



Wissen Sie, was sich hinter dem Begriff Verschlüsselung verbirgt? Überlegen Sie, ob die Verschlüsselung auch im Internet Anwendung finden könnte.

## 2 Möglichkeiten der Verschlüsselung



„Gestern habe ich im Fernsehen einen spannenden Beitrag über Verschlüsselung gesehen,“ erzählt Ali seinen Freunden. „Wäre es nicht toll, wenn wir unsere Nachrichten und Daten auch verschlüsseln könnten?“ Alis Freunde sind begeistert, aber auch skeptisch: „Das können wir sicher nicht – das ist bestimmt viel zu kompliziert.“



### Meine Ziele

Nach Bearbeitung dieses Kapitels kann ich

- die Ziele der Verschlüsselung erklären und die Begriffe abgrenzen;
- Methoden der Verschlüsselung nennen;
- Notwendigkeit des Einsatzes von Verschlüsselung begründen;
- einfache Verschlüsselungsverfahren anwenden.

KOMPETENZ-  
ERWERB

### 2.1 Grundlagen der Verschlüsselung

Während die Verschlüsselung in den vergangenen Jahrhunderten meist militärisch genutzt wurde, bekommt sie in Zeiten des Internets, des elektronischen Handels und des elektronischen Zahlungsverkehrs eine erhebliche Bedeutung für das gesamte gesellschaftliche Leben. Auch wissenschaftliche oder wirtschaftliche Fakten müssen heutzutage sicher übermittelt werden können.

## Aufgaben und Anwendungen der Verschlüsselung

- die Ver- und Entschlüsselung vertraulicher Informationen,
- die Sicherstellung von Identitäten im Internet sowie
- die Sicherung von Verbindungen gegen Abhören.

Im Zusammenhang mit den Aufgaben und Anwendungen unterscheidet man folgende Begriffe:

Wichtige Begriffe	Erklärung
Kryptografie	Nachrichten ver- und entschlüsseln
Kryptoanalyse	Verschlüsselung knacken
Kryptologie	Kryptografie und Kryptoanalyse

## Wovon schützt Verschlüsselung?

**Sicherheit** wird heute in vielen Bereichen über Verschlüsselung gewährleistet.

- **Datenverlust:** entsteht durch versehentliches Löschen, durch Hardwarefehler, durch Viren und Würmer oder durch nicht berechtigte Zugriffe.
- **Vertrauensverlust:** entsteht durch Nachlässigkeiten der Anwender/innen, durch Zweifel an der Authentizität oder durch nicht berechtigte Zugriffe.

Die folgende Tabelle gibt einen Überblick über Bedrohungen und Gefährdungen, vor denen Methoden der Verschlüsselung Schutz bieten:

Bedrohung	Beschreibung
Schutz vor Lauschern	Niemand soll unerlaubt mithören können.
Schutz vor Eindringlingen	Niemand soll unerlaubt Zugang zu Daten erhalten können. Dazu werden kryptografische und biometrische Methoden verwendet.
Schutz vor Fälschung	Die Echtheit von Dokumenten soll sichergestellt werden. Mithilfe digitaler Unterschriften kann nachgewiesen werden, von wem ein Dokument stammt.
Schutz vor Diebstahl geistigen Eigentums	Mit digitalen Wasserzeichen können Daten so gekennzeichnet werden, dass beim Kopieren diese Kennzeichnung nicht gelöscht oder verändert werden kann.

**Verschlüsselung** wird in folgenden Bereichen eingesetzt:

- Telefonkarten, Handys, Fernbedienungen
- Geldautomaten, Geldverkehr zwischen Banken
- Electronic Cash, Onlinebanking, sichere E-Mails
- Pay-TV
- Wegfahrsperrern in Autos
- Sichere Datenübertragung, z. B. im Internet

## Ziele der Verschlüsselung

- **Vertraulichkeit:** Schutz vor unberechtigtem Lesen durch Chiffrierung (Verschlüsselung)
- **Echtheit und Verbindlichkeit:** Schutz vor unberechtigtem Schreiben und Verfälschung (= Integrität), Unbestreitbarkeit von Inhalt und Urheberschaft (Authentizität)
- **Anonymität:** Geheimhaltung von Sender oder Empfänger.

Systeme gelten als sicher, wenn Sie ausreichend gegen Datenverlust und Vertrauensverlust schützen.



Wussten Sie, dass schon vor den Zeiten der Computertechnologie Nachrichten verschlüsselt wurden? Zum Beispiel mit unsichtbarer Tinte oder mit Codes.

### Vorgehensweise

Bei der Verschlüsselung wird der Klartext nach einer bestimmten Methode in eine scheinbar sinnlose Zeichenfolge umgewandelt. Die dazu verwendeten Methoden basieren auf speziellen Techniken und Algorithmen.

#### Beispiel: Pretty Good Privacy

Die ursprüngliche Nachricht lautet:

Kauflimit 100.000,00 €, Abschluss innerhalb von drei Tagen erwünscht.

Daraus ergibt sich folgende verschlüsselte Nachricht:

```

— BEGIN PGP MESSAGE —
Version: PGP 5.5.3i qANQR1DBwU4DdF6xT2vS010QCADu5nmyhls6d3BUWO
Dof10os3uJWmHS0Ms485xBoH1i8Q5BhNQ2NEKvV+206u8b8xodES+X7CenJTZ3
IPrauOSlyUdwVrYdH9yhJMFdcyEGYBUGkKzP+WucTv2NC2VhyJyZkzV3SbFPq
qzIQf8zM9LIXilmctG5hiMFN5PAI9cwOSyeeapvQuellBebojefEslo==wExE
— END PGP MESSAGE —
    
```



Verschlüsselung

## 2.2 Klassische Verschlüsselungsverfahren

Zu den klassischen Verschlüsselungsverfahren zählen:

- Caesar-Chiffre
- Vigenère-Chiffre
- Monoalphabetische Substitution

### Caesar-Chiffre

Das Verschlüsselungsalphabet ist gegenüber dem normalen um einige Stellen verschoben. So wird beispielsweise aus A ein D, aus B ein E, aus C ein F oder aus L ein O. Ist man am Ende des Alphabets angelangt, setzt man an dessen Anfang fort. Mathematisch entspricht diese Verschlüsselung einer buchstabenweisen Addition. Die Buchstaben werden entsprechend der alphabetischen Reihenfolge von 0 bis 25 nummeriert, der entsprechende Wert der Buchstaben wird addiert, das Ergebnis entspricht dem neuen Buchstaben.

	C	C	C	C	C	C	C	C	C	Erläuterung
+	A	B	E	N	D	Z	E	I	T	2 (C) + 0 (A) = 2 (C)
=	C	D	G	P	F	B	G	K	V	2 (C) + 4 (E) = 6 (G)

Die **ältesten** bekannten Verschlüsselungsverfahren sind:

- **Tattoos** auf kahlgeschorenen Köpfen von Sklaven (verdeckt durch nachgewachsene Haare)
- **Atbasch**: hebräische Geheimschrift, umgedrehtes Alphabet (um 600 v. Chr.)
- **Skytale**: militärische Verschlüsselungsmethode aus Sparta (etwa 500 v. Chr.)

## Vigenère-Chiffre

Eine weitere Methode der Verschlüsselung ist die Verwendung eines Schlüssels, der durch Aneinanderreihung eines kurzen Wortes entsteht, z. B. des Wortes Zebra.

	Z	E	B	R	A	Z	E	B	R	Erläuterung
+	A	B	E	N	D	Z	E	I	T	25 (Z) + 0 (A) = 25 (Z)
-	Z	F	F	E	D	Y	I	J	K	4 (E) + 1 (B) = 5 (F)

## Monoalphabetische Substitution

Beim Substitutions-Verschlüsselungsverfahren wird jeder Buchstabe des Textes durch einen anderen Buchstaben des Alphabets ersetzt. Dabei werden gleiche Buchstaben im Text auch immer durch den gleichen Buchstaben ersetzt.

Der Unterschied zum Caesar-Verschlüsselungsverfahren besteht darin, dass die Buchstaben nicht in einer bestimmten Reihenfolge einander zugeordnet werden, sondern durcheinandergemischt werden können.

Dies macht sich auch in der Anzahl der möglichen Schlüssel bemerkbar: Gibt es beim Caesar-Verschlüsselungsverfahren 26 mögliche Schlüssel, so hat man bei dieser Art von Ersetzung bereits  $26! = 4 \cdot 1026$  mögliche Schlüssel.

## 2.3 Moderne Verschlüsselungsverfahren

Zu den **modernen Verschlüsselungsverfahren** zählen:

- Symmetrische Verfahren
- Asymmetrische Verfahren
- Hybridverfahren

### Symmetrische Verfahren

Die Ver- und Entschlüsselung erfolgt mit demselben geheimen Schlüssel. Typisches Anwendungsgebiet ist die vertrauliche Speicherung von Daten einer Benutzerin/ eines Benutzers oder von gemeinsam genutzten Daten einer Benutzergruppe auf einem Datenträger oder auf dem Server. Problematisch wird dieses Verfahren, wenn in einem Netz die einzelnen Benutzer/innen vertraulich miteinander kommunizieren wollen. Hier müssten immer paarweise Schlüssel vereinbart werden. Bei einem Netz mit hundert Personen würden 5 000 Schlüssel benötigt.

Eine weitere Schwachstelle dieses Verschlüsselungsverfahrens ist, dass der Empfängerin/dem Empfänger der Nachricht der Schlüssel bekannt gegeben werden muss, wodurch das Risiko erhöht wird, dass der Schlüssel entweder beim Versenden oder durch Unachtsamkeit in falsche Hände gelangt.

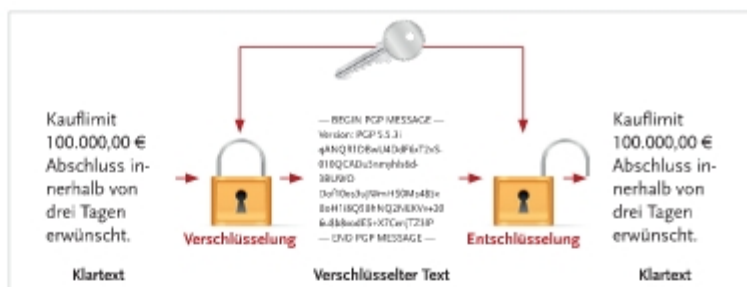
#### Beispiele: symmetrische Verfahren

- DES (Data Encryption Standard), Triple-DES
- RC2 und RC4
- Fortezza (PINs, TANs)
- IDEA (International Data Encryption Algorithm)
- AES (Advanced Encryption Standard)



Skytale





Verschlüsselung mit geheime Schlüssel

### Asymmetrische Verfahren

Dieses Verschlüsselungsverfahren verwendet Schlüsselpaare. Eine Nachricht wird nicht mehr mit ein und demselben Schlüssel ver- und entschlüsselt, sondern mit zwei unterschiedlichen, einander zugeordneten Schlüsseln. Ein Schlüssel ist der öffentliche Schlüssel (**Public Key**), da er öffentlich bekannt sein kann. Er wird verwendet, um eine Nachricht zu verschlüsseln. Der private Schlüssel (**Secret Key**) wird zur Decodierung genutzt. Wollen zwei Personen auf diese Art und Weise sicher miteinander kommunizieren, so müssen sie ihre öffentlichen Schlüssel austauschen.

Folgende Merkmale sind für ein asymmetrisches Verfahren typisch:

- Es werden zueinanderpassende Schlüsselpaare verwendet.
- Ein Schlüssel reicht zur Berechnung des anderen Schlüssels nicht aus.
- Der Secret Key wird nie aus der Hand gegeben.
- Der Public Key wird veröffentlicht und damit jedermann zugänglich gemacht.

#### Beispiele: asymmetrische Verfahren

- RSA (Rivest – Shamir – Adleman)
- DSS (Digital Signature Standard)



Verschlüsselung mit Schlüsselpaaren

### Hybridverfahren

Wegen des hohen Rechenaufwands, der mit asymmetrischen Verfahren verbunden ist, eignen sie sich nicht zur Verschlüsselung längerer Nachrichten. Dafür sind sogenannte Hybridverfahren besser geeignet, eine Kombination aus symmetrischen und asymmetrischen Verfahren.



Notizen

---



---



---



---



---



---



---



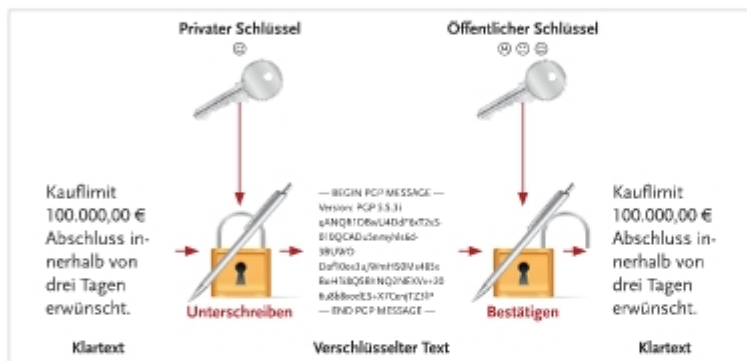
---

## 2.4 Digitale Signaturen

Digitale Signaturen werden für unterschiedliche Zwecke benötigt, besonders in der Rechts- und Finanzwelt. Sie sind mit einer Unterschrift oder einem Siegel gleichzusetzen, die die Echtheit von Dokumenten garantieren. Im Gegensatz zu herkömmlichen Dokumenten, bei denen diese Unterschriften gefälscht oder manipuliert werden könnten, sind digitale Signaturen fälschungssicher.

Die Signatur wird mit einem eindeutigen privaten Schlüssel erstellt und von den Empfängerinnen/Empfängern mit einem öffentlichen Schlüssel überprüft.

Eine digitale Signatur enthält zudem eine Zeitangabe mit dem Erstellungsdatum dieser Signatur, d. h. mit dem Zeitpunkt, zu dem das Dokument signiert wurde. Falls also jemand versucht, das Dokument nachträglich zu verändern, wird beim Überprüfen der Signatur eine Fehlermeldung ausgegeben.



Verschlüsselung – digitale Signatur

Die Signaturen können nach dem Konzept des Secret Key oder des Public Key realisiert sein.

Grundsätzlich sollen folgende Funktionen bereitgestellt werden:

- Die Empfängerinnen/Empfänger können die Identität der Senderinnen/Sender sicher verifizieren.
- Die Senderinnen/Sender können nachträglich das Abschicken der Nachricht nicht rückgängig machen.
- Die Empfängerinnen/Empfänger können die Nachricht nachträglich nicht modifizieren.

## 2.5 CRYPTOOL

CRYPTOOL ist ein kostenloses Programm – entwickelt von der Deutschen Bank –, mit dessen Hilfe kryptografische Verfahren angewendet und analysiert werden können. Sie können damit neue Dokumente erstellen und bestehende Dokumente öffnen und weiterbearbeiten. Ein Dokument kann mit verschiedenen Verschlüsselungsverfahren ver- und entschlüsselt werden.

Es stehen sowohl klassische (z. B. die Caesar-Chiffre) als auch moderne Kryptoverfahren (z. B. RSA) zur Verfügung. Außerdem kann CRYPTOOL von einem Dokument **Hashwerte** berechnen.



Die rechtliche Bedeutung digitaler Signaturen lernen Sie im nächsten Kapitel kennen.



CRYPTOOL finden Sie im Internet unter: [www.cryptool.de](http://www.cryptool.de)

**Hashwerte/-funktion** = Werte, mit denen überprüft wird, ob Daten verfälscht wurden.

Für die klassischen Verschlüsselungsverfahren stehen automatische Analysen zur Verfügung, mit denen Sie in der Lage sind, mit Kenntnis des verschlüsselten Dokuments und eventuell weiterer Informationen (unverschlüsseltes Dokument oder Sprache des Dokuments) den Schlüssel zu ermitteln.

### Beispiel: Caesar-Chiffre mit CRYPTOOL

Schlüsseingabe: Caesar / ROT-13

**Beschreibung**  
Hier können Sie für das Caesar-Verfahren den Schlüssel eingeben. Caesar ist eine monoalphabetische Substitution, bei der die Zeichen des Klartext Alphabets durch Shifts um einen bestimmten Wert auf der Geheimtext-Alphabet abgebildet werden. Dieser Verschiebewert ist der Schlüssel. Sie können den Schlüssel sowohl als Zahl als auch als einzelnes Alphabet-Zeichen eingeben.  
Rot-13 ist ein Spezialfall, bei dem der Schlüssel fest auf den Wert der halben Länge des Klartext-Alphabets gesetzt wird. Diese Variante ist nur wählbar, wenn die Länge des Alphabets eine gerade Zahl ist.

**Variante auswählen**

Caesar  
 Rot-13

**Interpretation des ersten Alphabetzeichers**

Wert des ersten Alphabetzeichers = 0 (z.B. 'A'='0')  
 Wert des ersten Alphabetzeichers = 1 (z.B. 'A'='1')

**Schlüsseingabe**

Alphabetzeichen    
 Zahlenwert

**Informationen zur Verschlüsselung**

Verschiebung um 6  
Das Alphabet (26 Zeichen) wird bei der Verschlüsselung abgebildet

von:   
auf:

### CRYPTOOL: Caesar – Schlüsseingabe

Cryp Tool 1.4.31 Beta 86 (VS2008) - Caesar-Verschlüsselung von <startbeispiel-de>, Schlüssel <G, KEY OFF...

Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/FK0 Einzelverfahren Analyse Optionen Fenster Hilfe

Startbeispiel-de

Startbeispiel zur CrypTool-Versionsfamilie 1.x (CT1)

CrypTool 1 (CT1) ist ein umfangreiches freies Lernprogramm zu den Themen Kryptographie und Kryptoanalyse mit ausführlicher Online-Hilfe.

Dies ist eine Textdatei

1) Den besten Überblick über die Windows-Online-Funktionen über Link Die Startseite selbst der Online-Hilfe im Internet können die Online-Hilfe aufrufen.

2) Als nächstes können über das Menü "Ver-

Caesar-Verschlüsselung von <startbeispiel-de>, Schlüssel <G, KEY OFFSET 0>

Yzgzthkoyvotr fax kexZuorBkoyouytpgorok 1.d (Z1)

breZuor 1 (Z1) oyz kot aslgtmkoinly ikokoly Rlohoumzogs fa jrt Znkst Qwezumogmekt atj Qwezugtreyk soz gaykxrooinxk Utratk-Norik atj soz bekind Bloyagroyokotemk.

Jokly oyz kotk Zkdzgzko, soz jox Yok Onrk koykt Yirkozsk soz IZ1 sginkt qötkit.

1) Jit hiyekt Ühlohreig ühix jok Somroinkozit but IZ1 holizkt jok "Yzgzzykozzi", jok yoin ot jox Cotjacy-Utratk-Norik hlotjiz. But jox Yzgzzykozsk gay qötkit Yok grk ckykztzoinkt Latzouitk ühix Rotzgy lookoinkt. Jok Yzgzzykozsk ylerhyz lookoinkt Yok ühix jgy Siktü "Norik" -> Yzgzzykozsk", ujox otjox Yok ot jox Utratk-Norik os Ojkd jkt Hkuxoll "Yzgzzykozsk" kotmkhkt. Yok qötkit jok Utratk-Norik soz L1 gt pljox Yzlenk ot IZ1 ötkit.

2) Gry Tänyzky qötkitk Yok kotk Jgzko f.H. soz jks lgykgy-Blozdnokt bkoyimryyykt - ühix jgy Siktü "Blox-fkzyimryyykt" -> Yesskzoxyn (arggyoyin)

Drücken Sie F1, um die Hilfe aufzurufen

Z:1 S:1 P:1

### CRYPTOOL: Caesar – Verschlüsselung



Notizen

## 2.6 Verschlüsselungsprotokolle

Damit Daten online sicher übertragen werden können, kommen verschiedene Verschlüsselungsprotokolle zum Einsatz.

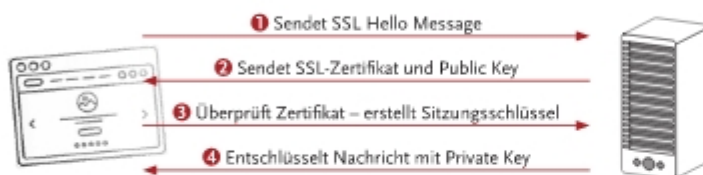
### Secure Socket Layer und Transport Layer Security

**SSL** ist ein Protokoll zur Authentifizierung und Verschlüsselung von Internetverbindungen. Die Echtheit des kontaktierten Servers wird durch ein Zertifikat garantiert und die Verbindung zwischen Server und Client verschlüsselt. **TLS** ist eine Weiterentwicklung von SSL.

#### Beispiel:

Anwendung finden das SSL- bzw. TLS-Protokoll für HTTPS z. B. bei Onlinebanking oder Onlineshopping.

#### Vereinfachter Aufbau einer HTTPS-Verbindung



1. Browser sendet eine SSL Hello Message an den Server. Die Nachricht beinhaltet:
  - Vom Browser unterstützte SSL- bzw. TLS-Versionen
  - Genutzter Hash-Algorithmus
  - Informationen, ob Komprimierung unterstützt wird
2. Server antwortet mit SSL-Zertifikat und sendet seinen Public Key. Server wählt die höchste, von Browser und Server unterstützte SSL- bzw. TLS-Version.
3. Der Browser überprüft das Zertifikat des Servers. Ist es gültig, wird ein Sitzungsschlüssel erstellt. Dieser wird mit dem Public Key des Servers verschlüsselt und gesendet.
4. Mithilfe seines Private Keys entschlüsselt der Server die Nachricht. Mit dem so erhaltenen symmetrischen Sitzungsschlüssel wird die weitere Verbindung verschlüsselt.

### GNU Privacy Guard

**GPG** ist eine Weiterentwicklung von **PGP**, das von Phil Zimmermann entwickelt wurde. Dieser Verschlüsselungsstandard wird für E-Mails verwendet. Es basiert auf einem gegenseitigen Vertrauensmodell zwischen Menschen die ihren öffentlichen Schlüssel gegenseitig austauschen und die Identität und Vertrauenswürdigkeit damit bestätigen.

### Verschlüsselungsprotokolle im WLAN


**WEP** wurde zur Authentifizierung, Verschlüsselung und Integritätsprüfung von WLANs entwickelt. Es sollten damit WLANs genauso sicher wie ein kabelgebundenes Netzwerk werden.

Nachfolger von WEP ist **WPA** und **WPA2**. Ab 2014 dürfen WLAN-Geräte kein WEP mehr unterstützen, da der WEP-Standard als anfällig für Angriffe gilt.

**SSL** = Secure Socket Layer

**TLS** = Transport Layer Security



Eine verschlüsselte Verbindung erkennen Sie in ihrem Browser an dem „s“ bei http, also https. Zusätzlich weist ein kleines Schloss  auf die Verschlüsselung hin.



**GPG** = GNU Privacy Guard

**PGP** = Pretty Good Privacy

**WEP** = Wired Equivalent Privacy

**WPA** = WiFi Protected Access

**WPA2** = WiFi Protected Access 2.



WPA2 verwendet den symmetrischen Verschlüsselungsalgorithmus **AES** (Advanced Encryption Standard).



**Tipp!**

Bei neuen WLAN-Routern ist die WPA2-Verschlüsselung standardmäßig aktiviert. Überprüfen Sie die Einstellungen trotzdem und wählen Sie ein sicheres Passwort. Die beste Verschlüsselung wird nutzlos bei schlechten Passwörtern.