

NUOVA **ANTOLOGIA** 
MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

N. 6
2025

Fascicolo 22. Aprile 2025
Storia Militare Antica e Bizantina (6)

a cura di
MARCO BETTALLI, ELENA FRANCHI E GIOACCHINO STRANO



Società Italiana di Storia Militare

Direttore scientifico Virgilio Ilari
Vicedirettore scientifico Giovanni Brizzi
Direttore responsabile Gregory Claude Alegi
Redazione Viviana Castelli

Consiglio Scientifico. Presidente: Massimo De Leonardis.

Membri stranieri: Jeremy Armstrong, Christopher Bassford, Floribert Baudet, Stathis Birthacas, Jeremy Martin Black, Loretana de Libero, Magdalena de Pazzis Pi Corrales, Tadeusz Grabarczyk, Gregory Hanlon, John Hattendorf, Rotem Kowner, Yann Le Bohec, Aleksei Nikolaevič Lobin, Prof. Armando Marques Guedes, Prof. Dennis Showalter (†). *Membri italiani:* Livio Antonielli, Marco Bettalli, Antonello Folco Biagini, Aldino Bondesan, Giampiero Brunelli, Franco Cardini, Piero Cimbolli Spagnesi, Alessandra Dattero, Piero del Negro, Giuseppe De Vergottini, Carlo Galli, Marco Gemignani, Maria Intriери, Roberta Ivaldi, Nicola Labanca, Luigi Loreto, Gian Enrico Rusconi, Carla Sodini, Gioacchino Strano, Donato Tamblé.

Comitato consultivo sulle scienze militari e gli studi di strategia, intelligence e geopolitica: Lucio Caracciolo, Flavio Carbone, Basilio Di Martino, Antulio Joseph Echevarria II, Carlo Jean, Gianfranco Linzi, Edward N. Luttwak, Matteo Paesano, Ferdinando Sanfelice di Monteforte.

Consulenti di aree scientifiche interdisciplinari: Donato Tamblé (Archival Sciences), Piero Cimbolli Spagnesi (Architecture and Engineering), Immacolata Eramo (Philology of Military Treatises), Simonetta Conti (Historical Geo-Cartography), Lucio Caracciolo (Geopolitics), Jeremy Martin Black (Global Military History), Elisabetta Fiocchi Malaspina (History of International Law of War), Gianfranco Linzi (Intelligence), Elena Franchi (Memory Studies and Anthropology of Conflicts), Virgilio Ilari (Military Bibliography), Luigi Loreto (Military Historiography), Basilio Di Martino (Military Technology and Air Studies), John Brewster Hattendorf (Naval History and Maritime Studies), Elina Gugliuzzo (Public History), Vincenzo Lavenia (War and Religion), Angela Teja (War and Sport), Stefano Pisu (War Cinema), Giuseppe Della Torre (War Economics).

Nuova Antologia Militare

Rivista interdisciplinare della Società Italiana di Storia Militare
Periodico telematico open-access annuale (www.nam-sism.org)
Registrazione del Tribunale Ordinario di Roma n. 06 del 30 Gennaio 2020
Scopus List of Accepted Titles October 2022 (No. 597)
Rivista scientifica ANVUR (5/9/2023) Area 11



Direzione, Via Bosco degli Arvali 24, 00148 Roma
Contatti: direzione@nam-sigm.org ; virgilio.ilari@gmail.com

©Authors hold the copyright of their own articles.

For the Journal: © Società Italiana di Storia Militare
(www.societaitalianastoriamilitare@org)

Grafica: Nadir Media Srl - Via Giuseppe Veronese, 22 - 00146 Roma
info@nadirmedia.it

Gruppo Editoriale Tab Srl -Viale Manzoni 24/c - 00185 Roma
www.tabedizioni.it

ISSN: 2704-9795

ISBN Fascicolo 979-12-5669-126-5

NUOVA **ANTOLOGIA** 
MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

N. 6
2025

Fascicolo 22. Aprile 2025
Storia Militare Antica e Bizantina (6)

a cura di
MARCO BETTALLI, ELENA FRANCHI E GIOACCHINO STRANO



Società Italiana di Storia Militare

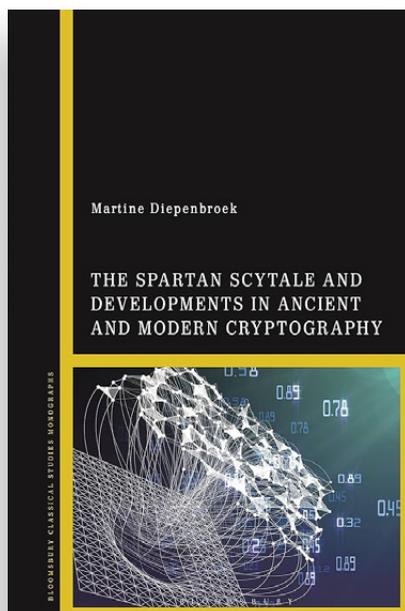


Bronze statue (2nd/3rd century AD) of the genius of a legion.
Enns (Upper Austria). Museum Lauriacum.
Foto 20912 Wolfgang Sauber, GNU Free Documentation License
Wikimedia Commons

MARTINE DIEPENBROEK

The Spartan Scytale
and Developments in Ancient and Modern Cryptography

Bloomsbury Academic, London, New York, Dublin, 2024



L'Autrice, una studiosa olandese, ha pubblicato negli ultimi anni numerosi saggi, compresa la sua tesi di dottorato presso l'Università di Bristol, riguardanti la scitala o scitale (greco σκυτάλη) impiegata nell'antica Sparta per trasmettere dispacci cifrati. Questo libro può considerarsi un compendio delle precedenti pubblicazioni.

La scitala crittografica è costituita da un bastone intorno al quale si avvolge a spirale un nastro di papiro, di pergamena o di pelle, scrivendo poi il messaggio da trasmettere su più righe, con il bastone tenuto in posizione orizzontale. Il nastro staccato dal bastone contiene il messaggio cifrato, poiché per esempio, nel caso

del messaggio in chiaro contenuto in due sole righe, alla prima lettera del testo in chiaro segue sul nastro la lettera del rigo inferiore e così via per le lettere successive. Il destinatario della striscia deve disporre di un bastone con diametro uguale a quello del mittente, nel caso in cui siano cilindrici, intorno a cui riavvolgere la striscia per poter leggere, riga per riga, il messaggio in chiaro. Una maggiore segretezza potrebbe ottenersi scrivendo le lettere sui bordi tra una striscia e l'altra. Questo metodo è ritenuto dai più noti autori di storia della Crittologia ed è comunemente riconosciuto come il primo esempio di "cifatura a trasposizione" in cui le lettere o i numeri di un messaggio in chiaro vengono spostate secondo regole e secondo chiave concordate tra mittente e destinatario. Nel caso della scitola la forma e la dimensione dei due bastoni rappresentano la chiave.

La cifatura con scitola si trova descritta nelle Vite di Plutarco (Vite di Lisandro di Artaserse e di Agesilao) del II secolo d.C. e poi anche nelle Notti Attiche di Aurelio Gellio che fanno riferimento a fatti accaduti circa 700 anni prima, cioè tra la fine del V e l'inizio del IV secolo d.C. Più precisamente allo scambio di messaggi tra gli Efori spartani e i loro Generali operanti sul campo, dall'inizio della Guerra del Peloponneso (431 a.C.). Tra le fonti anteriori a Plutarco, l'Autrice cita Tuciddide in relazione alla "scitola" inviata dagli Efori a Pausania dopo la conquista di Bisanzio (471 a.C.) per invitarlo a tornare immediatamente a Sparta ove era accusato di tradimento, senza però specificare se il messaggio fosse cifrato. Altri autori della Grecia antica, come il commediografo Aristofane e il Poeta Pindaro menzionano la scitola intesa come messaggio, anche se mancano chiari riferimenti alla cifatura.

L'Autrice considera inoltre l'impiego della scitola come coerente con l'evoluzione della natura delle guerre combattute dai Greci e soprattutto dagli Spartani, divenute sempre più vaste e complesse nel corso dell'evoluzione dal mondo arcaico a quello classico, richiedendo quindi l'invio di dispacci a grandi distanze. Parallelamente, l'impiego della scitola sarebbe cambiato da semplice mezzo di riconoscimento personale al sistema di cifatura descritto da Plutarco. D'altra parte, scitola significa "bastone", termine polisemico che può indicare, come si è accennato, anche il distintivo dei messaggeri e l'antico equivalente greco della "piastrina" di identificazione dei caduti in battaglia (per gli opliti si trattava infatti di un bastoncino con inciso il proprio nome). Abbondano altre accezioni del termine: da serpente a fallo.

Anche per la confusione che ne deriva, alcuni studiosi moderni hanno avanzato dubbi sul racconto di Plutarco, cioè sull'effettivo impiego del metodo di cifratura nella Grecia del V e del IV secolo a.C. Secondo diverse ipotesi, il bastone avrebbe potuto contenere il messaggio in chiaro sovrascritto o nascosto all'interno. In quest'ultimo caso si tratterebbe di un esempio di steganografia (comunicazioni celate come quelle con inchiostri simpatici), largamente impiegata dai popoli antichi compresi i Greci e i Romani. C'è inoltre chi attribuisce l'invenzione della scytala crittografica allo stesso Plutarco o addirittura ad Archimede, senza che vi sia alcuna prova in tal senso. I dubbi o la negazione dell'impiego della scytala crittografica nel V e nel IV secolo a. C., sarebbero avvalorati dal racconto di Enea il Tattico nel libro dedicato ai metodi per la resistenza negli assedi. Questo Autore, vissuto probabilmente nel IV secolo a.C., non cita la scytala, persino nel capitolo dedicato ai sistemi per comunicare al di là delle mura delle città assediate.

Diepenbroek giustifica invece tale mancanza, sostenendo che Enea il Tattico, interessato più ai sistemi di steganografia che a quelli di crittografia, avrebbe trattato esclusivamente le comunicazioni a breve distanza, mentre il sistema crittografico della scytala è idoneo a inviare messaggi a distanze maggiori, argomentazione questa non del tutto condivisibile. L'Autrice contesta inoltre l'argomento della pretesa rozzezza degli Spartani del V secolo a. C. sostenuta dagli Ateniesi che li definivano illetterati e sostiene invece la capacità almeno delle classi più elevate di saper scrivere e interpretare brevi messaggi come quelli delle scytale. Comunque, anche nel caso in cui la scytala crittografica sia stata inventata nel II secolo a.C., non si può non riconoscere, d'accordo con l'Autrice, il suo valore crittografico come primo metodo noto di cifratura a trasposizione.

Un capitolo del libro è dedicato alla descrizione dei sistemi di comunicazioni nascoste o cifrate della



Una ipotetica ricostruzione della scytala (Wikimedia Commons)

Roma antica, ponendo in evidenza la tendenza dei Romani a impiegare la Steganografia, senza quindi aver mai usata la scitala. Si descrive poi l'alfabeto di Cesare, uno dei primi esempi di "cifatura a sostituzione" monoalfabetica, in cui ogni lettera dell'alfabeto nel messaggio in chiaro viene sostituita da una lettera di un altro alfabeto, secondo una regola predefinita. Svetonio racconta come il Condottiero romano usasse nei suoi dispacci sostituire le lettere dell'alfabeto con quelle dello stesso alfabeto spostate di tre posizioni. Ovviamente sarebbe stato possibile variare la chiave di cifatura, pari in questo caso a 3, ma non sembra che Cesare l'abbia mai cambiata. L'Autrice si rammarica per la grande popolarità dell'alfabeto di Cesare tra gli storici della crittografia, a differenza di quanto accade per la scitala che sarebbe negletta o considerata poco più di un giuochino, mentre in effetti offrirebbe una maggiore segretezza rispetto a una lettera cifrata con un semplice alfabeto a sostituzione.

Nel descrivere i metodi crittografici ideati nel Rinascimento, Diepenbroek cerca di dimostrare la loro analogia con la scitala. Come è noto, sia il disco di Leon Battista Alberti, sia la *tabula recta* di Tritemio, come la tabella di Giovan Battista Bellaso, sono esempi di sostituzione polialfabetica di cui il primo, in assoluto, è il metodo ideato dall'Alberti. Le similitudini con la scitala ricercate dall'Autrice appaiono quanto meno forzate e non possono che limitarsi a caratteristiche comuni a tutti i metodi di cifatura privata, come il possesso della chiave e dello strumento cifrante/decifrante - per esempio un uguale disco ovvero un uguale bastone nel caso della scitala - da parte dei due corrispondenti.

Uno sforzo analogo è erogato per dimostrare l'analogia con i sistemi crittografici ideati dal 1800 in poi, anche se la gran parte di quelli presi in considerazione sono del tipo a sostituzione polialfabetica. Particolare attenzione è rivolta ai sistemi meccanici a dischi, descrivendo in dettaglio il funzionamento del primo esempio costituito dal "cilindro di Jefferson" ideato alla fine del XVIII secolo e reiventato in diverse versioni fino alla Seconda Guerra Mondiale. La forma cilindrica del dispositivo e la scrittura di un alfabeto sul bordo di ciascuno dei dischetti forati e montati in sequenza predefinita su un asse centrale, rendono probabilmente il cilindro di Jefferson in qualche modo assimilabile alla scitala. Tuttavia, anche i cilindri a dischi sono basati sulla sostituzione del messaggio in chiaro, composto dal mittente in sequenza, lettera per lettera, su ciascun disco, mentre il messaggio cifrato viene letto su un'altra riga del cilindro. Il ricevente deve comporre sul suo dispositivo le lettere del cifrato in sequenza e ricercare sulle altre righe un

insieme di lettere che abbia un senso compiuto. Anche la maggior parte degli altri esempi di cifrari menzionati per le analogie con la scitale, come il “cifrario di Vigenère” o le versioni moderne del “quadrato di Polibio” non sono a trasposizione. Fa eccezione il cifrario ADFGVX usato dall’Esercito tedesco verso la fine della Grande Guerra, in cui ad una prima cifratura effettuata con un quadrato di Polibio in cui le suddette lettere vengono disposte sulla prima riga e sulla prima colonna, segue una trasposizione per colonne con chiave. L’Autrice spiega, tra l’altro, il metodo descritto dal Bauer per decrittare i messaggi con cifre a trasposizione, forse per rappresentare le difficoltà di questa operazione. Insomma, il paragone tra la scitale e altri metodi crittografici appare, a giudizio di chi scrive, quanto meno inessenziale.

Per chiarire questo giudizio, si ricorda che il primo cifrario noto - detto cifrario di Atbash - risale al Libro del profeta Geremia, attivo nel VII secolo a. C., e adopera il metodo di sostituzione in cui la prima lettera dell’alfabeto ebraico viene sostituita con l’ultima, la seconda con la penultima e così via. La sostituzione monoalfabetica reinventata da Cesare ha dominato, in varie forme, le comunicazioni cifrate per più di un millennio, anche dopo l’invenzione del metodo delle frequenze da parte dei crittoanalisti arabi del X secolo d.C. Poi, l’ideazione della sostituzione polialfabetica nel Rinascimento ha esteso fino a tempi recenti la validità del metodo sostitutivo. Questo è il semplice motivo della “popolarità” goduta dalla cifratura a sostituzione tra gli storici della crittografia. Invece, dopo la scitale, non sembra che altri cifrari a trasposizione siano stati impiegati diffusamente, fino alla fine del XVIII secolo, quando sono comparse le trasposizioni per colonne, semplici, doppie, con chiave, ecc. e le prime griglie quadrate a rotazione. Questi metodi hanno trovato largo impiego sui campi di battaglia della Grande Guerra e in parte anche della Seconda Guerra Mondiale. Le macchine cifranti/decifranti elettromeccaniche, come Enigma, fondate su sostituzioni polialfabetiche multiple, hanno progressivamente sostituito i metodi di cifratura con carta e matita, compresi quelli a trasposizione, a partire dal decennio 1920 -30 fino all’avvento dei computer. Le notevoli capacità di memoria di questi ultimi consentono oggi di gestire notevoli quantità di dati e di implementare metodi complessi di cifratura comprendenti sostituzioni e trasposizioni multiple di sequenze di dati, come avviene nel Advanced Encryption Standard (AES), giustamente citato dall’Autrice.

Edited by
Andriana Domouzi & Silvio Bär

ARTIFICIAL INTELLIGENCE
IN GREEK AND ROMAN EPIC

BLOOMSBURY CLASSICAL STUDIES MONOGRAPHS



BLOOMSBURY



Cristo appare a San Mercurio e a Santa Caterina di Alessandria nell'atto di calpestare Giuliano l'Apostata la cui morte, supplicata da San Basilio difronte ad un'icona di San Mercurio, fu attribuita all'intercessione del santo. Icona del laboratorio di Georgios Klontzas, Creta, ca 1560/70.

Yale University Art Gallery, ID 255. Connecticut, U. S. Wikimedia Commons

Storia Militare Antica e Bizantina (6)

A Bibliographical Survey

- *Present and Past Approaches to the Ancient Military History. A Short Bibliographical Survey of the Current Studies,*
di VIRGILIO ILARI

STORIA GRECA

- *The dog barks around the hedgehog Reassessing the κόκλος in ancient naval warfare,*
by ALESSANDRO CARLI
- *Tra guerra e politica il caso dei mille logades di Argo,*
di ALESSANDRO BRAMBILLA

STORIA ROMANA

- *Early Roman Cavalry in Combat (6th – 3rd centuries BCE),*
by J. ARMSTRONG and G. NOTARI
- *The republican legionary cohort once again tactical reform in the Roman republic,*
by GABRIELE BRUSA

Insight

- ‘La giornata di Zama’.
Note in margine alla recente edizione di un saggio militare di Francesco Algarotti
di DENISE ARICÒ

- *L'importanza delle materie prime nella grand strategy romana*
di ALESSANDRO GIRAUDO

Articoli / Articles

- *Le nombre l'identité et l'origine des légions du Bellum Africum,*
par BATISTE GÉRARDIN
- *Autour de la bataille de Thapsus*
par OUIZA AIT AMARA
- *Le ballistae, i ballistarii delle legioni e le legioni di Ballistarii,*
di MAURIZIO COLOMBO
- *Riflessioni sulle componenti tecniche e sull'uso tattico della ballista quadritrotis e del tichodifrus (De rebus bellicis 7-8)*
di FRANCESCO FIORUCCI

STORIA BIZANTINA

- *L'imperatore e la guerra. Eraclio e la “guerra santa”.*
di FRANCESCO MORACA
- *Le facteur scythe dans la ‘dernière grande guerre de l’Antiquité’*
par GUILLAUME SARTOR
- *Magyar ‘raids’ and Frankish invasions: A new perspective*
by CHRISTOPHER SZABÓ
- *The Enseignements of Theodore Palaiologos*
by JÜRIG GASSMANN

Recensioni / Reviews

- LUCIANO CANFORA, *La grande guerra del Peloponneso, 447-394 a.C.*
(di ALESSANDRO CARLI)
- JOHN NASH, *Rulers of the Sea Maritime Strategy and Sea Power in Ancient Greece, 550 – 321 BCE*
(di VITTORIO CISNETTI)
- MARTINE DIEPENBROEK, *The Spartan Scytale and Developments in Ancient and Modern Cryptography*
(di COSMO COLAVITO)
- JEREMY ARMSTRONG, *War and Society in Early Rome From*

- Warlords to Generals*
(di GIANLUCA NOTARI)
- CHRISTOPHE BURGEON, *Hannibal. L'ennemi de Rome*
(di GIOVANNI ZAMPROGNO)
- ELIZABETH H. PEARSON, *Exploring the Mid-Republican Origins of Roman Military Administration*
(by GABRIELE BRUSA)
- ALAIN DEYBER, *La bataille d'Orange. Rome en péril – 6 octobre 105 avant J.-C.*
(di GABRIELE BRUSA)
- LUCIA FLORIDI, *Voci e Silenzi di Briseide. Da Omero a Pat Barker*
(di FABIANA ROSACI)

- FRANCESCO FIORUCCI (cur.), *La Scienza Militare Antica. Autori opere e la loro fortuna*
(di ALESSANDRO CARLI)
- ELENA SANTAGATI, *Filone di Bisanzio, Μηχανική Σύνταξις*
(di FRANCESCO FIORUCCI)
- GEORGIOS THEOTOKIS, *The campaign and battle of Manzikert, 1071*
(EFSTRATIA SYGKELLOU)
- LUCA LOSCHIAVO (cur.), *The Civilian Legacy of the Roman Army*
(LUIGI CAPOGROSSI)