

# Crittografia

Da Wikipedia, l'enciclopedia libera.

La **crittografia** (o **criptografia**, dal greco κρυπτός [*kryptós*], "nascosto", e γραφία [*graphía*], "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio non comprensibile/intelligibile a persone non autorizzate a leggerlo, garantendo così, in chiave moderna, il requisito di confidenzialità o riservatezza tipico della sicurezza informatica. Un tale messaggio si chiama comunemente *crittogramma* e i metodi usati sono detti *tecniche di cifratura*.

## Indice

### Storia

### Descrizione

Crittografia simmetrica

Crittografia asimmetrica

Crittografia quantistica

### Applicazioni

Software crittografici

Librerie crittografiche

### Aspetti legali

### Note

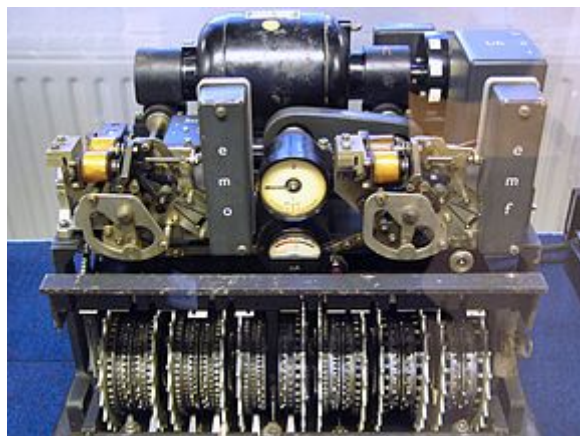
### Bibliografia

### Filmografia

### Voci correlate

### Altri progetti

### Collegamenti esterni



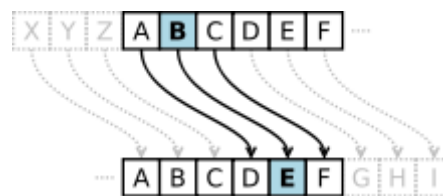
La cifratrice tedesca Lorenz, macchina utilizzata dai nazisti nella seconda guerra mondiale per crittografare le comunicazioni tra le gerarchie militari più elevate.

## Storia

Si hanno tracce di cifrari antichi utilizzate dagli Ebrei nel codice di atbash; gli Spartani avevano un loro particolare sistema di comunicazione dei messaggi segreti, la scitala; a Gaio Giulio Cesare si attribuisce l'uso del cosiddetto cifrario di Cesare, un sistema crittografico.

La storia della crittografia moderna inizia con la stesura del *De cifris* di Leon Battista Alberti, che per primo insegnò a cifrare per mezzo di un disco cifrante con un alfabeto segreto da spostare *ad libitum* ogni due o tre parole. Anche il tedesco Tritemio prevede una forma di cifratura polialfabetica, facendo scorrere l'alfabeto ordinato di un posto a ogni lettera del *chiaro* (come si definisce in gergo il testo non criptato). Nel 1526 Jacopo Silvestri pubblicò l'*Opus novum*, considerata una delle prime opere su questo argomento. Ma il vero progresso nella cifratura polialfabetica è stato compiuto dal bresciano Giovan Battista Bellaso, che ha inventato la tecnica di alternare alcuni alfabeti segreti formati con parola chiave sotto il controllo di un

lungo versetto chiamato contrassegno. La sua prima tavola a 11 alfabeti reciproci, uscita nel 1553, fu ripubblicata dal napoletano Giovanni Battista Della Porta dieci anni più tardi e ne prese il nome grazie alla notevole diffusione che ebbe il suo trattato *De furtivis literarum notis*.



Il cifrario di Cesare

Il francese Vigenère utilizzò poi il versetto per cifrare ciascuna lettera con la sua tavola ad alfabeti regolari identica a quella del Tritemio e che oggi porta il suo nome. Il suo sistema è stato considerato indecifrabile per tre secoli, finché nel 1863 il colonnello prussiano Friedrich Kasiski pubblicò un metodo per "forzarlo", chiamato Esame Kasiski. Qualsiasi sia il sistema crittografico utilizzato, la legge fondamentale sul corretto uso di tali tecniche fu scritta da Kerckhoffs ("Legge di Kerckhoffs") nel suo libro del 1883 *La Cryptographie Militaire* e di seguito riportata: «La sicurezza di un crittosistema non deve dipendere dal tener celato il crittoalgoritmo. La sicurezza dipenderà solo dal tener celata la chiave.» Nel 1918 Gilbert Vernam maggiore dell'esercito statunitense e tecnico all'AT&T Bell, perfezionò il metodo di Vigenère proponendo l'idea di usare chiavi segrete casuali lunghe almeno quanto il messaggio.



Cifrario del XVII secolo

Con il possesso di un sistema crittografico perfetto, la battaglia teorica tra crittografia e crittoanalisi si è risolta con una vittoria della prima sulla seconda. Ipotizzando di voler far uso di questa insuperabile protezione, restano però aperti molti problemi di ordine pratico. Bisogna infatti soddisfare gli stringenti requisiti del cifrario di Vernam: chiave lunga quanto il messaggio e mai più riutilizzabile. Tuttavia si hanno notizie di utilizzi di questo cifrario in ambiente militare (comunicazione con le spie: si veda a proposito *One Time Pad*), o per la protezione delle comunicazioni del telefono rosso tra Washington e Mosca durante la guerra fredda.

CIHJT UIHML FRUGC ZIBGD BQNE FQJG LPLIP YJYXN  
DCXAC JSJUK BIOYT MWQFX DLIRC BEXYK VKIMB TYIPE  
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI  
DZJYQ YKATE LIUYW DFOHU IOHZV SRNDD KPSSD JNPQT  
MIQHL QHQGD SMHNP IHIOHQ GXRPI XBXIP LLZAA VCMQG  
AWSSZ YHFN IATON IXPHY FOZLE CVYSJ XZGPU CTFQY  
HOVHU DCJGU QMWQV OIGOR BFHIZ TYFDB VBRMN XNLZC

Esempio di cifrario di Vernam

Durante la seconda guerra mondiale, la crittografia ha giocato un ruolo di primaria importanza e la superiorità degli alleati in questo campo è stata determinante. La Germania nazista considerava inattaccabile la sua macchina Enigma, tuttavia già nel 1932 l'ufficio cifrario polacco era riuscito a forzarla così come gli inglesi che più volte sono riusciti a decifrare i messaggi tedeschi generati da essa durante la guerra, e poi dalla macchina Lorenz a partire dal 1941. In più occasioni la superiorità in campo crittografico si è rivelata essere un fattore discriminante per le vittorie alleate come ad esempio nella Battaglia di Capo Matapan, in cui gli inglesi erano riusciti a decifrare i messaggi della marina tedesca che fornivano l'esatta posizione della flotta italiana che fu quindi distrutta nel marzo 1941, e nello Sbarco in Normandia, in cui gli alleati inviarono falsi messaggi sul loro sbarco a Calais facendo sì che i tedeschi mandassero in quella zona le loro migliori truppe in modo tale da avere una bassa resistenza in Normandia; gli inglesi seppero della riuscita dell'inganno decifrando i messaggi tedeschi generati dalla macchina Lorenz.



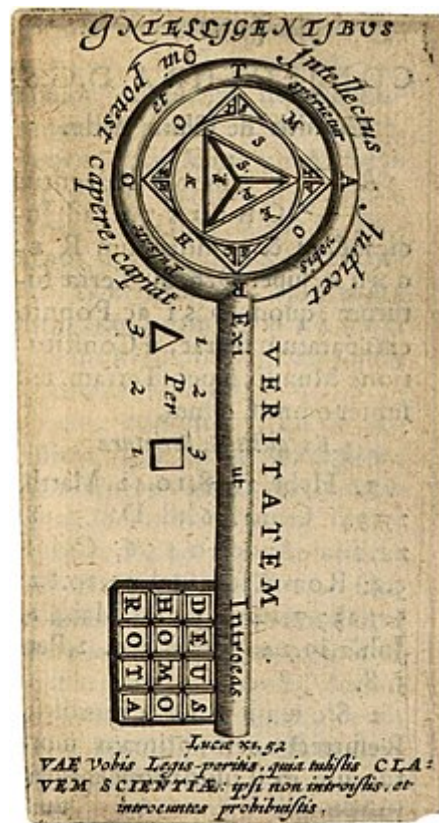
La Macchina enigma.

Nel corso della seconda guerra mondiale l'esercito scrisse telegrammi in lingua navajo per fare in modo che i giapponesi non li riuscissero a decifrare, gli statunitensi d'altronde, già a partire dal 1940, disponevano della macchina *Magic* con la quale decifravano i messaggi giapponesi cifrati con la macchina *Purple*. Fra tutti, vi sono due episodi conclamati in cui gli americani conoscevano le mosse nemiche: la Battaglia delle Midway e la morte dell'Ammiraglio Yamamoto. Successivamente, nel 1949, Claude Shannon, padre della teoria dell'informazione, nel lavoro La teoria della comunicazione nei sistemi crittografici dimostrò che questo è l'unico metodo crittografico possibile che sia totalmente sicuro.

## Descrizione

La crittografia si basa su un algoritmo e su una chiave crittografica. In tal modo si garantisce la confidenzialità delle informazioni che è uno dei requisiti essenziali nell'ambito della sicurezza informatica impedendo così la realizzazione di diversi tipi di attacchi informatici ai dati riservati (es. sniffing). L'approccio inverso di studio volto a rompere un meccanismo crittografico è detto invece crittoanalisi che rappresenta l'altra branca della crittologia. Cruciali sono anche i tempi necessari alla crittoanalisi per la decifrazione del messaggio: per diverse applicazioni di telecomunicazioni e informatica un sistema si può considerare sicuro anche se il suo sistema di cifratura risulta violabile, ma con tempi di realizzazione che renderebbero poi vani i successivi tentativi di attacco diretto.

L'attuale ricerca crittografica, avendo risolto il problema teorico della garanzia della sicurezza, si dedica al superamento dei forti limiti d'uso anzidetti. Si cercano metodi più comodi ma ciononostante estremamente sicuri che, possibilmente, utilizzino chiavi corte e riutilizzabili senza compromettere la loro utilità. Al momento non esiste alcuna tecnica crittografica che si possa definire sicura in senso assoluto, tranne il Cifrario di Vernam; tutte le altre tecniche rendono sicuro il dato solo per un certo arco temporale e non possono garantire la durata della segretezza.



Simbolo di una chiave crittografica

## Crittografia simmetrica

Fino a pochi anni fa era l'unico metodo crittografico esistente, con cui si faceva uso di un'unica chiave sia per proteggere il messaggio che per renderlo nuovamente leggibile. Tali algoritmi hanno però diversi problemi:

- La chiave segreta deve essere scambiata tra i due interlocutori, per cui esiste almeno un momento in cui una terza persona potrebbe impossessarsene durante la trasmissione.
- Se la chiave viene compromessa da una terza persona, questa non solo potrà decifrare tutto il traffico cifrato con quella chiave ma anche produrre dei messaggi falsi o alterare gli originali senza che il destinatario se ne renda conto.
- Ogni coppia di interlocutori deve definire una chiave per cui c'è la necessità di un grande numero di chiavi (in una rete con N utenti sono richieste  $N(N-1)/2$  chiavi).

La ricerca sulla crittografia simmetrica ha negli anni prodotto sistemi crittografici di tutto rispetto (ultimo tra tutti il cifrario Rijndael, scelto per il nuovo standard Advanced Encryption Standard per essere utilizzato nel prossimo ventennio, sostituendo l'ormai datato Data Encryption Standard).



## Crittografia asimmetrica

La vera novità del secolo scorso è l'invenzione di una tecnica crittografica che utilizza chiavi diverse per cifrare e per decifrare un messaggio, facilitando significativamente il compito di distribuzione delle chiavi. Infatti in questo caso non è necessario nascondere le chiavi o le password: c'è una chiave per crittografare (che chiunque può vedere) e una per decifrare, che conosce solo il destinatario senza necessità quindi di riceverla (scambiarla) dal mittente. In altre parole, se Alice vuole ricevere un messaggio segreto da Bob, manda a Bob la chiave pubblica. Bob usa la chiave pubblica per cifrare un messaggio che manda ad Alice, la quale è l'unica ad avere la chiave. Chiunque può veder passare il messaggio, ma non può decifrarlo, in quanto non ha la chiave privata. Alice deve però tenere al sicuro la chiave privata.

Nel 1976 Whitfield Diffie e Martin Hellman, un matematico e un ingegnere in forza alla Stanford University, introducono l'utilizzo della chiave pubblica per la crittazione e l'autenticazione; nell'anno seguente il gruppo di ricerca del MIT formato da Ronald L. Rivest, Adi Shamir e Leonard M. Adleman realizza il primo sistema a chiave pubblica, in questo modo viene ideato l'algoritmo RSA.<sup>[1]</sup> Il funzionamento di questo sistema è basato sul fatto che è matematicamente e computazionalmente molto facile moltiplicare due numeri primi (che singolarmente rappresentano la chiave privata, quella che solo Alice conosce per decifrare), ma è invece molto difficile il problema inverso, ovvero risalire ai fattori primi del numero ottenuto dal precedente prodotto (che invece rappresenta la chiave pubblica che chiunque può vedere e che si usa per crittografare).

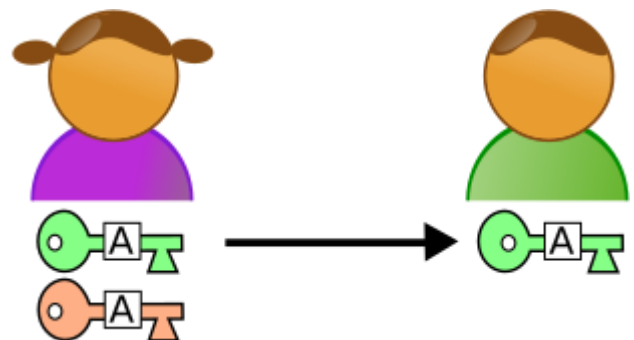
Siccome la crittografia asimmetrica è molto lenta, se si devono spedire grandi quantità di dati si usa solitamente questo tipo di crittografia per scambiarsi una chiave con cui iniziare una comunicazione in crittografia simmetrica, molto più semplice, veloce e sicura. Rientra nell'ambito della crittografia asimmetrica anche la promettente crittografia ellittica.

## Crittografia quantistica

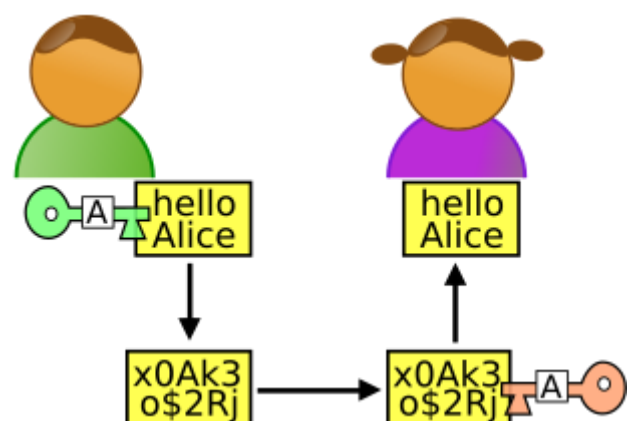
L'evoluzione dei sistemi crittografici, uniti all'evoluzione della fisica teorica hanno permesso di realizzare un cifrario di Vernam che si basa sull'utilizzo della meccanica quantistica nella fase dello scambio della chiave. Il vantaggio di questa tecnica consiste nel fatto di rendere inutilizzabili gli attacchi del tipo man in the middle: cioè, se durante lo scambio della chiave qualcuno riuscisse ad intercettarla, la cosa diverrebbe immediatamente evidente sia a chi emette sia a chi riceve il messaggio.



Schema sintetico della crittografia simmetrica.



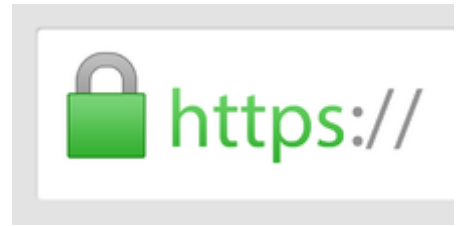
Esempio di crittografia asimmetrica, passo 1: Alice invia a Bob la chiave pubblica



Passo 2: Bob invia ad Alice un messaggio segreto usando la chiave pubblica

# Applicazioni

Le applicazioni della crittografia moderna sono diffuse nella sicurezza informatica ovvero nell'ambito informatico e telecomunicazionistico in tutti i casi in cui è richiesta confidenzialità dei dati, ad esempio, in messaggi e file presenti su supporti di memorizzazione, nelle procedure di Login (in particolare per crittografare la password dell'utente), nelle comunicazioni wireless (Wi-Fi e reti cellulari) per garantire la confidenzialità (ad es. WEP e WPA), nella Rete Internet per oscurare la comunicazione dati in transito tra client e server (protocolli SSH, SSL/TSL, HTTPS, IPsec), nelle transazioni finanziarie-bancarie (home banking), nella pay per view per impedire la visione di contenuti audiovisivi a pagamento ai non abbonati, nelle certificazioni di dispositivi o elementi di dispositivi, di componenti software critici (ad esempio boot loader di sistemi operativi, database Uefi, driver di unità), ecc... Anche un certificato digitale è protetto dalla chiave privata apposta dalla CA che lo ha firmato.

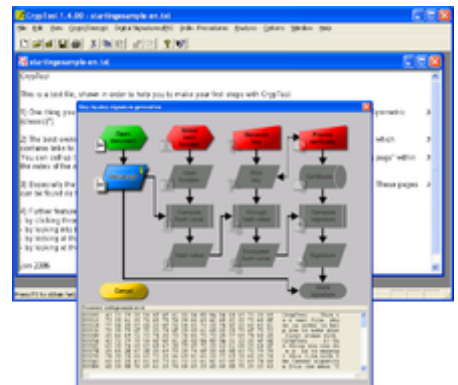


Icona HTTPS

## Software crittografici

Un elenco esemplificativo di alcuni software che a qualche titolo utilizzano crittografia:

- BitLocker Drive Encryption
- Conversations
- CrypTool
- GNUUp, su *gnupg.org*.
- PGP
- ProtonMail
- FreeOTFE
- Telegram
- Tresorit
- TrueCrypt
- Tutanota
- VeraCrypt
- WhatsApp



CrypTool

## Librerie crittografiche

Le molteplici librerie software che implementano algoritmi e protocolli crittografici si differenziano per efficienza, licenza, portabilità e supporto. Di seguito si riportano alcune delle maggiori:

Nome	Sviluppatore	Linguaggio di programmazione	Open source
<u>Botan</u>	Jack Lloyd	<u>C++</u>	Sì
<u>Bouncy Castle</u>	Legion of the Bouncy Castle Inc.	<u>Java</u> , <u>C#</u>	Sì
<u>Crypto++</u>	The Crypto++ project	C++	Sì
<u>GnuTLS</u>	Nikos Mavrogiannopoulos, Simon Josefsson	<u>C</u>	Sì
<u>LibreSSL</u>	OpenBSD Foundation	C	Sì
<u>Libgcrypt</u>	<u>GnuPG</u> community e g10code	C	Sì
<u>NaCl</u>	Daniel J. Bernstein, Tanja Lange, Peter Schwabe	C	Sì
<u>Network Security Services</u>	<u>Mozilla</u>	C	Sì
<u>OpenSSL</u>	The OpenSSL Project	C	Sì
<u>RSA BSAFE</u>	<u>RSA Security</u>	C, Java	No
<u>wolfCrypt</u>	wolfSSL, Inc.	C	Sì

## Aspetti legali

---

Poiché le conversazioni segrete potrebbero essere sfruttate dai criminali, la crittografia è stata a lungo oggetto di interesse da parte delle forze dell'ordine, ma è di notevole interesse anche per i sostenitori dei diritti civili, dato che agevola la privacy. Di conseguenza esistono una serie di controverse questioni legali che la riguardano, specialmente da quando l'avvento di computer economici ha reso possibile un accesso diffuso alla crittografia di alta qualità.

In alcuni paesi era vietato persino l'uso della crittografia domestica. Fino al 1999, la Francia ne limitava significativamente l'uso a livello nazionale, sebbene da allora abbia attenuato molte di queste regole. In Cina e in Iran è ancora necessaria una licenza per utilizzarla,<sup>[2]</sup> e molti altri paesi hanno severe restrizioni sul suo utilizzo. Tra le più restrittive vi sono leggi in Bielorussia, Kazakistan, Mongolia, Pakistan, Singapore, Tunisia e Vietnam. Negli Stati Uniti è legale per uso domestico, ma c'è stato molto dibattito sulle questioni legali relative al suo impiego.<sup>[3]</sup>

## Note

---

- <sup>1</sup>  Anna Lysyanskaya, *Come mantenere un segreto*, in *Le Scienze*, n. 483, novembre 2008, p. 104.
- <sup>2</sup>  (EN) Bert-Jaap Koops, *Overview per country*, in *cryptolaw.org*.
- <sup>3</sup>  (EN) Steve Ranger, *The undercover war on your internet secrets: How online surveillance cracked our trust in the web*, in *techrepublic.com* (archiviato dall'url originale il 12 giugno 2016).

## Bibliografia

---

- Simon Singh*, *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, BUR, 2001, p. 407, ISBN 88-17-12539-3.

## Filmografia

---

- [I signori della truffa](#), film del [1992](#) diretto da [Phil Alden Robinson](#)
- [Breaking the Code](#), film del [1996](#) diretto da [Herbert Wise](#)
- [Enigma](#), film del [2001](#) diretto da [Michael Apted](#)
- [The Imitation Game](#), film del [2014](#) diretto da [Morten Tyldum](#)





## Voci correlate

---

- [Canale laterale](#)
- [Chiave crittografica](#)
- [Cifrario](#)
- [Cifrario a griglia](#)
- [Cifrario Beale](#)
- [Cifratura autenticata](#)
- [Cifratura a blocchi](#)
- [Codice di atbash](#)
- [Criptazione televisiva](#)
- [Crittografia end-to-end](#)
- [Crittografia simmetrica](#)
- [Crittografia asimmetrica](#)
- [Crittografia negabile](#)
- [Crittoanalisi](#)
- [Crittologia](#)
- [Crittografia quantistica](#)
- [Crittografia visuale](#)
- [Crittografia mnemonica](#)
- [Crittografia ellittica](#)
- [Differenza fra cifratura simmetrica e asimmetrica](#)
- [End-to-end](#)
- [Firma digitale](#)
- [Limite di Bremermann](#)
- [Neurocrittografia](#)
- [Steganografia](#)
- [Storia della crittografia](#)
- [Secure voice](#)
- [Tipo di attacco](#)

## Altri progetti

---

-  Wikiquote contiene citazioni sulla **[crittografia](#)**
-  Wikibooks contiene testi o manuali sulla **[crittografia](#)**
-  Wikizionario contiene il lemma di dizionario «**[crittografia](#)**»
-  [Wikimedia Commons \(https://commons.wikimedia.org/wiki/?uselang=it\)](https://commons.wikimedia.org/wiki/?uselang=it) contiene immagini o altri file sulla **[crittografia](#)** (<https://commons.wikimedia.org/wiki/Category:Cryptography?uselang=it>)

## Collegamenti esterni

---

- 
- *crittografia*, su *Treccani.it – Enciclopedie on line*, Istituto dell'Enciclopedia Italiana.
- Ggiancarlo Bongiovanni, *Crittografia*, su *Treccani.it – Enciclopedie on line*, Istituto dell'Enciclopedia Italiana, 2004.
- Lazzaro Dessy, *CRITTOGRAFIA*, in *Enciclopedia Italiana*, II Appendice, Istituto dell'Enciclopedia Italiana, 1948.
- Vittorio Gamba, *CRITTOGRAFIA o crittografia*, in *Enciclopedia Italiana*, Istituto dell'Enciclopedia Italiana, 1931.
- (EN)  *Crittografia*, su *Enciclopedia Britannica*, Encyclopædia Britannica, Inc.
- (EN)  *Opere riguardanti Crittografia*, su *Open Library*, Internet Archive.
- *Video introduttivo sulla Crittografia*, su *youtube.com*.

### Controllo di autorità

Thesaurus BNCF 10374 (<https://thes.bncf.firenze.sbn.it/termine.php?id=10374>) · LCCN (EN)  sh85034453 (<http://id.loc.gov/authorities/subjects/sh85034453>) · BNF (FR)  cb11941832r (<https://catalogue.bnf.fr/ark:/12148/cb11941832r>) (data) (<https://data.bnf.fr/ark:/12148/cb11941832r>) · BNE (ES)  XX4659806 ([http://catalogo.bne.es/uhtbin/authoritybrowse.cgi?action=display&authority\\_id=XX4659806](http://catalogo.bne.es/uhtbin/authoritybrowse.cgi?action=display&authority_id=XX4659806)) (data) (<http://datos.bne.es/resource/XX4659806>)

---

Estratto da "<https://it.wikipedia.org/w/index.php?title=Crittografia&oldid=125631173>"

---

Questa pagina è stata modificata per l'ultima volta il 10 feb 2022 alle 08:36.

Il testo è disponibile secondo la licenza Creative Commons Attribuzione-Condividi allo stesso modo; possono applicarsi condizioni ulteriori. Vedi le condizioni d'uso per i dettagli.