WIKIPEDIA

Verschlüsselung

Verschlüsselung (auch: **Chiffrierung** oder **Kryptierung**)[1] ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch „Chiffrat“ oder „Schlüsseltext“ genannt), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.

Durch Verschlüsselung wird aus einem Klartext mithilfe eines Schlüssels ein Geheimtext erzeugt

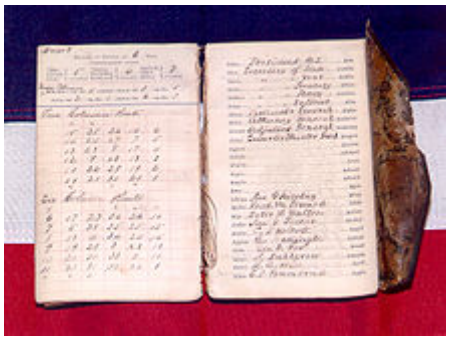
Verschlüsselung dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegen unbefugten Zugriff abzusichern oder um Nachrichten vertraulich zu übermitteln. Die Wissenschaft des Verschlüsselns wird als Kryptographie bezeichnet.[2]

Inhaltsverzeichnis

Grundlagen

Das Verschlüsseln

Durch Verschlüsseln wird ursprünglich der „offene Wortlaut“ eines Textes, genannt „Klartext“, in eine unverständliche Zeichenfolge umgewandelt, die als „Geheimtext“ bezeichnet wird. Die Fachbegriffe *Klartext* und *Geheimtext* sind historisch gewachsen und heutzutage deutlich weiter zu interpretieren. Außer Textnachrichten lassen sich auch alle anderen Arten von Information verschlüsseln, beispielsweise Sprachnachrichten, Bilder, Videos oder der Quellcode von Computerprogrammen. Die kryptographischen Prinzipien bleiben dabei die gleichen.



Kryptographisches Codebuch aus dem amerikanischen Bürgerkrieg

Eine besondere und relativ einfache Art der Verschlüsselung ist die Codierung (auch: Kodierung). Hierbei werden in der Regel nicht einzelne Klartextzeichen oder kurze Zeichenkombinationen verschlüsselt, sondern ganze Worte, Satzteile oder ganze Sätze. Beispielsweise können wichtige Befehle wie „Angriff im Morgengrauen!“ oder „Rückzug von den Hügeln!“ bestimmten Codewörtern oder unverständlichen Zeichenkombinationen aus Buchstaben, Ziffern oder anderen Geheimzeichen zugeordnet werden. Dies geschieht zumeist als tabellarische Liste, beispielsweise in Form von Codebüchern. Zur Steigerung der kryptographischen Sicherheit von Codes werden die damit erhaltenen Geheimtexte oft einem zweiten Verschlüsselungsschritt unterworfen. Dies wird als *Überschlüsselung* (auch: *Überverschlüsselung*) bezeichnet. Außer geheimen Codes gibt es auch offene Codes, wie den Morsecode und ASCII, die nicht kryptographischen Zwecken dienen und keine Verschlüsselung darstellen.

Der Schlüssel

Der entscheidende Parameter bei der Verschlüsselung ist der „Schlüssel“. Die gute Wahl eines Schlüssels und seine Geheimhaltung sind wichtige Voraussetzungen zur Wahrung des Geheimnisses. Im Fall der Codierung stellt das Codebuch den Schlüssel dar. Im Fall der meisten klassischen und auch einiger moderner Methoden zur Verschlüsselung ist es ein Passwort (auch: Kennwort, Schlüsselwort, Codewort oder Kodewort, Losung, Losungswort oder Parole von italienisch *la parola* „das Wort“; englisch *password*). Bei vielen modernen Verfahren, beispielsweise bei der E-Mail-Verschlüsselung, wird dem Benutzer inzwischen die Wahl eines Schlüssels abgenommen. Dieser wird automatisch generiert, ohne dass der Nutzer es bemerkt. Hierdurch wird auch der „menschliche Faktor“ eliminiert, nämlich die nicht selten zu sorglose Wahl eines unsicheren, weil zu kurzen und leicht zu erratenden, Passworts.

Das Entschlüsseln

Der zur *Verschlüsselung* umgekehrte Schritt ist die *Entschlüsselung*. Dabei gewinnt der befugte Empfänger den Klartext aus dem Geheimtext zurück. Zum *Entschlüsseln* wird ein geheimer Schlüssel benötigt. Bei symmetrischen Verschlüsselungsverfahren ist dies der gleiche wie für das Verschlüsseln, bei asymmetrischen Verfahren hingegen nicht. Geht der Schlüssel verloren, dann lässt sich der Geheimtext nicht mehr entschlüsseln. Gerät der Schlüssel in fremde Hände, dann können auch Dritte den Geheimtext lesen, das Geheimnis ist also nicht länger gewahrt. Ein zusammenfassender Begriff für Verschlüsseln und/oder Entschlüsseln ist das *Schlüsseln*.

Das Entziffern

Sprachlich zu trennen von der *Entschlüsselung* ist der Begriff der „Entzifferung“. Als *Entzifferung* wird die Kunst bezeichnet, dem Geheimtext seine geheime Nachricht zu entringen, *ohne* im Besitz des Schlüssels zu sein. Dies ist die Tätigkeit eines Kryptoanalytikers, häufig auch als „Codeknacker“ (englisch *codebreaker*)

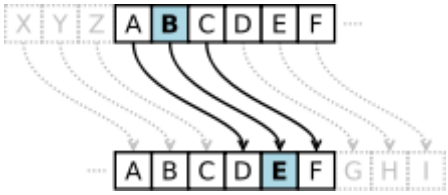
bezeichnet. Im Idealfall gelingt keine Entzifferung, weil das Verschlüsselungsverfahren ausreichend „stark“ ist. Es wird dann als „unbrechbar“ oder zumindest als „kryptographisch stark“ bezeichnet. Im Gegensatz zu einer „starken Verschlüsselung“ lässt sich eine „schwache Verschlüsselung“ ohne vorherige Kenntnis des Schlüssels mit vertretbarem Aufwand mithilfe kryptanalytischer Methoden brechen. Durch Fortschritte in der Kryptologie kann sich eine vermeintlich starke Verschlüsselung im Laufe der Zeit als schwach erweisen. So galt beispielsweise die „Vigenère-Verschlüsselung“ über Jahrhunderte hinweg als „Le Chiffre indéchiffrable“ („Die unentzifferbare Verschlüsselung“). Inzwischen weiß man, dass dem nicht so ist.

Das Arbeitsgebiet, das sich mit der Entzifferung von Geheimtexten befasst, ist die Kryptanalyse (älterer Ausdruck: Kryptoanalyse). Sie ist neben der Kryptographie das zweite Teilgebiet der Kryptologie. Die Kryptanalyse dient nicht nur zur unbefugten Entzifferung von Geheimnachrichten, sondern sie befasst sich auch mit „(Un-)Brechbarkeit“ von Verschlüsselungen, also der Prüfung der Sicherheit von Verschlüsselungsverfahren gegen unbefugte Entzifferung.

Die meisten Verschlüsselungsverfahren sind nur *pragmatisch sicher*, was bedeutet, dass bei ihrer Kryptanalyse keine praktikable Möglichkeit zur Entzifferung gefunden wurde. Dabei ist das Vertrauen in die Sicherheit umso mehr gerechtfertigt, je länger ein Verfahren bereits öffentlich bekannt ist und je verbreiteter es in der Anwendung ist, denn umso mehr kann man davon ausgehen, dass viele fähige Kryptologen es unabhängig voneinander untersucht haben und dass eine eventuell vorhandene Schwäche gefunden und veröffentlicht worden wäre (siehe auch Kerckhoffs’ Prinzip).

Es gibt Verfahren, deren Sicherheit unter Annahme der Gültigkeit bestimmter mathematischer Vermutungen beweisbar ist. So kann zum Beispiel für das RSA-Kryptosystem gezeigt werden: Der private Schlüssel eines Benutzers kann aus dessen öffentlichem Schlüssel genau dann effizient berechnet werden, wenn man eine große Zahl (in der Größenordnung von einigen hundert Dezimalstellen) effizient in ihre Primfaktoren zerlegen kann. Das einzige Verschlüsselungsverfahren, dessen Sicherheit wirklich bewiesen und nicht nur auf Vermutungen zurückgeführt wurde, ist das One-Time-Pad.

Beispiel



Caesar-Verschlüsselung mit Schlüssel „C“

Zur Illustration einer Verschlüsselung wird der unten (aus Gründen der besseren Unterscheidbarkeit wie üblich in Kleinbuchstaben) angegebene Klartext mithilfe eines sehr alten und äußerst simplen Verfahrens, der Caesar-Verschlüsselung, in einen Geheimtext (hier aus Großbuchstaben) umgewandelt. Als geheimer Schlüssel wird hier „C“ benutzt, also der dritte Buchstabe des lateinischen Alphabets. Das bedeutet die Ersetzung jedes einzelnen Klartextbuchstabens durch den jeweiligen im Alphabet um drei Stellen verschobenen Buchstaben. So wird beispielsweise aus dem Anfangsbuchstaben „B“ des Klartextes durch Verschlüsselung der im Alphabet drei Stellen später auftretende Buchstabe „E“ im Geheimtext, und so weiter:

```
bevordertextverschluesseltwirdisterklarlesbar
EHYRUGHUWHAWYHUVFKOXHVVHOWZLUGLVWHUNODUOHVEDU
```

Der im Beispiel mit „EHYRU“ beginnende, hier durch Caesar-Verschlüsselung entstandene (und aus Gründen der Illustration wie üblich in Großbuchstaben dargestellte) Geheimtext ist tatsächlich auf den ersten Blick unverständlich. Er eignet sich somit, um die im Klartext enthaltene Information vor fremdem Blicken zu verbergen. Kennt ein möglicher Angreifer das zugrundeliegende Verschlüsselungsverfahren nicht, oder gelingt es ihm nicht, den benutzten Schlüssel zu finden, dann bleibt der Geheimtext für ihn ohne Sinn. Natürlich ist die hier im Beispiel benutzte Methode, die schon die alten Römer kannten, viel zu

schwach, um die Geheimnachricht lange zu schützen. Einem erfahrenen Codebrecher wird es nicht viel Mühe bereiten, den Geheimtext nach kurzer Zeit zu entziffern, auch ohne vorherige Kenntnis von Schlüssel oder Verfahren.

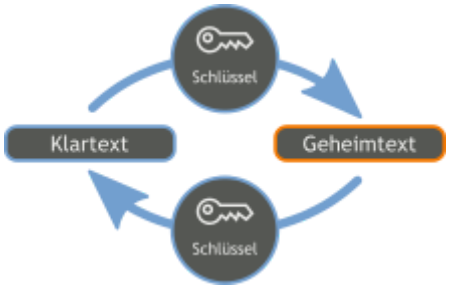
Im Laufe der Geschichte der Menschheit wurden daher immer stärkere Methoden zur Verschlüsselung entwickelt (siehe auch: Geschichte der Kryptographie). Ein modernes Verschlüsselungsverfahren ist der *Advanced Encryption Standard (AES)*, das zurzeit als unbrechbar gilt. Dies wird sich aber in kommenden Jahrzehnten möglicherweise ändern (siehe auch: Kryptanalytische Angriffe auf AES).

Klassifizierung

Prinzipiell unterscheidet man unterschiedliche klassische und moderne symmetrische Verschlüsselungsverfahren und die erst seit wenigen Jahrzehnten bekannten asymmetrischen Verschlüsselungsverfahren. Klassische Verschlüsselungsverfahren können nach dem verwendeten Alphabet klassifiziert werden.

Symmetrische Verschlüsselung

→ *Hauptartikel: Symmetrisches Kryptosystem*



Bei der symmetrischen Verschlüsselung dient der Schlüssel auch zur Entschlüsselung

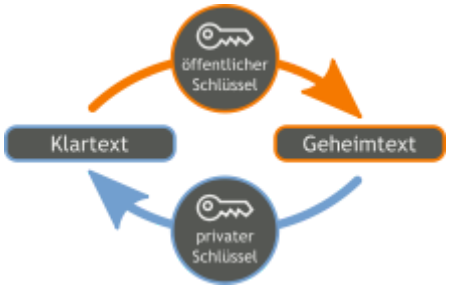
Symmetrische Verschlüsselungsverfahren verwenden zur Ver- und Entschlüsselung den gleichen Schlüssel. Bei historischen Verfahren lassen sich zwei Verschlüsselungsklassen unterscheiden. Bei der ersten werden, wie bei der im Beispiel benutzten Caesar-Verschlüsselung, die Buchstaben des Klartextes einzeln durch andere Buchstaben ersetzt. Mit dem lateinischen Wort *substituere* (deutsch: „ersetzen“) werden sie als Substitutionsverfahren bezeichnet. Im Gegensatz dazu bleibt bei der zweiten Verschlüsselungsklasse, genannt Transposition (von lateinisch: *transponere*; deutsch: „versetzen“), jeder Buchstabe *wie* er ist, aber nicht *wo* er ist. Sein Platz im Text wird verändert, die einzelnen Buchstaben des Textes werden sozusagen durcheinandergewürfelt. Eine besonders einfache Form einer Transpositions-Verschlüsselung ist die bei Kindern beliebte „Revertierung“ (von lateinisch: *reverse*; deutsch: „umkehren“) eines Textes. So entsteht beispielsweise aus dem Klartext „GEHEIMNIS“ der Geheimtext „SINMIEHEG“.

Bei modernen symmetrischen Verfahren werden Stromverschlüsselung und auf einer Blockverschlüsselung basierende Verfahren unterschieden. Bei der Stromverschlüsselung werden die Zeichen des Klartextes jeweils einzeln und nacheinander verschlüsselt. Bei einer Blockverschlüsselung hingegen wird der Klartext vorab in Blöcke einer bestimmten Größe aufgeteilt. Wie dann die Blöcke verschlüsselt werden, bestimmt der Betriebsmodus der Verschlüsselungsmethode.

Interessanterweise beruhen selbst moderne Blockchiffren, wie beispielsweise das über mehrere Jahrzehnte gegen Ende des 20. Jahrhunderts zum Standard erhobene Verschlüsselungsverfahren *DES (Data Encryption Standard)* auf den beiden klassischen Methoden Substitution und Transposition. Sie verwenden diese beiden Grundprinzipien in Kombination und beziehen ihre Stärke ganz maßgeblich durch die mehrfache wiederholte Anwendung von solchen Kombinationen nicht selten in Dutzenden von „Runden“. So wird, vergleichbar zum wiederholten Kneten von Teig, der Klartext immer stärker verschlüsselt. Die Stärke der Verschlüsselung steigt zumeist mit der Anzahl der verwendeten Runden.

Asymmetrische Verschlüsselung

→ *Hauptartikel: Asymmetrisches Kryptosystem*



Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel, den öffentlichen Schlüssel zur Verschlüsselung und den privaten Schlüssel zur Entschlüsselung

Über Jahrhunderte hinweg war man der Meinung, dass es keine Alternative zur symmetrischen Verschlüsselung und dem damit verknüpften Schlüsselverteilungsproblem gäbe. Erst vor wenigen Jahrzehnten wurde die asymmetrische Verschlüsselung (*Public-key cryptography*) erfunden. Kennzeichen der asymmetrischen Verschlüsselung ist, dass zur Verschlüsselung ein *völlig anderer Schlüssel* als zur Entschlüsselung benutzt wird. Man unterscheidet hier zwischen dem „öffentlichen Schlüssel“, der zum Verschlüsseln benutzt wird, und dem „privaten Schlüssel“ zum Entschlüsseln des Geheimtextes. Der private Schlüssel wird niemals weitergegeben oder gar veröffentlicht, der öffentliche Schlüssel hingegen wird dem Kommunikationspartner übergeben oder veröffentlicht. Er kann dann von jedermann benutzt werden, um Nachrichten zu verschlüsseln. Um diese jedoch entschlüsseln zu können, benötigt man den dazu passenden privaten Schlüssel. Nur damit kann die verschlüsselte Nachricht wieder entschlüsselt werden. Das heißt, noch nicht einmal der Verschlüssler selbst ist in der Lage, seine eigene Nachricht, die er mit dem öffentlichen Schlüssel der anderen Person verschlüsselt hat, wieder zu entschlüsseln.

Das Verfahren kann übrigens auch „umgekehrt“ verwendet werden, indem eine Person ihren privaten Schlüssel nutzt, um damit eine Information zu *ver*schlüsseln. Nun ist jedermann, der Zugriff auf den öffentlichen Schlüssel hat, in der Lage, damit die Nachricht zu *ent*schlüsseln. Hier geht es meist nicht um die Geheimhaltung einer Nachricht, sondern beispielsweise um die Authentifizierung einer Person beziehungsweise die digitale Signatur einer Nachricht. Jedermann kann leicht überprüfen und erkennen, dass die verschlüsselte Information nur von dieser einen Person stammen kann, denn nur diese besitzt den nötigen privaten Schlüssel. Zum Signieren allein genügt es, den Nachrichtentext unverschlüsselt als Klartext zu belassen, und beispielsweise nur eine Prüfsumme davon verschlüsselt anzuhängen. Wenn der öffentliche Schlüssel des Autors beim Entschlüsseln eine korrekte Prüfsumme freilegt, ist sowohl der Autor als auch die Unverfälschtheit der Nachricht bestätigt.

Da asymmetrische Verfahren algorithmisch aufwändiger sind als symmetrische und daher in der Ausführung langsamer, werden in der Praxis zumeist Kombinationen aus beiden, sogenannte Hybrid-Verfahren genutzt. Dabei wird beispielsweise zuerst ein zufällig generierter individueller Sitzungsschlüssel mithilfe eines asymmetrischen Verfahrens ausgetauscht, und dieser anschließend gemeinsam als Schlüssel für ein symmetrisches Verschlüsselungsverfahren benutzt, wodurch die eigentlich zu kommunizierende Information verschlüsselt wird.

Glossar

In der Kryptologie dient eine klare Abgrenzung von Begriffen und eine saubere und konsequent verwendete Fachterminologie zur Erleichterung der Arbeit und zur Vermeidung von Missverständnissen. Im Gegensatz dazu werden umgangssprachlich nicht selten Ausdrücke falsch benutzt und miteinander verwechselt, was zu unnötigen und leicht vermeidbaren Irritationen führen kann. Ein Beispiel ist die unsaubere Verwendung des Begriffs Entschlüsselung, wenn eigentlich Entzifferung gemeint ist.

- Alphabet – Eine in der Reihenfolge permutierte geordnete Anordnung von Symbolen, speziell der 26 lateinischen Großbuchstaben (Beispiel: E K M F L G D Q V Z N T O W Y H X U S P A I B R C J)
- Brechen

    - eines Geheimtextes – Anderer Ausdruck für *Entziffern*
    - Eines Verschlüsselungsverfahrens – Kompromittierung der Sicherheit des Verfahrens, etwa Entwicklung einer Methode zum Entziffern seiner Geheimtexte
- Chiffrat – Anderer Ausdruck für *Geheimtext*
- Chiffre – Anderer Ausdruck für *Verschlüsselungsverfahren*
- Chiffrieren – Anderer Ausdruck für *Verschlüsseln*
- Chiffrierung – Anderer Ausdruck für *Verschlüsselung*
- Codebuch – Hilfsmittel bei der Codierung
- Codeknacker – ugs. Ausdruck für *Kryptoanalytiker*
- Codierung – Zumeist feste Zuordnung von Klartextgruppen zu Geheimtextgruppen
- Dechiffrat – Text nach Entschlüsselung
- Entschlüsseln – Umwandlung des Geheimtextes in den Klartext mithilfe des Schlüssels
- Entziffern – Ermitteln des Klartextes aus dem Geheimtext ohne vorherige Kenntnis des Schlüssels
- Geheimtext – Durch Verschlüsselung aus dem Klartext erzeugter Text
- Involutorisch – Verschlüsselung und Entschlüsselung sind identisch
- Klartext – Offener (unverschlüsselter) Wortlaut der Nachricht
- Knacken – ugs. Ausdruck für *Entziffern*
- Kryptoanalytiker – Jemand, der Geheimtexte zu entziffern versucht oder kryptografische Verfahren auf ihre Sicherheit untersucht bzw. versucht, diese zu brechen
- Kryptogramm – Anderer Ausdruck für *Geheimtext*
- Schlüssel – Geheime Information, die bei der Verschlüsselung verwendet wird bzw. zur Entschlüsselung benötigt wird
- Schlüsseln – Zusammenfassender Begriff für *Verschlüsseln* und *Entschlüsseln*
- Schlüssler – Person, die Nachrichten ver- oder entschlüsselt
- Schlüsselraum – Menge aller möglichen Schlüssel
- Schlüsseltext – Anderer Ausdruck für *Geheimtext*
- Schwache Verschlüsselung – Verschlüsselung, die entziffert werden kann, also gebrochen ist oder gebrochen werden kann
- Starke Verschlüsselung – Verschlüsselung, die mit heutigen Kenntnissen und Methoden nicht entziffert werden kann
- Verschlüsseln – Umwandlung von Klartext in Geheimtext

Anwendungen in der Praxis der Informationstechnik

Nachrichtenübertragung in Netzwerken

Eine verschlüsselte Nachricht (z. B. eine E-Mail oder eine Webseite) muss in der Regel über mehrere Stationen übertragen werden. Heute handelt es sich dabei meist um einzelne Computersysteme, das heißt die verschlüsselte Nachricht wird über ein Rechnernetzwerk übertragen. Man unterscheidet dabei zwei grundlegend unterschiedliche Übertragungsweisen. Bei der Leitungsverschlüsselung wird die Nachricht nur jeweils für den Nachbarrechner verschlüsselt. Dieser entschlüsselt die Nachricht, verschlüsselt sie wiederum (mit einem möglicherweise anderen Verfahren) und schickt sie an seinen Nachbarn – und so weiter bis zum Zielrechner. Der Vorteil dieses Verfahrens besteht darin, dass sich jeweils nur Nachbarrechner auf ein Verschlüsselungsverfahren und verwendete Schlüssel einigen müssen. Darüber hinaus kann diese Übertragungsweise auf einer sehr niedrigen Protokollebene (etwa bereits in der Übertragungs-Hardware) angesiedelt werden. Der Nachteil besteht darin, dass jeder einzelne Rechner auf

dem Übertragungsweg vertrauenswürdig und sicher sein muss. Bei der Ende-zu-Ende-Verschlüsselung hingegen wird die Nachricht vom Absender verschlüsselt und in dieser Form unverändert über mehrere Rechner hinweg zum Empfänger übertragen. Hier hat keiner der übertragenden Rechner Einsicht in den Klartext der Nachricht. Der Nachteil besteht allerdings darin, dass sich der Absender mit jedem möglichen Empfänger auf ein Verschlüsselungsverfahren und zugehörige(n) Schlüssel einigen muss.

Verschlüsselung von Daten auf Datenträgern („Datentresor“)

[Für eine ausführliche Behandlung siehe Festplattenverschlüsselung]

Sensible Daten auf einem Datenträger lassen sich im Wesentlichen auf zwei Wegen vor unbefugtem Zugriff schützen:

- man verschlüsselt mit Hilfe von Verschlüsselungssoftware die gesamte Festplatte oder eine einzelne Partition (*Full Disk Encryption*, kurz *FDE*) oder auch nur einen Daten-Container in Form einer einzelnen Datei auf dem Datenträger;
- bei der hardware-seitigen Verschlüsselung (*Hardware encryption*) übernimmt ein Mikrochip auf dem USB-Laufwerk eine automatische und transparente Verschlüsselung. Die Authentifizierung wird beispielsweise dadurch erreicht, dass das Gerät über eine physische Tastatur verfügt, über die vor der Verwendung ein PIN-Code einzugeben ist.

Literatur

- Friedrich L. Bauer: *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie.* 3., überarbeitete und erweiterte Auflage. Springer, Berlin u. a. 2000, ISBN 3-540-67931-6.
- Linda A. Bertram, Gunther van Dooble, et al. (Hrsg.): *Nomenclatura – Encyclopedia of modern Cryptography and Internet Security. From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys.* Books on Demand, Norderstedt 2019, ISBN 978-3746-06668-4.
- Albrecht Beutelspacher *Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen ohne alle Geheimniskrämerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums*. Vieweg & Teubner, 9. aktualisierte Auflage, Braunschweig 2009, ISBN 978-3-8348-0253-8.
- Klaus Beyrer (Hrsg.): *Streng geheim! Die Welt der verschlüsselten Kommunikation*. Braus Verlag, Heidelberg 1999.
- Johannes Buchmann: *Einführung in die Kryptographie*. Springer, 4. erweiterte Auflage, Berlin 2008, ISBN 978-3-540-74451-1.
- Michael Miller: *Symmetrische Verschlüsselungsverfahren – Design, Entwicklung und Kryptoanalyse klassischer und moderner Chiffren*. Teubner, Wiesbaden 2003, ISBN 3-519-02399-7.
- Klaus Schmeh: *Codeknacker gegen Codemacher – Die faszinierende Geschichte der Verschlüsselung*. W3L-Verlag, 2. Auflage, Herdecke 2008, ISBN 978-3-937137-89-6.
- Bruce Schneier: *Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C.* Pearson Studium, München 2006, ISBN 3-8273-7228-3.
- Simon Singh: *Geheime Botschaften*. Carl Hanser Verlag, München 2000, ISBN 3-446-19873-3.
- Fred B. Wrixon: *Codes, Chiffren & andere Geheimsprachen – Von den ägyptischen Hieroglyphen bis zur Computerkryptologie*. Könemann, Köln 2000, ISBN 3-8290-3888-7.

Weblinks

Wiktionary: Verschlüsselung – Bedeutungserklärungen, Wortherkunft, Synonyme, Übersetzungen
Wikinews: Kategorie: Verschlüsselung – in den Nachrichten

- Eine Einführung in die Anwendung der Verschlüsselung (http://www.hermetic.ch/crypto/intro g.htm)
- Verschlüsselungsverfahren und ihre Anwendungen (https://www.heise.de/security/artikel/Ha rte-Nuesse-Verschluesselungsverfahren-und-ihre-Anwendungen-270266.html)
- Simon Singh: The Code Book (1999) (http://simonsingh.net/books/the-code-book/the-book/) (englisch).
- Einführung in das Thema Verschlüsselung (http://www.verschluesselungen.net)
- Verschlüsselung: Häufige Schwachstellen (http://m-witkowski.de/verschlusselung-grundlag en/)
- Christian Spannagel: Verschlüsselung (https://av.tib.eu/series/237/). Vorlesungsreihe, 2012.

Einzelnachweise

1. Bundeswehr-Drohne fliegt mit deutscher „Kryptierung“ (https://www.heise.de/newsticker/mel dung/Bundeswehr-Drohne-fliegt-mit-deutscher-Kryptierung-3341890.html) auf *heise online* vom 6. Oktober 2016, abgerufen am 30. April 2019.
2. Wolfgang Ertel: *Angewandte Kryptographie*. 4., überarbeitete und ergänzte Auflage. Carl Hanser Verlag, München 2012, ISBN 978-3-446-43196-6.