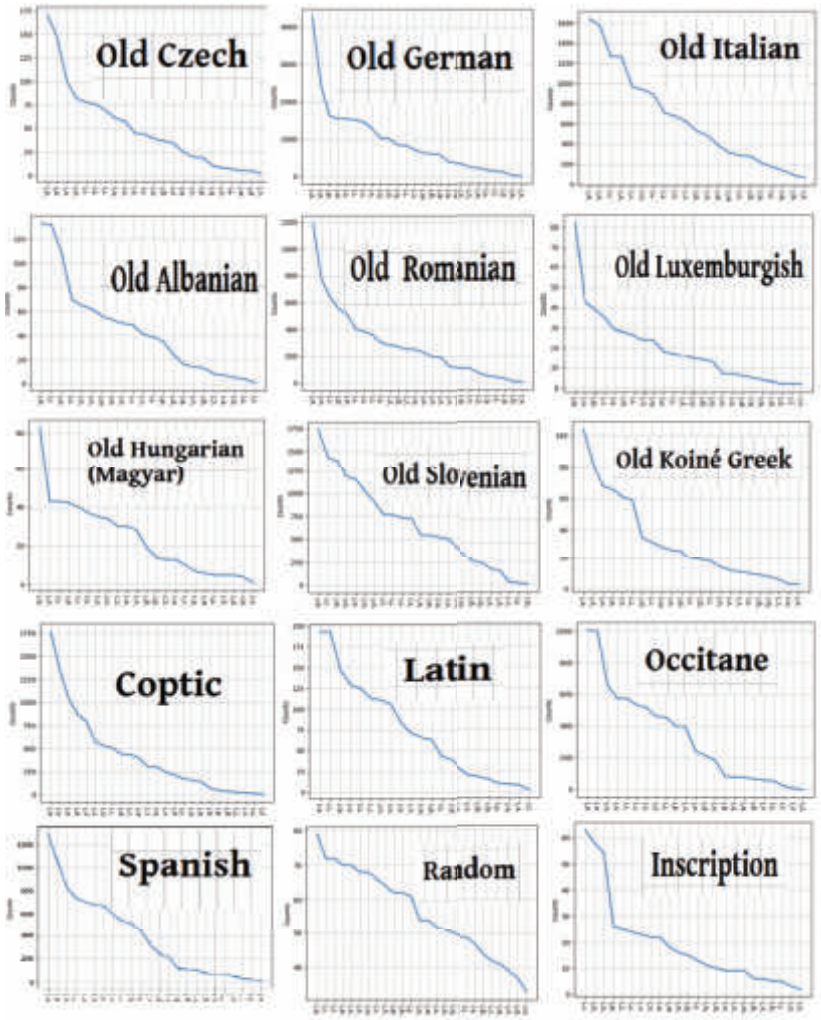


Tavola 2: Una visione sinottica della distribuzione di frequenza dei caratteri per tutte le lingue candidate, eseguita su frammenti casuali di lunghezza simile a quella dell'iscrizione, estratti dai relativi corpora. Dall'alto a sinistra, procedendo verso il basso e verso destra: Ceco Antico (Boemo), Tedesco Antico, Italiano Antico, Albanese Antico, Rumeno Antico, Lussemburghese Antico (Mosellano), Ungherese Antico (Magiaro), Slavonico ecclesiastico, Greco Koiné, Copto, Latino, Occitano, Spagnolo, Testo Casuale, Epigrafe.

Indice di Coincidenza

L'incertezza derivata da queste osservazioni preliminari ha indotto la necessità di un'analisi statistica. La letteratura correlata riporta diversi metodi per la valutazione della lingua del testo chiaro per un testo cifrato, tra i quali l'Indice di Coincidenza e l'Entropia dell'Informazione di Shannon rappresentano i più conosciuti ed efficienti. L'Indice di Coincidenza (IC) è una misura che riflette la probabilità che in un determinato testo due lettere selezionate casualmente coincidano. È utilizzato in crittologia per l'identificazione della lingua del testo chiaro, poiché ogni lingua ha un IC relativamente costante. Nell'equazione dell'IC, N rappresenta la lunghezza del testo, da *n1* fino a *nc* sono le frequenze (come interi) delle c lettere dell'alfabeto.

$$\mathbf{IC} = \frac{\sum_{i=1}^{c} n_i\,(n_i - 1)}{N(N-1)/c}$$

Tuttavia, si deve considerare che lo stile di scrittura e le convenzioni per le epigrafi sono molto diversi da quelli normali: la soppressione di tutte le doppie, così come l'uso di abbreviazioni, riducono automaticamente l'IC. D'altra parte, la *scriptio continua* [7] aumenta la stessa probabilità, poiché la lettera finale di una parola può corrispondere alla lettera iniziale di quella successiva. Per parametrizzare queste discrepanze nell'equazione dell'IC, sarebbe desiderabile analizzare queste variazioni su un corpus più ampio di epigrafi, scritte in entrambi gli stili, un compito che non è necessario intraprendere per questo lavoro. L'IC è stato calcolato automaticamente mediante la funzione "getIOC" del progetto, che implementa la suddetta formula.

Ulteriori test statistici

Un'altra misura attraverso cui una lingua intera può essere catturata è l'Entropia dell'Informazione di Shannon (SIE), definita come segue (Shannon, 1951):

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$$

La formula calcola il livello medio di informazione, intrinseco ai possibili esiti della variabile (nel nostro caso, i caratteri), dove un esito più informativo è inteso come quello meno atteso.

Altri metodi per la valutazione della lingua del testo chiaro sono test di somiglianza statistica, come il χ^2, il test di Kolmogorov-Smirnov o il test di divergenza di Kullback-Leibler, concepiti per misurare quanto sono simili due campioni, cioè quanto è probabile che siano generati dalla stessa funzione di distribuzione.

[7] Dal latino, letteralmente: scrittura continua, cioè lo spazio tra le parole è omesso. Questo stile di scrittura è tipico anche dell'epigrafia greca.

Lingua candidata	IC Normalizzato
Iscrizione	1,72
Testo casuale	1,03
Ungherese antico	1,61
Lussemburghese antico	1,87
Romeno antico	1,71
Ungherese antico 2	1,75
Copto	1,87
Greco Koiné	1,88
Latino	1,94
Albanese antico	1,73
Sloveno antico	1,52
Spagnolo antico	1,81
Italiano antico	1,53
Tedesco antico	1,95
Ceco antico	1,30

Tavola 3: IC Normalizzato per diverse lingue candidate

Ancora una volta, la lunghezza limitata dell'iscrizione non permette di prendere in seria considerazione questo metodo. Condizione per il confronto è che i campioni, resi algoritmicamente come due vettori, siano della stessa lunghezza. Inoltre, i loro valori devono essere normalizzati, poiché le distribuzioni di frequenza dei caratteri possono provenire da corpora di dimensioni diverse[8].

Analisi statistica sugli N-grammi: un breve excursus sul software AZdecrypt

L'attacco crittologico basato sugli N-grammi è stato supportato da *AZdecrypt* [2], lo stesso software utilizzato per decifrare il famoso codice Zodiac [6]. Sebbene non sia il software più "user-friendly" e avanzato a disposizione in termini di comunità di supporto e periodicità delle nuove versioni, è estremamente flessibile nell'incorporare nuovi corpora. *AZdecrypt* è concepito per la crittoanalisi moderna, specialmente per i cifrari omofoni, tuttavia è facilmente adattabile ai cifrari storici[9]. I vocabolari di n-grammi inclusi in AZdecrypt sono formattati in binario, ma è possibile includerli attraverso un file di testo. Nel progetto *MariaLaNova* la funzione che genera un file di N-grammi adatto ad essere elaborato da *AZdecrypt* può essere

[8] Le procedure che hanno prodotto i risultati di questi test statistici si trovano nel progetto *MariaLaNova*, nel file "Graphs.py" [16]

[9] Il repository contenente tutti gli output, ordinati per lingua e modalità di decrittazione, è accessibile all'indirizzo [17].

Lingua candidata	**SIE**
Iscrizione	∼ 4,1
Testo casuale	∼ 4,7
Ungherese antico	∼ 4,1
Lussemburghese antico	∼ 4,2
Romeno antico	∼ 4,3
Copto	∼ 4,2
Greco Koiné	∼ 5,0
Latino	∼ 4,1
Ceco antico	∼ 4,3
Albanese antico	∼ 4,4
Sloveno antico	∼ 4,4
Spagnolo antico	∼ 4,2
Italiano antico	∼ 4,2
Tedesco antico	∼ 4,1

Tavola 4: Valori SIE per diverse lingue candidate

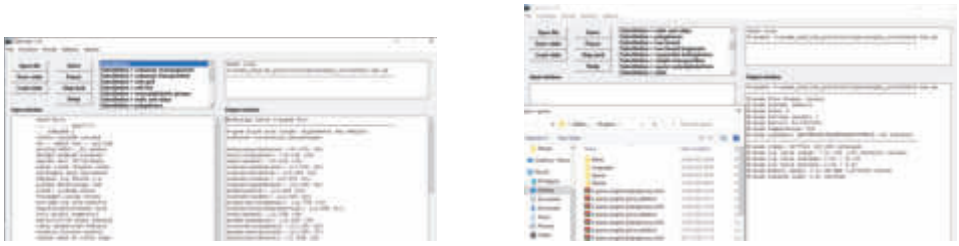
eseguita con il comando: *ngramsAZ(file, 5, case = "lower")* , dove il primo parametro è un corpus, il secondo è l'N desiderato, e il terzo, opzionale, per rendere l'output in minuscolo o maiuscolo. Il file di output elencherà ogni N-gramma immediatamente seguito dal suo valore log, un numero tra 0 e 255 ottenuto da: $log_{10}(frequenzangramma_{corpus}) * 10$ Tutti gli N-grammi seguiti da "000" potrebbero essere rimossi. La libreria GUI utilizzata per AZdecrypt non supporta Unicode. Pertanto, solo le lingue che possono essere rappresentate in ASCII sono supportate visivamente. Un espediente per questo problema è sostituire Unicode con ASCII e poi fornire una tabella di mappatura da ASCII a Unicode nel file *.ini* dell'n-gramma. Il formato *.ini* è utilizzato per semplici file di testo contenenti parametri di inizializzazione. In *AZdecrypt*, accompagna ogni file N-gramma nella cartella "Ngrams". Il suo aspetto per il persiano, una lingua non supportata da Unicode, è:

```
N-gram size=b5
N-gram factor=90.11
Entropy weight=1
Alphabet=#<*)576%4$
,3:-+?1;0(2&"!8'/.>9=
Temperature=700
```

, dove nella prima riga la "b" sta per "binario"[10]. Dovrebbe essere eliminata per tutti i file N-grammi non formattati in binario. La riga dell'alfabeto deve contenere

[10] Per un file di 4-grammi binario, ad esempio, il primo byte rappresenterebbe il valore (log) da 0 a 255 del n-gramma AAAA, il secondo byte sarebbe AAAB... e così via fino a ZZZZ. Tutti i possibili n-grammi devono essere inclusi in questo ordine.

tutti i caratteri presenti nel file N-grammi correlato. La variabile *temperatura* si riferisce alla probabilità di accettare una modifica con un adattamento inferiore. Diminuisce continuamente, emulando il processo di ricottura in metallurgia, da cui il nome. La strategia adottata nel mio studio per evitare caratteri non supportati è trasporre il corpus in caratteri latini *prima* di generare il file N-grammi. Questo viene ottenuto dalle funzioni contenute nel file "Replace.py", e allo stato dell'arte sono disponibili per greco, copto e cirillico. Altri alfabeti possono essere mappati facilmente seguendo lo stesso modello usato per le altre funzioni "Replace".



(a) (b)

Figura 4: (a) La funzione "Languages" di AZdecrypt. (b) Una tipica vista dell'ambiente di lavoro di AZdecrypt.

.

Prima di tentare la decrittazione attraverso tutte le modalità disponibili nel software, un protocollo corretto prevede di utilizzare la funzione "Languages" per determinare in quale lingua in chiaro un dato cifrario di input potrebbe essere, selezionando "File", poi "Batch n-grams (substitution)", e aprendo "Languages.azd" sotto "Languages". Tuttavia, è stata la mia precedente analisi statistica a suggerirmi quali lingue avrebbero dovuto essere prioritarie nel mio attacco supportato dal software, ovvero latino, ungherese, ceco, romeno, albanese e slavo ecclesiastico.

Cliccando su "File" e poi su "Load N-grams" si accede alla cartella con tutti gli N-grammi. Prima di eseguire la decrittazione in una delle modalità selezionate nell'elenco sopra[11], sul lato destro della finestra viene visualizzato il contenuto del file ".ini", così come osservazioni statistiche sul file N-grammi caricato. L'analisi degli N-grammi ha incluso anche un esperimento, per il quale il software non era richiesto. Partendo dall'osservazione che tutte le lingue analizzate mostrano tutte le loro vocali entro le prime otto lettere classificate per frequenza, si può investigare un intreccio vocali-consonanti anche se siamo ancora ignari del testo in chiaro.

[11] Tra tutte, ho utilizzato solo le funzioni per "Sostituzione", "Sostituzione + Nulli & Salti", "Sostituzione + trasposizione semplice", "Sostituzione + polialfabetismo sparso".

Sostituendo nell'epigrafe *tutte le possibili* vocali (tutti i primi otto glifi classificati) con una V, possiamo osservare se il comportamento delle possibili vocali con le consonanti riflette quello delle altre lingue. Questo esperimento si basa sull'assunzione che mentre non tutte le V sono sicuramente vocali, tutte le non-V sono necessariamente consonanti. Dopo aver eseguito questa operazione, si trovano molti 3-, 4- e 5-grammi composti solo da consonanti. Di solito, tre consonanti in sequenza sono già piuttosto rare, cinque quasi impossibili, in quasi tutte le lingue, il che costituirebbe un forte argomento a favore della trasposizione, o addirittura della casualità.

Risultati

Seguendo i passaggi sopra menzionati, sono stati generati numerosi file di testo per ogni lingua in chiaro considerata, attualmente ancora in fase di esame. Non c'è alcuna certezza effettiva che la misteriosa epigrafe di Santa Maria la Nova non sia già stata decifrata 'accidentalmente'. Inserendo in *Google Translate* alcuni frammenti degli output dal latino o dall'ungherese, ci troviamo di fronte a traduzioni affascinanti di notevole coerenza. Nonostante ciò, non possono essere corrette allo stesso tempo; inoltre, *Google Translate* si è dimostrato estremamente inaffidabile perché le parole prive di senso vengono spesso rese con il termine significativo loro più simile e tradotte di conseguenza. Questa osservazione è servita a comprendere che una reale conoscenza delle lingue candidate è una condizione indispensabile per ottenere miglioramenti consistenti verso la decrittazione. Per sopperire alla mancata conoscenza di alcune lingue tra quelle individuate, è inevitabile raccogliere l'aiuto della comunità scientifica, perché solo uno sforzo sinergico può portare alla risoluzione di questo enigma secolare. L'approccio statistico sembra fallire a un primo tentativo, ma ci sono molte strategie che possono ancora essere prese in considerazione. Oltre alla trasposizione e alla sostituzione, ci sono infatti altri espedienti che potrebbero permettere al testo cifrato di mantenere le sue caratteristiche statistiche, come accade nella settima sfida di Bellaso [4], dove la distribuzione di frequenza dei caratteri assomiglia a quella della nostra iscrizione, sebbene sia stata cifrata principalmente con il metodo degli *alfabeti mescolati*.

Conclusioni e lavori futuri

A differenza di altri casi di studio, dove il testo cifrato è solitamente molto più lungo e pulito, ci siamo trovati di fronte a una sfida crittologica per la quale le euristiche di risoluzione probabilistica potrebbero risultare non essere sufficienti, evidenziando la necessità di una decrittazione consapevole anche della semantica del testo. Ciononostante, ci sono ancora alcune opzioni da prendere in considerazione, sempre coerenti con la sostituzione monoalfabetica, come la congettura secondo cui l'epigrafe potrebbe essere redatta in più di una lingua. Questa strada potrebbe

essere percorsa creando molti corpora bilingui, dai quali estrarre gli N-grammi. Un altro scenario possibile potrebbe essere l'assenza di vocali, cioè l'iscrizione potrebbe contenere solo consonanti. Un'opzione che non può essere esplorata realisticamente è l'uso della *steganografia* [24]: anche in quel caso ricadremmo nel grande ostacolo dei glifi esoterici utilizzati, che è ulteriormente aggravato dalla pratica consolidata tra i crittografi coevi di inserire volontariamente errori o abbreviazioni nel testo in chiaro, al fine di impedire la decrittazione. Nel caso in cui intuizioni da elementi collaterali, magari scoperti all'interno della chiesa, suggeriscano che l'iscrizione possa contenere una o più parole, la funzione *Substitution + Crib grid* di *AZdecrypt* può essere utilizzata per verificare se nell'epigrafe siano contenute combinazioni di glifi che permettano quella precisa parola. Questa strada è già stata tentata con termini come 'Santa Maria' e 'Gesù Cristo', tradotti nelle principali lingue candidate, senza successo. Un'ulteriore idea che non deve essere scartata potrebbe essere la creazione di un corpus interamente costituito da parole magiche/esoteriche, raccolte da grimorii, glossari di lingue artificiali come la *Lingua Ignota* di Santa Ildegarda, papiri magici, biblioteche gnostiche e altri libri sull'occultismo e l'alchimia: se l'alfabeto è stato inventato, nulla vieta che anche il relativo vocabolario lo sia.

Appendice

Elenco delle funzioni rilevanti da *MariaLaNova*

1. **Freqvoc**: questa funzione prende un file ".txt" come input e restituisce un dizionario di frequenza delle parole in esso contenute.
2. **letterngramsfilerank**: questa funzione genera un file di n-grammi di un dato file di input classificato per frequenza.
3. **generateioccorpus**: il corpus di input di "ngramsaz" viene creato selezionando file il cui Indice di Coincidenza è più simile a quello dell'epigrafe mediante questa funzione.
4. **ngramsaz**: questa funzione prende un corpus come input (come quello generato nella funzione precedente) e genera un file ".txt" contenente i valori logaritmici per tutti gli n-grammi nel formato richiesto da AZdecrypt (5-grammi): "examp123xamp009exam007".
5. **patternsearch**: questa funzione percorre una particolare lista di parole cercando un pattern. Prende come parametri il numero di caratteri e il pattern. 'k' significa consonante, 'y' vocale e 'u' tutte lettere diverse.
6. **matchwordscrco**: questa funzione attraversa un file ".txt" per trovare una parola che corrisponde alla parola di input come parametro, ad esempio: parola="polo" e file="bebe; marmelade; mouse; poster; fata", il risultato sarà "fata". In questa versione, assumiamo che lo script non contenga spazi (vedi *matchword* altrimenti).

(a) (b)

Figura 5: (a) Codelet della funzione in Python per generare l'Indice di Coincidenza di un corpus. (b) Codelet della funzione in Python per la generazione del modello linguistico in N-grammi da inserire in input al software *AZdecrypt*.

.

Ringraziamenti

Questo lavoro ha beneficiato del supporto di molti studiosi. Ringrazio i miei supervisori di dottorato la Dott.ssa Maria Pia Di Buono e la Prof.ssa Johanna Monti, così come la Prof.ssa Beata Megyesi e la Dott.ssa Carola Dahlke per le preziose critiche relative alle lacune della prima bozza in termini di struttura e contenuto. Ringrazio anche il Dott. Richard Bean e il Dott. Ivan Parisi per gli approfondimenti che mi hanno permesso di apportare cambiamenti sostanziali alla prima versione del documento, in particolare con un'analisi statistica più approfondita. Francesco Pastore e Francesco Afro Di Falco hanno condiviso con me interessanti considerazioni sull'epigrafe, sia dal punto di vista storico che esoterico. Il Prof. Giuseppe Reale, responsabile dell'associazione "Oltre il Chiostro", mi ha fornito dettagliate descrizioni della chiesa di Santa Maria La Nova, nonché concesso l'ingresso gratuito al museo e fotografie digitali dell'iscrizione di alta qualità. Infine, il Dott. Jarl Van Eycke e David Oranchak sono stati molto pazienti e generosi nel mostrarmi come integrare il software AZdecrypt con il corpus storico multilingue necessario per la mia indagine.

Riferimenti bibliografici

1. I. J. Adeigo. *The Carian Language*. Brill, 2006.
2. AZdecrypt. Azdecrypt, 2023. `https://github.com/doranchak/azdecrypt`, Accessed: 2022-11-30.
3. André Bataille. Thèbes gréco-romaine. *Chronique d'Égypte*, 26(52):325–353, 1951.
4. G. B. Bellaso. *Il vero modo di scrivere in cifra con facilita, prestezza et securezza*. Jacobo Britanico, 1564.
5. G. B. Della Porta. *De Furtivis Literarum Notis*. Apud Ioa. Mariam Scotum, 1563.
6. James Felton. FBI Confirms Zodiac Killer's Infamous 340 Cipher Has Been Decoded, And His Message Finally Revealed. IFL Science. `https://www.iflscience.com/fbi-confirms-zodiac-killers-infamous-340-cipher-has-been-decoded-and-his-message-finally-revealed-62044`.
7. Margherita Guarducci. La misteriosa iscrizione medievale Di Pisa, Barga E Lucca. *Rendiconti della Classe di Scienze Morali, Storiche e Filologiche*, 14:216–228, 1959.
8. B. Hauer and G. Kondrak. Decoding anagrammed texts written in an unknown language and script. *Transactions of the Association for Computational Linguistics*, 4:75–86, 2016.
9. HistCorp. Histcorp-historical corpora, 2023. `https://cl.lingfil.uu.se/histcorp/index.html`, Accessed: 2022-10-23.
10. D. A. King. *The Ciphers of the Monks: A Forgotten Number-notation of the Middle Ages*. Franz Steiner Verlag, Wiesbaden, 2001.
11. K. Knight, B. Megyesi, and C. Schaefer. The Copiale cipher. In *4th Workshop on Building and Using Comparable Corpora: Comparable Corpora and the Web BUCC*, pages 12–19, Portland, Oregon, 2011. Association for Computational Linguistics.
12. H. Kranz and W. Oberschelp. *Mechanisches Memorieren und Chiffrieren um 1430, Johannes Fontanas "Tractatus de instrumentis artis memoriae"*. Boethius. Franz Steiner Verlag, 2009.
13. Aloys Meister. *Die Anfänge der moderne diplomatische Geheimschriften: Beiträge zur Geschichte der italienischen kryptographie des XV Jahrhunderts*. Schöningh, 1902.
14. L. Miriello. *Sulla presunta tomba di Dracula a Napoli*. Stamperia del Valentino, 2021.
15. E. Moutafov. Translating encrypted messages: Greek and Slavonic tetragrams as a mixture of languages or as a universal code. *Journal of Software Engineering & Intelligent Systems*, 2006.
16. Cosimo Palma. `https://github.com/Glottocrisio/MariaLaNova`.
17. Cosimo Palma. `https://github.com/Glottocrisio/AZDecryptMariaLaNova`.
18. K. Pommerening. Cryptology Part I: Classic Ciphers (Mathematical Version). *Semantic Scholar*, 2021.
19. Gaetano Rocco. *Il convento e la chiesa di S. Maria la Nova di Napoli nella storia e nell'arte*. Tipografia Pontificia degli Artigianelli, Napoli, 1928.
20. Patricia A. Rosenmeyer. Encrypted inscriptions: a paradoxical practice. In *From Document to History*, pages 373–392. Brill, 2019.
21. Anne-Simone Rous and Martin Mulsow, editors. *Geheime Post-Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Fruhen Neuzeit*, volume 106 of *Historische Forschungen (HF)*. Duncker & Humblot, Berlin, 2015.

22. F. Schöning. *Geheimschrift im deinste der päpstlichen Kurie von ihren Anfängen bis zum Ende des XVI Jahrhunderts*. Nabu Press, 2014.
23. J. W. Somogyi. Caratteristiche strutturali di cifrari monoalfabetici italiani nei secoli xiv e xv. *Verbum–Analecta Neolatina*, 17:195–213, 1906.
24. J. Trithemius. *Polygraphiae libri sex*. apud Ioannem Birckmannum et Wernerum Richwinum, 1518.

Il nuovo framework giuridico cyber dell'Italia. La crittografia come strumento di cybersicurezza e per l'autonomia strategica nazionale

Marcello Albergoni

Agenzia per la Cybersicurezza Nazionale
m.albergoni@acn.gov.it

Sommario Il nuovo framework giuridico cyber dell'Italia pone la crittografia al centro della strategia nazionale per la cybersicurezza e dell'autonomia strategica. L'adozione di tecnologie crittografiche avanzate è essenziale per proteggere le infrastrutture critiche e i dati sensibili, rafforzando al contempo la sovranità digitale dello Stato.

Keywords: Cybersecurity · Sovranità digitale

Evoluzione delle Tecniche di Comunicazione e Implicazioni sulla Sicurezza Informatica

Il 9 marzo scorso, un lancio dell'ANSA ha dato la notizia che, nell'era dei satelliti, i russi – e non solo (vale, infatti, sempre secondo la stessa Agenzia di stampa, anche per i francesi e gli israeliani) – sono tornati all'uso del linguaggio Morse per talune comunicazioni, trasmesse usando tecniche crittografiche.

Il successivo 15 marzo, un altro lancio, questa volta dell'agenzia DIRE, riporta che la password più hackerata del mondo, apparsa 37 milioni di volte nel corso di violazioni di dati è stata "123456" – talora resa opportunamente più sicura (si fa per dire) con l'aggiunta della terzina "789" – seguita da ripetizioni di "1", ovvero di "123". In Italia, poi, le password più usate sarebbero "123456789" (per i più scrupolosi), "Andrea", "admin", o "Francesco". Insomma, una fotografia che, essendo nell'anno 2024, lascia un po' sconfortati sul livello diffuso di (in)consapevolezza nella materia della sicurezza informatica e, allo stesso tempo, rappresenta un forte elemento motivazionale per chi ha, tra i propri compiti istituzionali, quello della diffusione di una cultura della cybersicurezza (c.d. *awareness*) e formazione in materia.

De Cifris Koine – Eruditorum ACTA 2024 –https://doi.org/10.69091/koine/vol-3-E04

Tornando ai numeri, secondo alcune tra le statistiche disponibili in rete, i dati rubati vengono utilizzati per effettuare accessi abusivi nei siti di intrattenimento (per una percentuale vicina al 35%), nei social media (per una percentuale pari al 22% circa), nonché nei portali di e-commerce (per una percentuale vicina al 21%).

Questa breve panoramica, a prescindere dalle specifiche percentuali[1], evidenzia come gli attacchi informatici impattino sul godimento di diritti fondamentali, esercitati attraverso i dati in rete e attraverso quello che potrebbe chiamarsi il nostro *Doppelgänger* digitale.

In una realtà in cui, ormai da anni, attori statali o criminali attuano la politica dell'*harvest now, decrypt later*, il tema della crittografia e dello sviluppo crittografico resistente alle continue evoluzioni tecnologiche (si pensi, fra tutte, al *quantum computing*) è divenuto centrale. Tanto centrale, che ritengo personalmente fondamentale che si debba parlare di *cryptography by design*, quale requisito essenziale per lo sviluppo di piattaforme e sistemi informativi che andranno a gestire e trattare i dati (personali e non) di noi cittadini, delle nostre imprese, dei nostri enti pubblici. Il problema della criminalità informatica, ovvero dell'acquisizione di informazioni – quando non di vere e proprie esfiltrazioni di dati – da parte di attori statali, non riguarda infatti soltanto dati personali, su cui da anni l'attenzione è ai massimi livelli e per la cui tutela esistono strumenti normativi, quali il GDPR, che sono la pietra angolare della disciplina europea (UE) sui dati e le tecnologie digitali [7]. Tali operazioni di violazione della sicurezza dei dati, nelle varie dimensioni della confidenzialità, dell'integrità e della disponibilità[2], possono infatti ben riguardare anche i dati relativi ai patrimoni informativi aziendali, dalle strategie al *know-how* aziendale, dai dati coperti da segreto industriale e oggetto di brevetto, ai dati attinenti all'organizzazione dei sistemi di sicurezza (fisica e non).

Appare, pertanto, di tutta evidenza l'importanza, non solo di usare la crittografia a tutela dei dati (di tutti i dati, personali e non), ma anche delle copie dei dati, occorrendo a volte, infatti, che, nelle operazioni di *back-up*, i dati vengano copiati in chiaro. In tale contesto, non è secondario il ruolo istituzionale giocato dall'ACN.

[1] Per dei numeri con valenza statistica ufficiale dovremo attendere la prima attuazione delle disposizioni di recente introdotte con la legge n. 90 del 2024, che ha previsto che l'Agenzia per la cybersicurezza nazionale (ACN) debba provvedere "alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti" (art. 4). Si tratterà, quindi, come recita il medesimo provvedimento legislativo, di "dati ufficiali di riferimento degli attacchi informatici (...) nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza".

[2] Le si ricorda anche con l'acronimo inglese CIA (*confidentiality, integrity, availability*).

L'Agenzia per la Cybersicurezza Nazionale: Evoluzione Normativa e Implementazione delle Strategie di Crittografia

Autorità governativa di carattere tecnico, come l'ha connotata di recente parte della dottrina [1], l'ACN – il cui ruolo principale è quello di Autorità nazionale per la cybersicurezza – è stata istituita con il decreto-legge 14 giugno 2021, n. 82, a valle di un percorso che ha visto dal 2012 progressivamente disciplinare, da parte del Governo e del Parlamento, il settore della sicurezza e della resilienza cibernetica, anche a tutela della sicurezza nazionale nello spazio cibernetico. L'obiettivo è stato quello di riformare la governance della cybersicurezza, nell'ottica di un approccio olistico alla materia, di una razionalizzazione e di un efficientamento delle risorse e dei livelli di interlocuzione per i diversi soggetti interessati, pubblici e privati, di dotare l'istituenda Agenzia di personale altamente specializzato, di puntare sulla formazione di una forza lavoro parimenti specializzata, di valorizzare l'importanza della diffusione della cultura e degli strumenti di cybersicurezza.

Orbene, il decreto-legge istitutivo dell'ACN è stato arricchito in sede di esame parlamentare per la sua conversione in legge, avvenuta il 4 agosto 2021, prevedendo, con particolare riferimento all'oggetto di questo convegno, che tra le competenze dell'Agenzia, declinate nell'ambito dell'articolo 7, vi fosse anche quella di assumere "le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia [nazionale di cybersicurezza] (...)", nonché di "attiva[re] ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali" (lettera m-bis).

A tale competenza, come si è visto specificamente dedicata alla crittografia, si affianca quella di "supporta[re] negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche", anche al fine di favorire il "trasferimento tecnologico dei risultati della ricerca nel settore".

È proprio nell'ambito dell'esercizio di tali attribuzioni, che la Strategia nazionale di cybersicurezza 2022-2026 [9], tra le 82 misure previste dal suo piano di implementazione, dedica una sezione e due specifiche misure alla "Promozione dell'uso della crittografia"[3]. Nello specifico, si tratta delle misure n. 22 e 23 – il cui soggetto responsabile è stato individuato nella stessa Agenzia – volte, rispettivamente, alla promozione dell'uso della crittografia in ambiti che non riguardano la trattazione di informazioni classificate[4] ("quale impostazione predefinita e comunque fin dalla

[3] La strategia, corredata dal suo piano di implementazione, è stata adottata con il DPCM del 17/05/2022, pubblicato nella G.U. della Repubblica italiana del 1/06/2022 [4].

[4] Si tratta delle informazioni soggette ad una classifica di segretezza ("riservato", "riservatissimo", "segreto", "segretissimo") ai sensi dell'articolo 42 della legge [3].

fase di progettazione di reti, applicazioni e servizi"), e allo sviluppo di tecnologie e sistemi di cifratura nazionale, sempre in ambito "non classificato".

L'impegno strategico continua poi con l'Agenda di Ricerca e Innovazione[5], che dedica la prima delle sei aree di intervento alla sicurezza dei dati e alla privacy e, nella prima sub-area, intitolata "ingegneria della protezione dei dati", fa espresso riferimento all'uso della crittografia omomorfica quale tecnica, fra le altre indicate, per "l'elaborazione *privacy-preserving* dei dati"; mentre nella seconda sub-area, specificamente dedicata alla "crittografia", tratta dell'importanza della "ricerca di nuove primitive, algoritmi e protocolli per Post-Quantum Cryptography (PQC)", dello studio della crittografia quantistica, così come delle soluzioni di crittografia omomorfica (*homomorphic encryption*).

Infine, sono di recente arrivate specifiche disposizioni in materia introdotte nell'ambito dei lavori parlamentari sul disegno di legge di iniziativa del Governo in materia di cybersicurezza (il c.d. DDL cybersicurezza[6]), di recente divenuta la legge 28 giugno 2024, n. 90. Il riferimento è, nello specifico, a quelle disposizioni recate dagli articoli 9 e 10 della richiamata legge. Da un lato, con l'introduzione dell'articolo 9, il legislatore ha voluto imporre – alle strutture di cybersicurezza delle amministrazioni pubbliche destinatarie delle nuove disposizioni e agli enti pubblici e privati inseriti nel perimetro di sicurezza nazionale cibernetica, ovvero tenuti al rispetto della normativa NIS – sia un'attività di verifica (di compliance) dei programmi e delle applicazioni informatiche e di comunicazione elettronica in uso rispetto alle linee guida sulla crittografia, nonché a quelle sulla conservazione delle password, adottate dall'ACN e dal Garante per la protezione dei dati personali, sia un'ulteriore attività volta a verificare che tali programmi e applicazioni non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati. Dall'altro, poi, la materia della crittografia è stata ulteriormente attenzionata e valorizzata in sede parlamentare con la novella della sopra illustrata lettera m-bis) dell'articolo 7 del decreto-legge istitutivo dell'Agenzia, che ora affida all'ACN anche il compito di provvedere "allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici, nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia *blockchain*, come strumento di cybersicurezza". La stessa disposizione, consacrando l'importanza della materia e chiudendo il cerchio normativo sopra delineato, ha infine previsto l'istituzione – presso l'Agenzia stessa – del Centro nazionale di crittografia, chiamato a svolgere le funzioni di *"centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato"*.

[5] Adottata dal Ministero dell'università e della ricerca e dall'Agenzia per la cybersicurezza nazionale il 22 giugno 2023, reperibile sul sito: [8].

[6] DDL recante: "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" [2, 5].

Alla luce di questa panoramica sull'armamentario normativo e strategico in materia, appare ora utile soffermarsi, pur se nella sintesi richiesta, sul come, dal lato dell'ACN, si affrontino e si dia concretezza a quelle sfide, a quelle linee strategiche, a quelle previsioni di legge brevemente passate in rassegna.

Aspetti Finanziari e Organizzativi dell'Agenzia per la Cybersicurezza Nazionale: Ruolo e Competenze in Materia di Crittografia

Sotto un profilo finanziario, l'Agenzia è soggetto attuatore dell'investimento 1.5 del PNRR, dedicato alla cybersicurezza e che prevede un costo totale di 623 milioni di euro, e gestisce i due Fondi previsti nella legge di bilancio 2023 [6], uno "per l'attuazione della Strategia nazionale di cybersicurezza", con una dotazione crescente, dai 70 milioni ai 150 milioni di euro a decorrere dal 2026 e sino al 2037; l'altro con una dotazione, anch'essa crescente, dai 10 milioni ai 70 milioni di euro annui a decorrere dal 2025. Inoltre, l'Agenzia ha una dotazione di bilancio conferitale con il decreto-legge istitutivo, che prevede un finanziamento progressivamente crescente – in ragione del progressivo sviluppo delle proprie capacità e del piano di progressive acquisizioni di professionalità specializzate – sino ad arrivare ai 122 milioni di euro annui a decorrere dal 2027, da cui pure attinge per specifiche progettualità volte al perseguimento dei suoi scopi istituzionali.

Sotto un profilo organizzativo, diverse sono le articolazioni dell'Agenzia che assumono un ruolo nella materia della crittografia. Dal *Servizio programmi industriali, tecnologici, di ricerca e formazione*, al *Servizio certificazione e vigilanza* (nel cui ambito, credo meriti essere evidenziato, sono state immesse anche specifiche professionalità altamente specializzate ed esperte in crittografia), dal *Gabinetto* (in relazione, in particolare, alle attività ed iniziative di natura normativa), al *Servizio regolazione*, per finire con l'attribuzione al Vice Direttore generale di una specifica delega – a testimonianza concreta della particolare attenzione posta su tali attribuzioni istituzionali – per le funzioni dell'Agenzia relative alla consapevolezza e alla formazione sulla cybersicurezza, peraltro ora oggetto della competenza di due Divisioni all'uopo istituite.

Sotto altro profilo, poi, l'ACN ha adottato nello scorso mese di dicembre tre documenti di ausilio e indirizzo, "Le linee guida funzioni crittografiche", che sono dedicati, alle "funzioni di *hash*" (funzioni che, in estrema sintesi, rendono possibile la verifica dell'integrità dei dati), ai "codici di autenticazione dei messaggi (MAC)" (codici che, sempre in sintesi, consentono di garantire l'autenticazione del mittente e l'integrità di un messaggio) e, infine, alla "conservazione delle password" (ponendo in questo caso l'accento sulle misure tecniche per proteggere gli archivi delle password in caso di attacchi e *data breach*). Questo ultimo documento è stato adottato in stretta collaborazione con il Garante per la protezione dei dati personali.

Sinergie Interdisciplinari tra Diritto e Tecnologia

In conclusione, mi sia consentito, vista anche la sede del Convegno (la Facoltà di Giurisprudenza dell'Università di Trento), di dedicare un breve passaggio anche all'attività di promozione, elaborazione e produzione normativa nella materia della sicurezza e della resilienza nello spazio cibernetico, posta in essere dall'Agenzia, sin da quando ha iniziato a muovere i suoi primi passi. Le norme giuridiche, infatti, rappresentano non solo la cornice di legittimità dell'azione dei pubblici poteri e, più in generale, di tutti i soggetti rientranti nel loro ambito applicativo, ma anche la precondizione affinché, legittimamente, si possano adottare comportamenti, atti, provvedimenti che producano efficacemente effetti giuridici e che siano ritenuti meritevoli di tutela da parte dell'ordinamento giuridico. È grazie ad un quadro normativo di riferimento opportunamente congegnato e calibrato, aggiornato o creato, che è, infatti, possibile per una pubblica amministrazione poter legittimamente indirizzare l'azione amministrativa e che, quindi, sono possibili l'adozione e l'attuazione di strategie e progettualità, così come il dispiegamento di azioni proattive o di risposta in caso di incidenti, lo scambio informativo, ovvero l'avvio di collaborazioni e progettualità con soggetti pubblici e privati, con le università e con gli enti di ricerca.

Peraltro, proprio la conferenza organizzata in materia di crittografia, tra storia e diritto, con la presenza di relatori provenienti da diversi ambiti accademici, tanto scientifici quanto umanistici, dimostra l'importanza della commistione tra saperi e consapevolezze, tra diritto e tecnologia, tra storia e matematica.

Riferimenti bibliografici

1. S. Calzolaio. Autorità Indipendenti e di Governo della Società Digitale. In F. Pizzetti, editor, *La Regolazione Europea della Società Digitale*. Giappichelli Editore, 2024. https://iris.uniroma3.it/handle/11590/467707.
2. Camera dei Deputati. Atto Camera 1717, XVIII Legislatura. https://www.camera.it/leg19/126?leg=19&idDocumento=1717.
3. Camera dei deputati e Senato della Repubblica. Legge 3 agosto 2007, n. 124, Articolo 42, 2007. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2007-08-03;124.
4. Presidenza del Consiglio dei Ministri. Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2022 - Adozione della Strategia nazionale di cybersicurezza 2022-2026 e del Piano di implementazione 2022-2026, June 2022. https://www.gazzettaufficiale.it/eli/id/2022/06/01/22A03288/sg.
5. Senato della Repubblica. Atto Senato 1143, XIX Legislatura. https://www.senato.it/leg/19/BGT/Schede/Ddliter/58250.htm.
6. Parlamento della Repubblica Italiana. Legge 29 dicembre 2022, n. 197, Articolo 1, paragrafi 899 et seq., 2022. https://www.gazzettaufficiale.it/eli/id/2023/01/16/23A00141/sg.

7. A. Iannuzzi. Le Fonti del Diritto per la Disciplina della Società Digitale. In F. Pizzetti, editor, *La Regolazione Europea della Società Digitale*, page 10. Giappichelli Editore, 2024. https://iris.uniroma3.it/handle/11590/467707.
8. Agenzia per la Cybersicurezza Nazionale. Agenda di Ricerca e Innovazione per la Cypersicurezza 2023-2026, 2023. https://www.acn.gov.it/portale/agenda-di-ricerca-e-innovazione.
9. Agenzia per la Cybersicurezza Nazionale (ACN). Manuale operativo ad implementazione della misura #82, 2022. https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza.

Human Rights Implications of Encryption Backdoors

Antonino Alì

Università di Trento, Italia
antonino.ali@unitn.it

Sommario This contribution examines the human rights implications of encryption backdoors, focusing on the landmark Podchasov v. Russia case. It analyzes the tension between national security and privacy rights in the digital age, highlighting key international instruments on encryption's role in protecting human rights. It concludes by advocating for a balanced approach that respects both security needs and fundamental rights in our increasingly interconnected world.

Introduction

Historically, intelligence agencies have adopted advanced methods to meet the challenges of modern cryptography. These organisations do not work in isolation, but actively collaborate with various partners, both internal and external, to identify potential threats and overcome the most sophisticated digital defences. There are several key components to this strategy. There is certainly constant investment in cutting-edge technology, with a focus on computing power, which enables them to tackle increasingly complex cryptographic algorithms.

However, the strategy of intelligence services is not limited to mere technological improvement. A crucial aspect is the attempt to influence the global market for commercial cryptography. This approach aims to maintain control and accessibility even in a rapidly changing digital security landscape. Through these methods, intelligence agencies seek to keep pace with the evolution of privacy techniques, balancing the need for national security with the challenges posed by modern cryptographic technologies. This is done through strategic business relationships and international cooperation. At the same time, there is a strong emphasis on developing in-house expertise. Experts in this field collaborate to create innovative approaches to cryptographic analysis. The aim is to stay one step ahead of the most robust cryptographic available technologies[1].

De Cifris Koine – Eruditorum ACTA 2024 –https://doi.org/10.69091/koine/vol-3-E05

[1] See the document "NSA's SIGINT Strategy, 2012-2016" [26]. The strategy contains objectives that underline the NSA's strategic interest in countering the challenges of cryptography to its signal intelligence missions [14, 27].

The question of weakening encryption is a classic dilemma between security and freedom, which has been exacerbated in the digital age. On the one hand, government authorities and law enforcement agencies argue that they need access to encrypted communications to counter national security threats, fight organised crime and protect children from online abuse. On the other hand, cybersecurity experts [1], digital rights advocates and much of the technology industry warn that compromising the integrity of encryption systems would pose far greater risks to collective and individual security. The essence of the dilemma lies in the primary function of robust cryptography: when implemented effectively, it prevents unauthorised access to communications, without distinguishing between malicious parties and government authorities [24].

The use of backdoors in encryption

At a time when digital security is at the centre of public debate, proposals to weaken encryption are gaining increasing attention. These initiatives, which include the introduction of 'backdoors' (a hidden function that bypasses normal security measures and allows unauthorised access to encrypted data) or the requirement for companies to retain decryption keys, aim to create exceptions to the principle of secure digital communications and attempt to strike an often precarious balance between citizens' privacy and the needs of public safety and national security. [2]

[2] The Crypto AG case, revealed in 2020, shows how hardware backdoors are used for large-scale espionage. Operation Rubicon, carried out by the CIA and BND, allowed encryption devices sold by Crypto AG to over 120 countries to be manipulated, allowing intelligence agencies to decipher the secret communications of many governments [22, 18]. Similarly, the case of the Dual_EC_DRBG algorithm, proposed by the NSA for use in the public sector, emerged in 2006. In 2007, two Microsoft researchers discovered that the algorithm could contain a backdoor, potentially allowing those who knew its details to predict its output and compromise the security of encrypted communications. Both cases highlight how backdoors, both hardware and software, can be exploited for large-scale espionage activities, raising serious concerns about the security and privacy of global communications [7]. Moreover, the case of the Clipper chip in the US in the 1990s illustrates well the debate on 'state backdoors' in encryption systems. This chip, developed at the request of government authorities, contained the Skipjack algorithm that allowed access to encrypted data in case of need. Despite the security measures provided, such as a unique serial number and a legal access unit, the project attracted strong criticism. The main concerns were the potential vulnerabilities introduced by the backdoor, the difficulty of implementing such systems securely, and the implications for privacy and data sovereignty. These concerns, combined with a lack of industry acceptance, led to the abandonment of the project. The Clipper chip case highlights the challenges and risks associated with introducing backdoors into security systems, even when requested by government authorities.

The basic idea, which may seem reasonable at first glance, is to allow authorities to access encrypted data by bypassing the encryption itself. However, when you dig deeper, there are critical issues that deserve careful consideration, especially when you consider the potential long-term implications. From a technical perspective, introducing deliberate vulnerabilities into cryptographic systems is a minefield of risks. Strong cryptography, based on mathematical algorithms so complex that even experts' heads spin, makes it virtually impossible to decipher a message without the right key. Weakening these systems, whether by using simpler keys or less secure algorithms, would be like leaving your front door open: not only could the authorities break in, but thieves and attackers could also find their way in.

Implementing secure backdoors is a tricky business, even for the most brilliant cryptographers. If designed with the best of intentions to be accessible only to authorized authorities, these vulnerabilities could still be discovered and exploited by others, creating a veritable digital Pandora's box. It is a thought-provoking paradox: in an attempt to grant access to the relevant authorities, the entire integrity of cryptographic systems may be compromised, exposing millions of users to unpredictable risks. In an increasingly interconnected world, where digital borders are as fluid as water, weakening encryption in a country could have a global impact on digital security. It is like throwing a stone into a pond: the ripples would spread far beyond the initial point of impact. And let us not forget the more sophisticated users, including potential criminals, who could simply jump into another boat, towards alternative encryption solutions and defeating, at least in part, the original purpose of the restrictions. The consequences of such a weakening are not merely technical, but extend like tentacles into the social and economic fabric. Confidence in secure digital communications is the pillar on which entire sectors, from e-commerce to financial services, rest. Compromising this trust would be like removing the foundations of a building: the impact on digital economy may be devastating [8].

The existence of backdoors, even as a possibility, could undermine user confidence in cryptographic systems and create a climate of suspicion and paranoia. The knowledge that private communications can be accessed by government authorities, even in compliance with legal procedures, could discourage the widespread adoption of encryption, much as if people stopped speaking freely for fear of being overheard.

Finally, we must not forget those for whom strong encryption is not a luxury but a vital necessity. Journalists, activists and other vulnerable groups depend on these systems to operate securely, often in contexts where their own safety is at risk. For them, weakening encryption could mean the difference between being able to do their work safely and being exposed to real and tangible dangers.

While authorities' concerns about the misuse of cryptography are understandable, experts believe that the risks of weakening cryptography outweigh the potential benefits. The challenge for the future will be to find a balance that allows legitimate security concerns to be addressed without compromising the fundamental integrity of encryption systems, which are essential for security and privacy in the digital age.

Ultimately, while backdoors appear to be a pragmatic solution to reconcile different needs, their use raises significant concerns about the overall security of systems and user trust, and requires a careful assessment of risks and benefits.

No backdoor for surveillance: ECHR protects encryption

The increasing *normalisation* of electronic surveillance,[3] and the resulting defensive countermeasures, is a phenomenon of great significance in the contemporary digital age [2]. A turning point was the revelations by Edward Snowden in 2013, which brought to light the scope and depth of surveillance activities carried out by American and British intelligence agencies. These revelations set off a chain reaction in both the technology sector and civil society[4]. The widespread adoption of end-to-end (E2E) encryption is an important response to the normalisation of surveillance [16]. Several major companies have implemented this technology for their messaging and video calling services. Some have extended end-to-end encryption to all message exchanges on their platforms, while others enhanced the security of their email services by introducing new features to increase the confidentiality of communications, although metadata generally remains accessible to the platforms.

The trend towards increased security has also led to tensions with government authorities. In the US, for example, the FBI has repeatedly raised concerns about 'going dark', arguing that strong encryption hinders legitimate investigations.[5] This fuelled debates about 'backdoors' in encryption systems, an idea strongly contested by technology companies and privacy activists.

[3] *Normalisation of surveillance* refers to the process of gradual integration of mass surveillance practices into legal and social frameworks. The European Court of Justice has, through a series of rulings, established the legality of 'bulk data collection' under certain conditions, to prevent abuses of power. The legality of such practices has specific requirements, including: clear and accessible legal basis, proportionality and necessity of the measure, independent supervision and procedural safeguards for individual rights. These rulings created a legal framework that, while recognising the potential utility of mass surveillance, seeks to balance it with the protection of citizens' rights [17, 10, 28].

[4] For an overview of cryptography and human rights issues see [25].

[5] The Apple case related to the 2016 San Bernardino massacre highlighted the complex balance between national security and privacy. When the FBI asked Apple to unlock the phone of one of the attackers, the company objected (see [3]). Apple argued that circumventing the encryption on its devices was not only technically impossible, but creating a backdoor would compromise their security. This position reflected Apple's broader concern for user privacy. Although the FBI eventually managed to unlock the phone, the case reignited the debate about government access to strong encryption. This episode showed the ongoing tension between the investigative needs of law enforcement and the need to protect the privacy of users of encrypted technologies, raising crucial questions about the future of digital security and individual rights [23].

The 'Telegram' case

A recent ruling by the European Court of Human Rights raises fundamental questions about the delicate balance between national security and individual rights to privacy and freedom of expression in the digital age. Telegram, an instant messaging application known for its emphasis on privacy and security through encryption, found itself at the centre of a legal dispute with the Federal Security Service of the Russian Federation (FSB).

The conflict arose when the FSB demanded that Telegram provide the data necessary to decrypt the communications of certain users suspected of involvement in terrorist activities. Telegram resisted these requests, claiming that providing such 'encryption keys' would compromise the security and privacy of all users of the application. In response to Telegram's refusal, the Russian authorities imposed fines and ordered the application to be blocked on Russian territory.

The dispute takes place in a complex legal context. The legislation of the Russian Federation, in particular the Information Law and subsequent decrees, imposes significant obligations on Internet communication organisations (ICOs). These include the storage of communications data on Russian territory, the transmission of such data to the competent authorities upon request, and the provision of information necessary for the decryption of encrypted electronic communications. Anton Valeryevich Podchasov, a Telegram user, had filed his application against the Russian Federation with the European Court of Human Rights (ECHR) on 18 June 2019, after exhausting domestic remedies in Russia. This was almost three years before Russia's withdrawal from the Council of Europe and the ECHR. Podchasov, along with 34 other individuals, challenged a disclosure order issued by the Russian Federal Security Service (FSB) requiring Telegram to provide technical information to decrypt the communications of users suspected of terrorist activity. The plaintiffs argued that providing the encryption keys would allow the FSB to decrypt the communications of all Telegram users, thereby violating the right to privacy and confidentiality of communications. Furthermore, they argued that once the FSB obtained the keys, it would be able to access all communications without the judicial authorisation required under Russian law.

On 25 February 2022, the Committee of Ministers of the Council of Europe suspended Russia's right of representation in the organisation, considering the aggression against Ukraine to be a serious breach of its statutory obligations. On 15 March 2022, Russia officially notified the Secretary General of the Council of Europe of its withdrawal from the organisation under Article 7 of the Statute and of its 'intention' to denounce the ECHR. The following day, 16 March 2022, the Committee of Ministers decided to expel Russia with immediate effect, despite its notification of withdrawal.

The expulsion of Russia from the Council of Europe on 16 March 2022, following the invasion of Ukraine, began the process of ending Russia's membership of the ECHR. However, a six-month transitional period was established, from 16 March to 16 September 2022,[6] during which the ECHR retained jurisdiction over cases against Russia relating to events that had occurred by the end of that period. On 5 September 2022, the plenary session of the ECHR formalised this principle, stating that the Court would retain jurisdiction to hear applications against Russia in respect of acts or omissions occurring up to 16 September 2022.[7]

The events at the centre of the Podchasov case, including the adoption of the contested law and the specific actions of the Russian authorities, occurred before 16 September 2022 and thus fall within the temporal jurisdiction of the Court. Both the Russian Government and the applicant had already submitted observations on the case before Russia's withdrawal from the ECHR, enabling the Court to proceed with its assessment.

The 'Yarovaya' Law of the Russian Federation and the obligations of 'Internet Communication Organisers' ICO

In recent years, Russia has made significant changes to its information legislation, with a particular focus on online communications.

In 2014, the Federal Law on Information, Information Technology and Information Protection was substantially amended. It introduced the concept of Internet communications organisations (ICOs), which are broadly defined to include virtually any entity that operates systems or programs for electronic communications over the Internet. The responsibilities imposed on ICOs are considerable and have a profound impact on online privacy. At the heart of the Act are its data retention requirements: ICOs must retain the metadata of user communications for a full year. This metadata includes information such as the time, date and duration of the communications, as well as the parties involved, but not the actual content of the messages. In parallel, the Act requires ICOs to retain the actual content of all communications for six months. This includes text, voice recordings, images and any other type of content exchanged by users.

[6] According to the prevailing interpretation of Article 58 of the Convention, the ECHR continued to apply to Russia for a period of six months after it ceased to be a member of the Council of Europe, thus until 16 September 2022.

[7] See the critical remarks of [5]. The Author points out that this expulsion decision raises some legal questions, as Article 8 of the Council of Europe Statute provides for a specific procedure for expulsion, which does not seem to have been fully respected.

These provisions raise important questions about the protection of privacy and freedom of online communication in Russia.[8] Indeed, the law requires ICOs to provide the authorities with the information necessary to decrypt encrypted communications, essentially requiring them to compromise the security of their systems and hand over decryption keys upon request. The technical implications of the Russian law are significant. ICOs must not only ensure that their equipment meets specific technical requirements set by the government, but also that it facilitates the work of the authorities. In practice, this could mean the integration of surveillance technologies directly into the communications infrastructure. For instant messaging services, the restrictions are even more stringent. In addition to all other requirements, these services must identify their users by their mobile phone numbers. This provision makes anonymous use of such platforms virtually impossible, raising further concerns about privacy and freedom of expression.

As reported, a particularly controversial aspect of the law is the requirement for ICOs to provide decryption keys to authorities on request. This means that in the case of encrypted communications, companies will have to provide the means to decrypt that data, raising serious concerns about user privacy and the overall security of communications systems.

The law has been presented as an anti-terrorism and national security measure aimed at assisting law enforcement and security services in their activities to prevent and investigate crime and terrorism. However, the obligation to provide decryption keys was widely perceived as a direct threat to end-to-end encryption and the confidentiality of private communications. Many industry players found it technically difficult, if not impossible, to comply with the law without compromising the security of the overall communications system. This technical difficulty highlighted the conflict between national security needs and the protection of digital privacy.

It was in this complex context that the Podchasov v. Russia case arose, which led the European Court of Human Rights to assess the compatibility of such measures with the right to privacy guaranteed by the European Convention on Human Rights. This case has become central to the debate on the regulation of encryption and the protection of personal data in the digital age.

[8] See the English text of [9].

The reasoning of the Court

In Podchasov v Russia, the European Court of Justice refers to several international instruments that underline the importance of cryptography in the context of human rights and digital security. These instruments form a coherent framework that highlights the crucial role of cryptography in protecting privacy and freedom of expression in the digital age. The 2022 report of the UN High Commissioner for Human Rights [21] emerges as a key pillar in this discussion.[9] It portrays cryptography not only as a technical tool, but as a real guarantor of fundamental rights. The report emphasises how encryption is essential to allow people to communicate freely, without fear that their information may be intercepted or misused. Particularly relevant is its warning against government restrictions on encryption, highlighting how such measures can have disproportionately negative effects on the entire population.

This view is reinforced by the 2012 Recommendation of the Committee of Ministers of the Council of Europe, which specifically encourages the use of end-to-end encryption in social networking services. This document emphasises the importance of actively protecting the privacy of online users and recognises encryption as a key tool in this endeavour.

[9] See also [15]; in this report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, the fundamental importance of encryption and anonymity in the digital age to ensure human rights, in particular freedom of expression and privacy, is emphasised. The paper highlights how encryption and anonymity provide the necessary security for people to freely express their opinions online without fear of retaliation or surveillance. These tools are considered essential not only for freedom of expression, but also for other rights such as privacy, due process, freedom of peaceful assembly and association, and even the right to life and physical integrity. The report strongly criticises the restrictions imposed by some states on the use of online encryption and anonymity. It points out that such restrictions often fail to meet the criteria of necessity and proportionality required by international human rights law. In particular, practices such as general bans on encryption, the intentional weakening of security standards, cryptographic key deposit systems and the requirement to disclose decryption keys are condemned. The Special Rapporteur recommends that states adopt policies that promote and protect the use of encryption and anonymity, limiting restrictions only to specific cases and on the basis of judicial orders. It emphasises the importance of a transparent public debate on any legislative proposals that would restrict the online security of individuals. The report also calls on international organisations, the private sector and civil society to actively promote the use of secure communication tools. In particular, it urges the UN system to improve its communication practices to ensure the safety of those interacting with the organisation. Finally, the document emphasises the importance of educating the public on the use of these digital security tools. The Special Rapporteur encourages states, civil society organisations and companies to engage in campaigns to promote the widespread adoption of encryption and provide the necessary tools for those at risk to securely exercise their right to freedom of opinion and expression. See also [6].

The 2015 Resolution of the Parliamentary Assembly of the Council of Europe adds a further dimension to this debate, expressing concern about the practices of some intelligence services that seek to create or exploit weaknesses in security systems. The resolution highlights the risks associated with weakening encryption, not only for individual privacy, but also for collective security against threats such as terrorism and cybercrime [4].

The Court also cites some well-known rulings of the Court of Justice of the European Union on the protection of privacy in electronic communications [19, 20]. These decisions emphasise that generalised access to the content of electronic communications is incompatible with the fundamental rights guaranteed by the EU Charter of Fundamental Rights. The 2016 Joint Statement of Europol and ENISA offers a practical perspective, recognising the need to balance investigative needs with privacy protection [12, 13]. This document advises against the introduction of mandatory backdoors or key escrow systems, emphasising how such measures can weaken overall security and be easily circumvented by criminals. Finally, the recent joint EDPB-EDPS Opinion of 2022 further reinforces the importance of encryption, warning against measures that could discourage its use [11]. This opinion emphasises how the weakening of encryption could have negative effects not only on privacy, but also on freedom of expression and digital innovation.

Overall, these instruments express a consensus on the importance of cryptography as an essential tool for the protection of human rights in the digital age. They emphasise the need for a balanced approach that respects both public security needs and the fundamental rights of citizens, and highlight the risks associated with policies that could weaken encryption. These references also show how the Court based its decision on a wide range of international sources, recognising the importance of encryption and the protection of privacy in today's digital context.

Data retention measures and the obligation to provide decryption keys

The Court found that the law violated Article 8 of the European Convention on Human Rights, which protects the right to privacy and correspondence, on three main grounds. The indiscriminate retention of data on all internet users is an "exceptionally wide and serious interference" with privacy. Adequate safeguards against abuse of data access by authorities are lacking. The obligation to decrypt end-to-end encrypted communications is disproportionate. In particular, the Court stressed that weakening encryption for all users in order to allow access by the authorities would 'seriously compromise the security of electronic communications of all users'.

This ruling is a significant victory for digital privacy, establishing that strong encryption is essential to protect fundamental rights in the digital age. The Court recognised that there are alternative methods of investigation that are less intrusive.

The issue of bulk collection of data is closely linked to the issue of encryption in Podchasov v Russia. The European Court of Human Rights recognised that the data retention measures and the obligation to provide decryption keys under Russian law constitute a de facto form of mass surveillance. Encryption, especially end-to-end encryption, is seen as a crucial defence against indiscriminate surveillance. Forcing service providers to weaken encryption or provide backdoors is tantamount to enabling mass surveillance on a large scale, compromising the privacy of all users, not just those under investigation.

The Court stressed that the indiscriminate retention of data and potential access to all encrypted communications constituted an overbroad and serious interference with the private life of individuals. This approach was considered disproportionate to the legitimate objectives of national security and crime prevention. In paragraph 70, the Court highlights the extent and gravity of the interference caused by the challenged legislation. The law provides for the automatic and continuous retention of the content of all Internet communications for six months and of related data for one year. The Court emphasises that this measure affects all users of Internet communications, irrespective of any suspicion of criminal activity, and covers the content of all communications without any limitation in terms of territorial or temporal scope or categories of persons. In paragraph 77, the Court addresses the problem of the weakening of encryption. It stresses that in order to decrypt communications protected by end-to-end encryption, such as those of Telegram, it would be necessary to weaken the encryption for all users. This cannot be limited to certain individuals and would affect everyone indiscriminately. The Court concludes that weakening encryption by creating 'backdoors' would make routine, general and indiscriminate surveillance of personal electronic communications technically possible and would seriously undermine the security of all users.

Conclusions

The decision of the European Court of Human Rights (ECHR) in Podchasov v. Russia has indeed set an important precedent for the debate on digital privacy and national security in Europe. In this case, the ECHR condemned Russia for violating the European Convention on Human Rights through its surveillance activities and failure to protect digital privacy.

This ruling has several important implications. It reaffirms the primacy of human rights and freedom of communication over national security concerns and calls on Council of Europe member states to protect these rights even when operating in the security sphere. The key role of strong cryptography in protecting privacy and digital security is clearly recognised, sending a clear message against legislative trends that aim to weaken cryptographic systems.

The Court stresses the importance of striking a balance between national security needs and respect for fundamental rights. It urges states to adopt proportionate and targeted approaches in the fight against crime and terrorism and discourages the use of generalised forms of surveillance that violate the rights to privacy and freedom of communication. This judgment marks a turning point in the protection of digital rights in Europe and provides a solid legal basis for future developments in technology and legislation.

Riferimenti bibliografici

1. H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, and D. J. Weitzner. Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communication. In *Enigma 2016*. USENIX Association, 2016. `https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf?ref=hackernoon.com`.
2. A. Alì. La sorveglianza elettronica su vasta scala per finalità di intelligence nella giurisprudenza della Corte europea dei diritti dell'uomo. *La Comunità Internationale*, 1:101–115, 2022.
3. Apple. Customer letter, February 2016. `https://www.apple.com/customer-letter/`.
4. Parliamentary Assembly. Resolution 2045 (2015), 2015. `https://pace.coe.int/files/21692/pdf`.
5. L. Borlini. L'espulsione della federazione russa dal Consiglio d'Europa e le conseguenze giuridiche della cessazione della qualità di membro. *Rivista di Diritto Internazionale*, 1:37–76, 2023.
6. UCI Law International Justice Clinic. Selected References: Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression, 2015. `https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf`.
7. C. Comella. Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza Safe Harbor della Corte di giustizia dell'Unione Europea. In G. Resta and Z. Zencovich, editors, *La protezione transnazionale dei dati personali. Dai "safe harbour princples" al "privacy shield"*, pages 49–71. Romatre-Press, Rome, 2016.
8. K. W. Dam and H. S. Lin. Cryptography's Role in Securing the Information Society. *National Academy Press*, 1996. `https://nap.nationalacademies.org/read/5131/chapter/1`.
9. State Duma and Federation Council. Federal Law No. 149-FZ of 27 July 2006 on Information, Information Technology and Protection of Information (as amended), July 2006. `https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru126en.pdf`.
10. Grand Chamber European Court of Human Rights. Big Brother Watch and Others v. The United Kingdom, 2021. `https://hudoc.echr.coe.int/fre?i=001-210077`.
11. European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). Joint Opinion on the Regulation of the European Parliament and of the

Council on Addressing the Dissemination of Terrorist Content Online, July 2022. https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf.
12. European Union Agency for Cybersecurity (ENISA). On Lawful Criminal Investigation that Respects 21st Century Data Protection, 2016. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection.
13. Europol. On Lawful Criminal Investigation Respecting 21st Century Data Protection, 2016. https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century_data_protection_1.pdf.
14. David P. Fidler, editor. *The Snowden Reader*. Indiana University Press, Bloomington, IN, 2015.
15. D. Kaye. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. *Human Rights Council, Twenty-ninth Session*, 2015. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/HRC/35/22&Lang=E.
16. R. Lakra. Cracking the Code: How Podchasov v. Russia Upholds Encryption and Reshapes Surveillance. *EJIL: Talk*, March 2024. https://www.ejiltalk.org/cracking-the-code-how-podchasov-v-russia-upholds-encryption-and-reshapes-surveillance/.
17. M. Milanovich. The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa. *EJIL: Talk!*, 2021. https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.
18. G. Miller. How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades. *Washington Post*, February 2020. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.
19. Court of Justice of the European Union. Judgment of the Court of Justice of the European Union in the Joined Cases of Digital Rights Ireland and Seitlinger and Others. case C-293/12 and C-594/12 (EU:C:2014:238), 2014.
20. Court of Justice of the European Union. Judgment of the Court of Justice of the European Union in the Case of Maximillian Schrems v. Data Protection Commissioner. case C-362/14 (EU:C:2015:650), 2015.
21. Office of the United Nations High Commissioner for Human Rights. The Right to Privacy in the Digital Age. *Human Rights Council, Fifty-first Session*, 2022. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/HRC/51/17&Lang=E.
22. Parliament of the Swiss Confederation. Affaire Crypto AG: Rapport de la Délégation des Commissions de gestion des Chambres fédérales, November 2020. https://www.parlament.ch/centers/documents/fr/bericht-gpdel-2020-11-10-f.pdf.
23. M. Sala. La Crittografia al centro dello scontro tra Apple ed FBI. *Gnosis*, 2:139–143, 2015. https://gnosis.aisi.gov.it/Gnosis/rivista47.nsf/servnavig/47-39.pdf/$File/47-39.pdf?OpenElement.
24. B. Schneier. The Value of Encryption. The Ripon Forum, 2016. https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.htm.

25. W. Schulz and J. van Hoboken, editors. *Human Rights and Encryption.* UNESCO Internet Freedom Series. UNESCO Publishing, 2016. https://www.hiig.de/wp-content/uploads/2016/12/246527E.pdf.
26. New York Times. A Strategy for Surveillance Powers, 2013. https://archive.nytimes.com/www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html.
27. U.S. House of Representatives. Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. Technical report, U.S. Government Printing Office, 2016. https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf.
28. E. Watt. *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law.* Edward Elgar Publishing, Cheltenham, 2021.

Ringraziamenti

Vogliamo ringraziare tutti i volontari e collaboratori di De Cifris, fondamentali per la pubblicazione di questo Volume.

In particolare, ringraziamo il Tesoriere dell'Associazione Elisa Cermignani, nonché i volontari Elena Broggini, Leonardo Errati, Naima Noukti.

L'uso di fotoriproduzioni di documenti conservati dall'Archivio di Stato di Venezia è stato concesso con suo Nulla Osta dal protocollo ASVe 3269/2024.