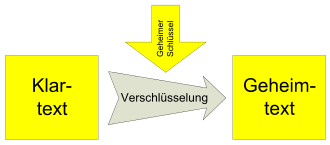
Verschlüsselung

#### Grundlagen

***Definition:*** *Umwandlung von „Klartext“ in „Geheimsprache“, mithilfe eines Schlüssels, welcher der einzige Weg ist, die Daten zu ver- und entschlüsseln*

[](https://de.wikipedia.org/wiki/Datei:Verschl%C3%BCsselung_(symmetrisches_Kryptosystem)_Schema.svg)

<https://de.wikipedia.org/wiki/Datei:Verschl%C3%BCsselung_(symmetrisches_Kryptosystem)_Schema.svg>

**Verschlüsseln**

Durch Verschlüsseln wird ein „Klartext“, also ein lesbarer Text, in einen „Geheimtext“, also in eine unverständliche Zeichenfolge umgewandelt. Nicht nur Textnachrichten kann man verschlüsseln, sondern auch andere Arten von Information, wie Sprachnachrichten, Bildaufzeichnungen oder der Quellcode von Programmen.

Eine einfache und oft verwendete Art der Verschlüsselung ist die Codierung. Hier werden in der Regel keine einzelnen Klartextzeichen oder kurze Zeichenkombinationen verschlüsselt, sondern ganze Satzteile, Worte oder ganze Sätze. Um Worte oder ganze Sätze umzuwandeln, geschieht dies meist als tabellarische Liste, z.B. in Form von Codebüchern

[https://www.bing.com/images/search?view=detailV2&id=E690EF6 3196EC87A778C5B305A09E3F2F2824F4E&thid=OIP.bXizy0TLKXEmW rVyDf3TcQHaJ0&mediaurl=http%3A%2F%2Fwww.cirth.de%2Fange rthasenglischmodus.gif&exph=690&expw=520&q=verschl%c3%bcsse ltes+codebuch&selectedindex=6&ajaxhist=0&vt=0](https://www.bing.com/images/search?view=detailV2&id=E690EF6%203196EC87A778C5B305A09E3F2F2824F4E&thid=OIP.bXizy0TLKXEmW%20rVyDf3TcQHaJ0&mediaurl=http%3A%2F%2Fwww.cirth.de%2Fange%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20rthasenglischmodus.gif&exph=690&expw=520&q=verschl%c3%bcsse%20ltes+codebuch&selectedindex=6&ajaxhist=0&vt=0)

Zur Steigerung der kryptographischen Sicherheit von Codes werden die damit erhaltenen Geheimtexte oft einem zweiten Verschlüsselungsschritt unterworfen. Zu den geheimen Codes gibt es auchoffene Codes, wie den Morsecode und ASCII, die nicht kryptographischen Zwecken dienen und keine Verschlüsselungdarstellen.

**Der Schlüssel**

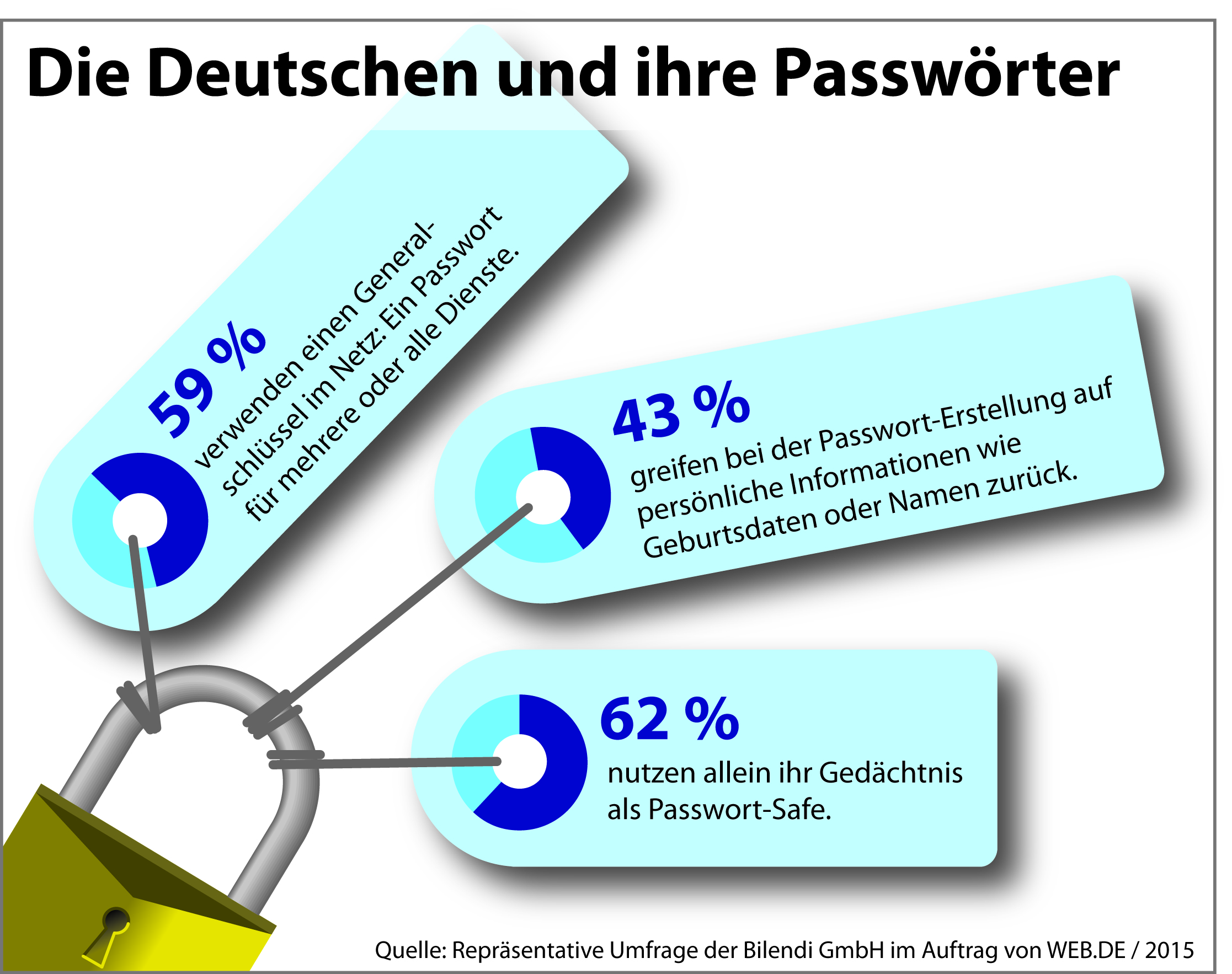
Der entscheidende und wichtigste Parameter bei der Verschlüsselung ist der „Schlüssel“. Die gute Wahl eines Schlüssels und sein sicherer Schutz vor unerlaubtem Zugriff sind essentielle Voraussetzungen zur Wahrung des verschlüsselten Geheimnisses. Im Fall der Codierung stellt das Codebuch den Schlüssel dar. Im Fall der meisten klassischen und auch einiger moderner Methoden zur Verschlüsselung ist es ein Passwort. Jedoch nimmt der Mensch oft ein unbedachtes Passwort, was es anderen leichter ermöglicht unbefugt auf die verschlüsselten Daten zuzugreifen.

**Das Entschlüsseln**

Der zur Verschlüsselung umgekehrte Schritt ist die Entschlüsselung. Zum Entschlüsseln wird der geheime Schlüssel verwendet, mit dessen Hilfe der befugte Empfänger den Geheimtext wieder in den Klartext zurückverwandeln kann. 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.

**Das Entziffern**

Sprachlich zu trennen von der Entschlüsselung ist der Begriff der „Entzifferung“. Als Entzifferung wird es bezeichnet, dem Geheimtext seine geheime Nachricht zu entringen, ohne im Besitz des Schlüssels zu sein. Dies ist die Tätigkeit eines Kryptoanalytikers, auch als „Codeknacker“ 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 eine schwache Verschlüsselung herausstellen.



<https://newsroom.web.de/wp-content/uploads/sites/19/2015/06/Passwort-Studie_2015_Grafik.jpg>

Das Arbeitsgebiet, das sich mit der Entzifferung von Geheimtexten befasst, ist die Kryptanalyse. 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 unerlaubte Entzifferung. Je länger ein Verfahren bereits öffentlich bekannt ist, desto häufiger erfolgt die Anwendung .

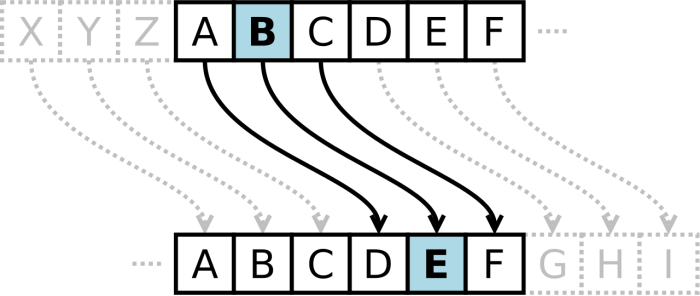
#### Beispiel

Caesar-Verschlüsselung mit Schlüssel „C“

Als geheimer Schlüssel wird hier „C“ genutzt, also der dritte Buchstabe des lateinischen Alphabets. Das bedeutet die Ersetzung jedes Klartextbuchstabens durch den jeweiligen im Alphabet um drei Stellen verschobenen Buchstaben. So wird z.B. aus dem Anfangsbuchstaben „B“ des Klartextes durch Verschlüsselung der im Alphabet drei Stellen später auftretende Buchstabe „E“ im Geheimtext, und so weiter:

bevordertextverschluesseltwirdisterklarlesbar

EHYRUGHUWHAWYHUVFKOXHVVHOWZLUGLVWHUNODUOHVEDU



<https://upload.wikimedia.org/wikipedia/commons/2/2b/Caesar3.svg>

*Schlüssel animation:*

<http://bestanimations.com/HomeOffice/Keys/key-animated-gif-3.gif>

**Anwendung in der Praxis**

*Nachrichtenübertragung in Netzwerken*

Eine verschlüsselte Nachricht (z. B. eine E-Mail oder eine Webseite) muss meistens über mehrere Stationen übertragen werden. Heut zu tage handelt es sich dabei in der Regel um einzelne Computersysteme, das bedeutet die verschlüsselte Nachricht wird über ein Rechnernetzwerk übertragen. Es gibt insgesamt zwei grundlegend unterschiedliche Übertragungsarten. Bei der Leitungsverschlüsselung wird die Nachricht nur jeweils für den Nachbarrechner verschlüsselt. Dieser entschlüsselt die Nachricht, verschlüsselt sie wiederum) und schickt sie an seinen Nachbarn – und so weiter bis zum Zielrechner. Der Vorteil dieser Übertragungsart ist, dass sich jeweils nur Nachbarrechner auf ein Verschlüsselungsverfahren und verwendete Schlüssel einigen müssen. Darüber hinaus kann diese Übertragungsart auf einer sehr niedrigen Protokollebene angesiedelt werden. Der Nachteil ist, dass jeder einzelne Rechner auf dem Übertragungsweg sicher sein muss. Bei der Ende-zu-Ende-Verschlüsselung hingegen wird die Nachricht vom Absender verschlüsselt und in dieser Form unberührt über mehrere Rechner bis zum Empfänger übertragen. Hier kann keiner der übertragenden Rechner den Klartext der Nachricht entziffern. Der Nachteilist jedoch, dass sich der Absender mit jedem möglichen Empfänger auf ein Verschlüsselungsverfahren und zugehörige(n) Schlüssel einigen muss.

**Verschlüsselung von Daten auf Datenträgern**

Wichtige Daten auf einem Datenträger lassen sich auf zwei Arten vor unbefugtem Zugriff schützen:

* man verschlüsselt mit Verschlüsselungssoftware die komplette Festplatte oder eine einzelne Teile oder auch nur einen Daten-Container in Form einer einzelnen Datei auf dem Datenträger
* bei der hardware-seitigen Verschlüsselung übernimmt ein Mikrochip auf dem USB-Laufwerk eine automatische und transparente Verschlüsselung. Die Authentifizierung wird z.B. erreicht, dass das Gerät über eine physische Tastatur verfügt, mit der man ein PIN-Code einzugeben kann

#### 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**

Bei der symmetrischen Verschlüsselung ist der Schlüssel dazu da auch zu Entschlüsseln

Symmetrische Verschlüsselungsprozesse verwenden zur Ver- und Entschlüsselung den selben Schlüssel. Bei historischen Verfahren lassen sich zwei Verschlüsselungsklassen unterscheiden. Bei der ersten werden 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 anderen Verschlüsselungsklasse, genannt Transposition (deutsch: „versetzen“), jeder Buchstabe wie er ist, aber nicht wo er ist. Sein Platz im Text wird geändert, die einzelnen Buchstaben des Textes werden aslo zufällig durcheinandergewürfelt. Eine einfache Form einer Transpositions-Verschlüsselung ist die „Revertierung“ (deutsch: „umkehren“) eines Textes. So entsteht z.B. aus dem Klartext „Geheimnis“ der Geheimtext SINMIEHEG.

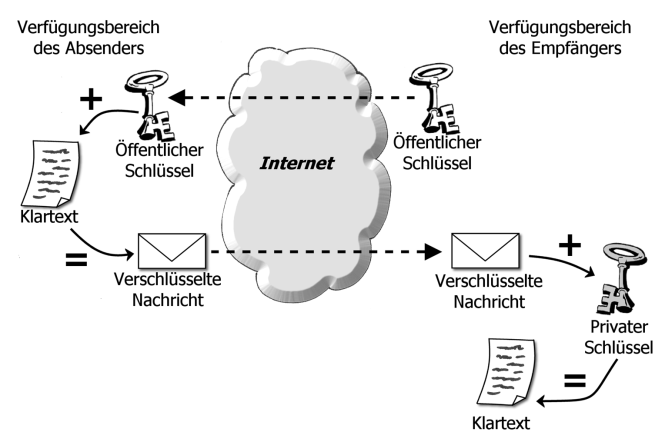
Bei aktuelleren symmetrischen Verfahren werden Stromverschlüsselung und auf einer Blockverschlüsselung basierende Verfahren unterschieden. Bei der Stromverschlüsselung werden die Zeichen des Klartextes alle einzeln und nacheinander verschlüsselt. Bei einer Blockverschlüsselung hingegen wird der Klartext zuerst in Blöcke einer bestimmten Größe aufgeteilt. Wie dann die Blöcke verschlüsselt werden, hängt von dem Betriebsmodus der Verschlüsselungsmethodeab.

**Asymmetrische Verschlüsselung**

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

Über viele Jahre war man der Meinung, dass es keine Alternative zur symmetrischen Verschlüsselung und dem damit verknüpften Schlüsselverteilungsproblem gäbe. Erst vor ein paar Jahrzehnten wurde die asymmetrische Verschlüsselung erfunden. Ein Merkmal der asymmetrischen Verschlüsselung ist, dass zur Verschlüsselung ein ganz anderer Schlüssel als zur Entschlüsselung verwendet wird. Man unterscheidet zwischen dem „öffentlichen Schlüssel“, der zum Verschlüsseln benutzt wird, und dem „privaten Schlüssel“ zum Entschlüsseln des Geheimtextes.

Da asymmetrische Verfahren algorithmisch aufwändiger sind als symmetrische und daher in der Ausführung etwas langsamer, werden in der Praxis oft Kombinationen aus beiden, sogenannte Hybrid-Verfahren genutzt. Dabei wird z.B. erster ein zufällig generierter individueller Sitzungsschlüssel mit einem asymmetrischen Verfahrens ausgetauscht, und dieser anschließend gemeinsam als Schlüssel für ein symmetrisches Verschlüsselungsverfahren benutzt, wodurch die eigentlich zu kommunizierende Information dann verschlüsselt wird.

<https://www.datenschutzzentrum.de/uploads/verschluesselung/Asymmetrische-Verschluesselung.png>