
Kryptographie
Die Verschlüsselung von Informationen
im digitalen Zeitalter

# Kryptographie – Die Verschlüsselung von Informationen im digitalen Zeitalter

Seit es Menschen gibt, gibt es **Geheimnisse**. Manche Informationen sind einfach **nicht für jeden bestimmt** und das Miteinander erscheint weniger kompliziert, wenn nicht alles gerechtfertigt werden muss. Solange also ein **Geheimnisträger** verschwiegen ist, scheint auch das **Geheimnis sicher** zu sein.

Allerdings ist das menschliche Gehirn ein **unzuverlässiger Speicher** und kein dauerhaft sicherer Ort für eine Information, die **unverfälscht** aufbewahrt werden soll. Sicherer ist eine **Niederschrift**. Eine Notiz oder ein Brief garantiert eine **exaktere Wiedergabe der Information**, als es das Gedächtnis könnte. Doch sobald die Information auf einem Zettel **physische Gestalt** angenommen hat, wird sie angreifbar.

Zettel können **verloren** gehen oder entwendet werden. Briefe können **abgefangen** und gelesen werden. Mit diesem Problem waren schon **geheime Liebespaare in der Antike** konfrontiert, genauso wie die Generäle von Armeen. Obwohl mit sehr unterschiedlichen Absichten wollten sowohl das Pärchen als auch die Heerführer nicht, dass ihre Briefwechsel **von unbefugten Dritten** entdeckt und gelesen werden.

Das erschwert den Austausch von Informationen und der einzige Ausweg scheint die **Befestigung der Kommunikationswege** zu sein. Eine Möglichkeit wäre ein **eingeschworener Bote**. Doch auch diese können auf verschiedene Weise dazu gebracht werden, die Nachricht herauszugeben. Damit ist **das zentrale Problem** immer noch nicht gelöst. Wie kann verhindert werden, dass jemand anders als der bestimmte Empfänger **auf den Inhalt der Nachricht** zugreifen kann?

Schon in der Antike entwickelten sich die Methoden, die auch **heute noch angewendet** werden, um Nachrichten zu verschleiern und zu verschlüsseln. Auf der einen Seite die **Steganographie**, die Kunst Nachrichten in einem Medium zu verbergen. Und auf der anderen Seite die **Kryptographie**, die Kunst Nachrichten unlesbar zu machen. →

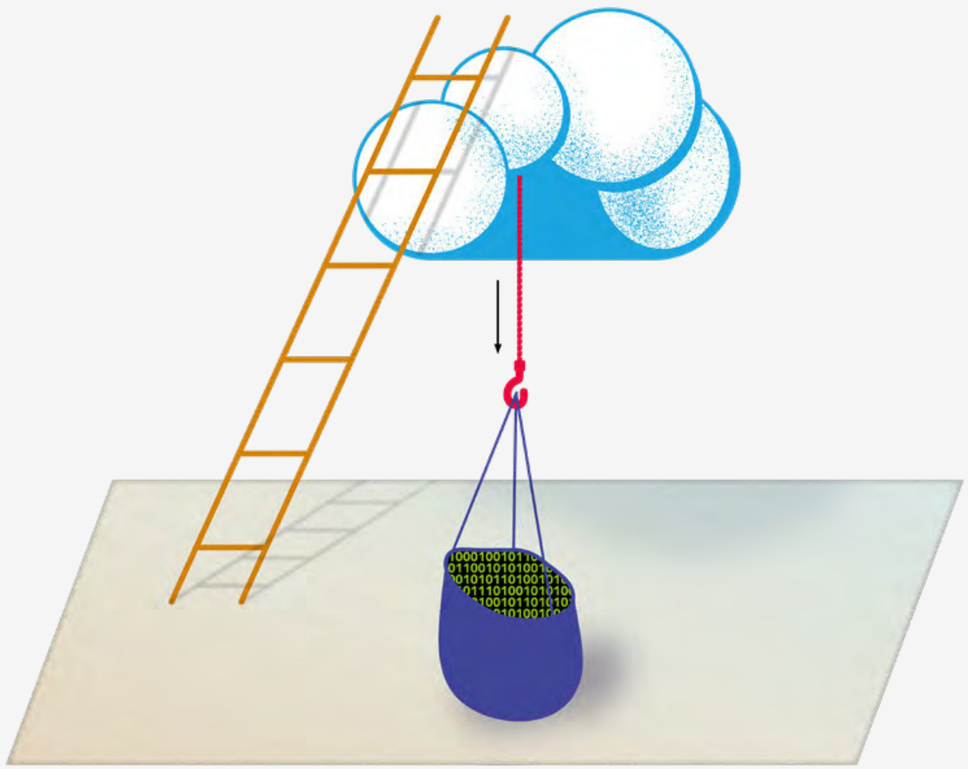
Während die Steganographie beinahe nur noch in **Agentenfilmen** anzutreffen ist, füllt Kryptologie **Hörsäle und Fachbücher**. Seit der massenhaften Digitalisierung und dem Aufkommen der automatisierten Verarbeitung personenbezogener Daten ist die Kryptologie auch in den **Alltag der Normalbürger** eingekehrt. Nachdem aufgedeckt wurde, mit welchem Eifer **die Geheimdienste der Industtrienationen** ohne Anlass Daten sammeln und auswerten, wurde die Bedeutung von Maßnahmen für die eigene Datensicherheit immer klarer.

Nachdem die **Aufdeckung der Geheimdienstaktivitäten** begannen die ersten Personen damit, all ihre elektrische Kommunikation zu verschlüsseln. Flächendeckendes **Interesse für Datensicherheit** lösten jedoch Ereignisse wie das sogenannte „Fappening“ aus. Durch die Ausnutzung einer Schwachstelle wurden aus der **Apple iCloud** eine große Menge Bilder **ausgeleitet und veröffentlicht**. Darunter befanden sich auch private Nacktfotos von prominenten Personen. Mit diesem Ereignis wurde allen, die das Internet für scheinbar **alltägliche Belanglosigkeiten** nutzen, klar, dass die eigenen Daten in den Weiten des Internets nicht zwangsläufig sicher sind.

In diesem E-Book möchten wir Ihnen die **Herkunft, Bedeutung und Funktion** von Kryptographie und kryptographischen Verfahren näherbringen. Dazu werden wir auf die **Geschichte und klassischen Probleme** der Kryptographie eingehen, die heute noch so aktuell sind, wie sie es in der Antike waren und auch durch die **Digitalisierung** nur wenig komplexer geworden sind.

# Inhalt





# Geschichte der Methoden um Nachrichten zu schützen

## Steganographie: Die Kunst Nachrichten zu verstecken

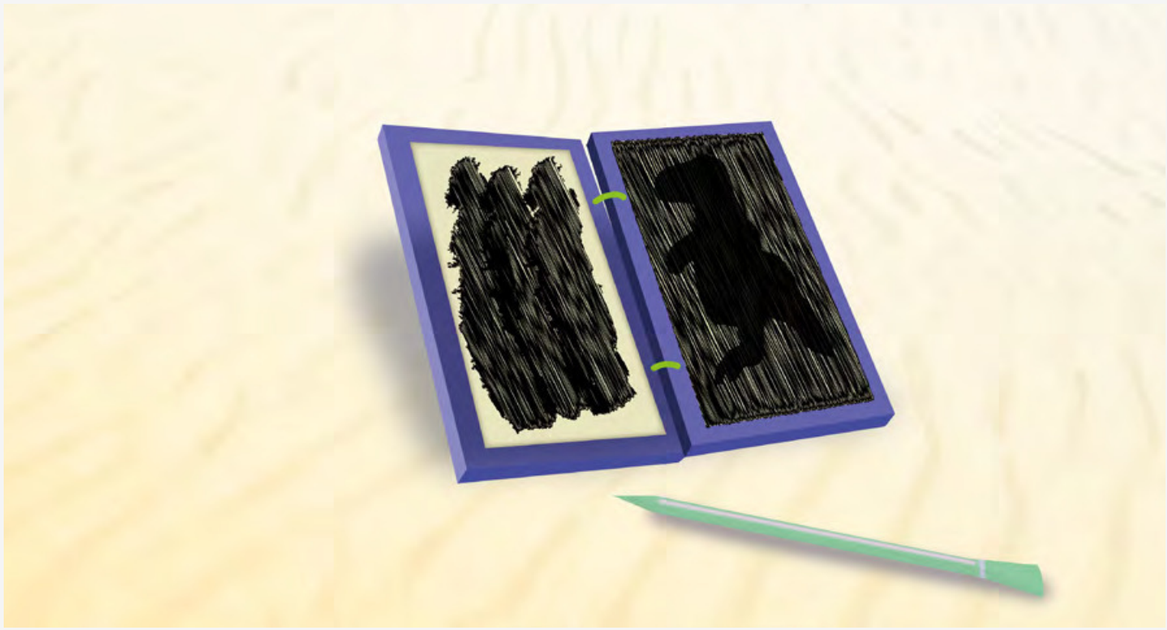
Bevor eine **Nachricht** gelesen werden kann, muss sie erst einmal entdeckt werden. Deswegen ist eine der ersten Methoden, mit der der **Schutz von Informationen** ermöglicht werden sollte, die Steganographie. Diese Kunst versucht **Nachrichten zu verstecken**, so dass die bloße Existenz der Nachricht für den **Uneingeweihten** nicht ersichtlich ist.

Der Grieche **Herodot** schrieb im 5. Jahrhundert vor Christus darüber, wie ein junger Grieche in der Verbannung die **Aufrüstung Persiens** beobachtet. Um seine Heimat zu beschützen, möchte er eine Nachricht schicken, doch die Wege werden von den Persern **kontrolliert**. Also nimmt der junge Grieche eine **Wachstafel** (das übliche Schreibgerät zu der Zeit), entfernt das Wachs und ritzt die Nachricht **in das Holz der Tafel**. Nach getaner Arbeit platziert er das Wachs wieder auf dem Holz und die **Warnung** gelangt unerkannt nach Sparta.

Doch wie die meisten griechischen Mythen ist auch dieser Mythos zum Teil ein **Lehrstück**. Denn in Sparta **wussten die Griechen nichts** von einer geheimen Botschaft. Das Dilemma konnte gelöst werden, als eine sparsame Frau etwas **Wachs für Kerze**n von der Tafel nahm und die Nachricht entdeckte. So wurden die Griechen **gewarnt** und die Perser trafen auf ein gerüstetes Heer als sie einen überraschten Feind erwarteten.

Doch **das zentrale Problem** bleibt bestehen. Geheime Botschaften benötigen ein **gemeinsames Geheimnis**. Ob es das Wissen darum ist, wo die Nachricht versteckt ist oder der **Schlüssel zum Entziffern** einer Chiffre. Die Grundlage stellt jeweils ein geteiltes Geheimnis dar.

Obwohl Steganographie in der elektronischen Datenverarbeitung **keine große oder relevante Rolle** mehr spielt, werden manchmal auch **Dateien in Dateien versteckt**. Damit lässt sich **die Existenz** von elektronischen Daten jedoch nur oberflächlich und für das ungeschulte menschliche Auge verbergen. Datenverarbeitungsprogramme lassen sich **nicht so leicht überlisten**.



# Kryptographie: Die Kunst den Inhalt unleserlich zu machen

Obwohl Steganographie **ein gewisses Maß an Sicherheit** bietet, funktioniert sie in erster Linie dann, wenn der potenzielle Angreifer nichts von der Nachricht weiß. Wenn damit gerechnet werden muss, dass die Nachricht abgefangen wird, ist **der Punkt erreicht**, an dem nur noch eine Verschlüsselung der Nachricht die Information **vor Unbefugten schützen** kann.

Kryptographische Methoden sind **mindestens genauso alt** wie steganographische. Jedoch hat sich die Kryptographie im Laufe der Jahre **zu einer Wissenschaft gemausert**, die zwischen Mathematik und Informatik einen festen Platz gefunden hat. Was **im Altertum** als valide Verschlüsselungsmethode galt wird heute in Form von Rätselheften verkauft und stellt kaum mehr als **ein aufwändiges Logikrätsel** dar. Grundlegend unterscheiden sich **in der Kryptographie** zwei unterschiedliche Methoden: Die **Transposition** und die **Substitution**. Beide waren großer Bedeutung, als Informationen und Nachrichten noch **an Boten und Briefe** gebunden waren.

## *Transposition*

Die Transposition macht **die Nachricht unleserlich**, indem einzelnen Buchstaben vertauscht werden oder zusätzliche Zeichen zwischen den relevanten Buchstaben gestreut werden. So wird **nach einem bestimmten Muster die Nachricht zerhackt** und unleserlich gemacht.

Ein altes Beispiel für diese Art der Verschlüsselung ist die **Skytale**. Der eckige Stab wurde im antiken Griechenland verwendet. Wieder waren es **die kriegerischen Spartaner**, die ihre Kommunikation **vor feindlichem Zugriff** schützen wollten und so eins der ersten kryptographischen Verfahren anwendeten.

Dazu wurde **ein Stück Stoff oder Leder** um einen eckigen Stab gewunden und dann senkrecht zur Richtung des gewickelten Materials **beschrieben**. Wenn der Streifen wieder abgewickelt wurde, waren die Buchstaben **nicht mehr geordnet** und konnten nicht ohne weiteres gelesen werden.

### *Substitution*

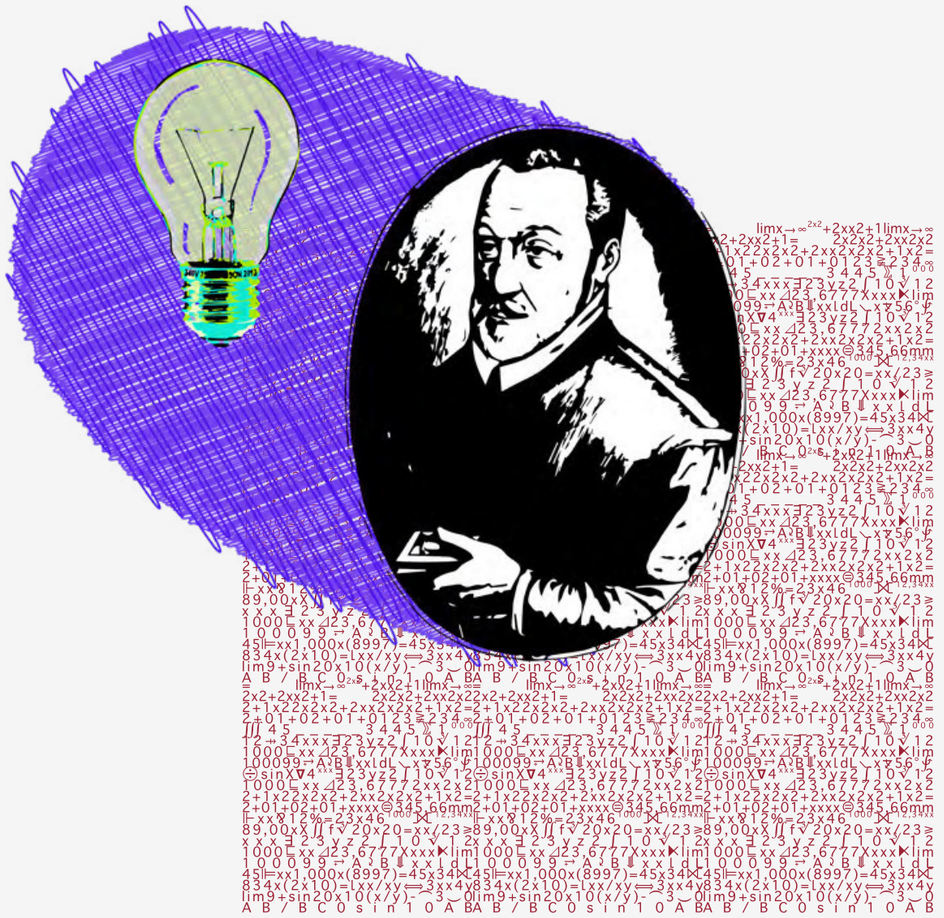
Bei der Substitution wird **nicht die Ordnung der Zeichen** gestört, um dem Leser die Information vorzuenthalten, sondern Zeichen **werden durch andere Zeichen ersetzt**. Nachdem die Kunst der Verschlüsselung **im antiken Griechenland** blühte, ist aus dem dunklen Mittelalter wenig darüber bekannt, **ob und wie** Nachrichten geschützt wurden.

Erst im **15. Jahrhundert** erblühte die Kryptographie in den italienischen Stadtstaaten. Diese konkurrierten wirtschaftlich und militärisch. Eben diese Konkurrenz **begünstigte die Entwicklung** von Agentennetzwerken und damit auch die Entwicklung für und gegen die **Verschlüsselung von Nachrichten**.

Denn während die **Herrscher der italienischen Kleinstaaten** eine sichere Methode suchten, ihre Nachrichten zu schützen, arbeiteten mindestens genauso viele Leute daran, die aufwändigen **Codes zu knacken** und die Nachrichten aus den verschlüsselten Dokumenten herauszukitzeln.

Seit der Antike hatte die Verschlüsselung keine solche Blüte, wie **in den Tagen der Renaissance**. Der akademische Austausch und **der Druck nationaler Konkurrenz** beschleunigte die Entwicklung der Verschlüsselung ungemein. Hier wurde Verschlüsselung soweit weiterentwickelt, dass sie letztendlich eine **Disziplin der Mathematik** geworden ist.

Einfache monoalphabetische Verschlüsselungen wurden durch **sequenzielle oder polyalphabetische Verschlüsselung** ersetzt und die Verfahren, die bereits geknackt wurden, konnten Stück für Stück ersetzt werden und der Grundstein für **modern mathematikbasierte Verschlüsselung** wurde gelegt.



# Grundbegriffe der Kryptographie

Spätestens seit sich die Kryptographie zur Wissenschaft erhoben hat, sind einige Begriffe immer wieder in der gleichen Weise gebraucht worden und haben sich so als Grundbegriffe der Kryptographie etabliert. Ein Überblick über diese Begriffe soll hier geboten werden.

### *Klartext*

Klartext ist der Terminus, der die geschriebene Nachricht bezeichnet. Im Klartext sind alle Informationen, die kryptographisch verschleiert werden sollen, einsehbar.

### *Geheimtext*

Der Geheimtext ist der Text, der sich aus der Anwendung eines kryptographischen Verfahrens auf einen Klartext (oder einen bereits bestehenden Geheimtext) ergibt.

### *Schlüssel*

Der Schlüssel ist das notwendige Geheimnis, dass bestenfalls nur dem Sender und dem Empfänger bekannt ist. Ein Schlüssel kann ein Wort, ein komplexer Satz, eine Zahl oder ein beliebige Zeichenfolge sein. Er ist nötig um einen Klartext zu ver- oder zu entschlüsseln. Meistens gibt das Verfahren vor, wie der Schlüssel aussehen kann.

### *Monoalphabetische Verschlüsselung*

Bei dieser Art der Verschlüsselung werden einzelne Zeichen des Klartextes durch andere Zeichen eines Schlüsselalphabets ersetzt. Je nach Länge und Komplexität von verwendetem Alphabet und Schlüssel dauert es unterschiedlich lang den Code zu knacken.

### *Polyalphabetische Verschlüsselung*

Bei der polyalphabetischen Verschlüsselung wird der Klartext mit einem fortlaufenden Schlüsselalphabet in unlesbaren Geheimtext umgewandelt. Dabei bestimmen Länge und Komplexität des Schlüssels die Sicherheit der Verschlüsselung, bis hin zum sogenannten One-Time-Pad, das als unknackbar gilt.

### *Symmetrische Verschlüsselung*

Sowohl das monoalphabetische Verfahren wie auch die polyalphabetische Verschlüsselung stellen Varianten der symmetrischen Verschlüsselung dar. Bei dieser Art der Kryptographie wird derselbe Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet. Dieser Schlüssel muss jedoch auch übertragen werden, wodurch dieser wiederum zum Ziel für Angreifer werden kann.

### *Asymmetrische Verschlüsselung*

Bei der asymmetrischen Verschlüsselung wird mit zwei unterschiedlichen Schlüsseln ver- und entschlüsselt. Die etablierten Varianten verwenden dabei einen öffentlichen Schlüssel (public key) um Daten zu verschlüsseln. Dieser öffentliche Schlüssel ist (wie der Name schon sagt) nicht geheim. Unter Verschluss ist nur der private Schlüssel (private key), mit dem die Daten bzw. der Geheimtext wieder entschlüsselt werden kann, um dann unverschlüsselt als Klartext lesbar zu sein.

# Klassische Verschlüsselungsverfahren

**Ab diesem Punkt** verwandelte sich die Kryptographie in eine **Wettbewerbsdisziplin der europäischen Geheimdienste**. Verschiedene Verfahren wurden entwickelt, eingesetzt, geknackt und landeten dann meist im Geschichtsbuch der vormals unknackbaren Verschlüsselungen. Nur wenige Methoden haben sich **als funktional erwiesen**, so dass sie auch den modernen Ansprüchen an Verschlüsselung genügen können.

## *Caesar-Verschlüsselung*

Eine der **einfachsten Arten** der Verschlüsselung ist die sogenannte **Caesar-Verschlüsselung**. Hierbei wird das Alphabet einfach „**verschoben**“. Der Wert der Verschiebung bzw. das aus der Verschiebung **resultierende Alphabet** ist dann der Schlüssel. Die Zeichen, deren **modifizierter Wert** über den höchsten Wert hinausgeht, beginnen die Folge **wieder von vorn**. (1)

Mit dieser Verschiebung kann ein Satz **bis zur Unleserlichkeit entstellt** werden, wie das folgende Beispiel mit einer klassischen Geheimbotschaft zeigt. (2)

Diese Verschlüsselung wird heute **nur noch spielerisch** verwendet und stellt mit seiner begrenzten Varianz von **26 möglichen Verschlüsselungen** für kaum jemanden ein Hindernis dar, wobei eine dieser Verschlüsselungen den Klartext als Geheimtext ausgibt und somit **nutzlos** ist.

1.

| Klaralphabet | A | B | C | D | E | ... | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|
| Zahlenwert | 1 | 2 | 3 | 4 | 5 | ... | 23 | 24 | 25 | 26 |
| Schlüsselwert | +3 | +3 | +3 | +3 | +3 | ... | +3 | +3 | +3 | +3 |
| Zahlenwert | 4 | 5 | 6 | 7 | 8 | ... | 26 | 1 | 2 | 3 |
| Geheimalphabet | D | E | F | G | H | ... | Z | A | B | C |

2.

| Klaralphabet | I | C | H | L | I | E | B | E | D | I | C | H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Zahlenwert | 9 | 3 | 8 | 12 | 9 | 5 | 2 | 5 | 4 | 9 | 3 | 8 |
| Schlüsselwert | +7 | +7 | +7 | +7 | +7 | +7 | +7 | +7 | +7 | +7 | +7 | +7 |
| Zahlenwert | 16 | 10 | 15 | 18 | 16 | 12 | 9 | 12 | 11 | 16 | 10 | 15 |
| Geheimalphabet | P | J | O | S | P | L | I | L | K | P | J | O |

## *Vigenére-Verschlüsselung*

Eine **sicherere Variante** ist da eine polyalphabetische Substitution, wie die Vigenére-Verschlüsselung. Hierbei werden die **26 Alphabete der Caesar-Verschlüsselung** verwendet, um die Änderung nicht linear berechenbar zu machen. Der Schlüssel ist dann ein **Kennwort, -satz oder –text**, der die Reihenfolge der anzuwendenden Alphabete bestimmt.

Bei unserem Beispiel **verschlüsseln** wir wieder den Satz „Ich liebe dich“ ohne die Leerzeichen mit **dem berühmten Kennwort** „Kennwort“. Dazu verschlüsseln wir **das erste Zeichen** des Klartextes mit **dem korrespondierenden Zeichen** des Kennworts im Vigenére-Quadrat. In **Spalte I** wird das I also durch das korrespondierende Zeichen der **Zeile K** ersetzt. Damit ist die Nachricht „Ich liebe dich“ in den **Geheimtext** „SGUYESSXNMPU“ übertragen und ist **ohne den Schlüssel** „Kennwort“ nicht zu entziffern. Dieses Verfahren **erfüllt** einen der modernen Ansprüche an Verschlüsselung. Die Sicherheit basiert nicht auf der **Unkenntnis des Verschlüsselungssystems** sondern auf der Geheimhaltung des Schlüssels.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Klartext** | I | C | H | L | I | E | B | E | D | I | C | H |
| **Referenzzeile** | K | E | N | N | W | O | R | T | K | E | N | N |
| **Geheimtext** | S | G | U | Y | E | S | S | X | N | M | P | U |

Klartext

| Schlüssel | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Das **One-Time-Pad** ist ein Sonderfall der Vigenére-Verschlüsselung. Hierbei ist der Schlüssel **genauso lang**, wie der Klartext. Technisch gesprochen werden die beiden „Texte“ **addiert**. Das bietet die Möglichkeit, die **Schlüsselübertragung** sicherer zu gestalten. Beispielsweise könnte der **Text berühmter Bücher** verwendet werden, um den Klartext zu verschlüsseln. Dann muss **nicht der ganze Schlüssel** sondern nur eine Seiten- oder Kapitelnummer übertragen werden, die einem Mithörer **ohne Kontext** auch nicht weiterhilft. Im Gegensatz zur Vigenére-Verschlüsselung mit einem **sich wiederholenden Schlüssel** kann das One-Time-Pad faktisch nicht geknackt werden, wenn nicht derselbe Text mehrmals als Schlüssel verwendet wird. Eine Wiederholung des Schlüssels würde **das notwendige Muster** bieten, um die Verschlüsselung zu knacken.

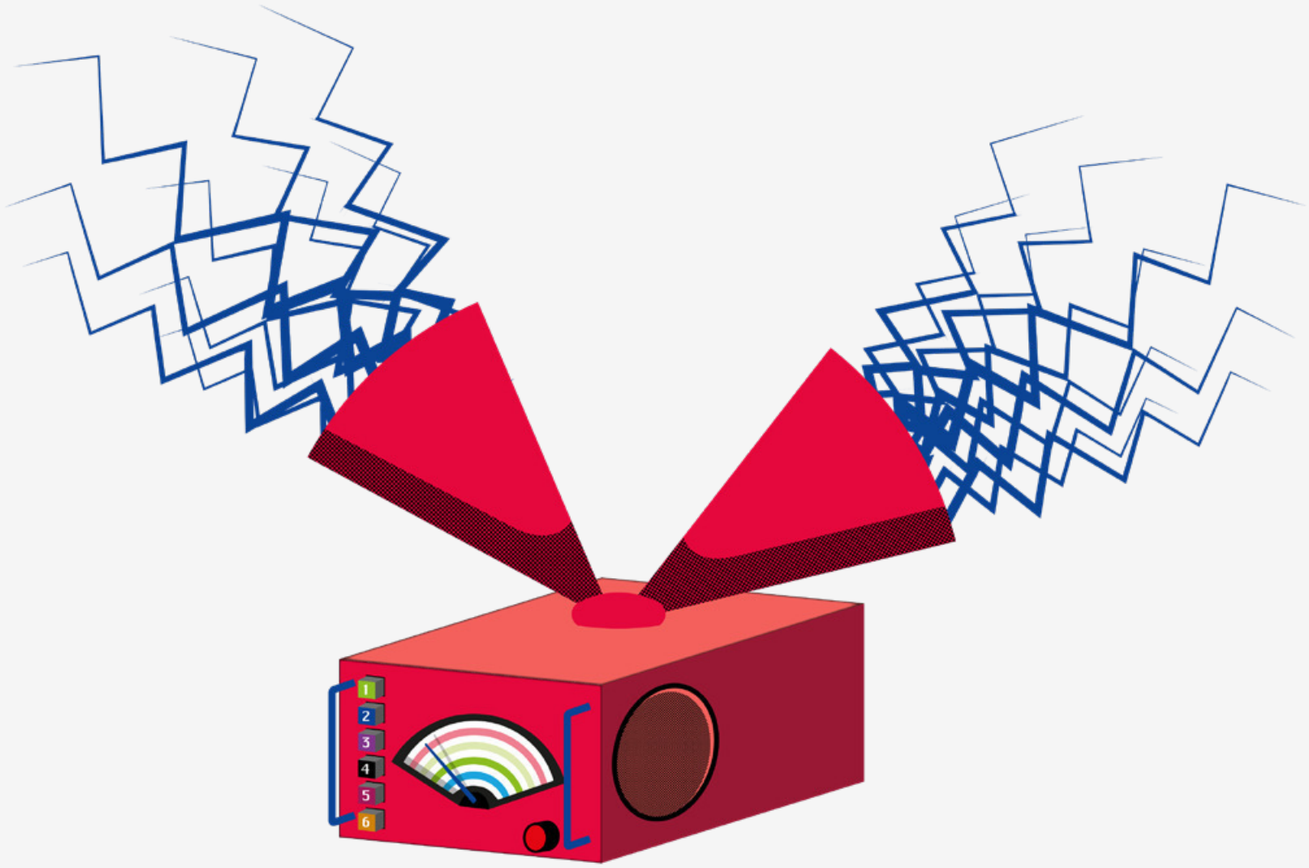
Damit ist auch **das zentrale Problem der klassischen Verschlüsselungen** benannt. Mit der modernen Rechentechnik und den Möglichkeiten schnell aus großen Datensätzen **Muster zu isolieren** sind die Verschlüsselungen **kaum noch geeignet**, Nachrichten oder Datenbestände zu sichern.

# Moderne Verschlüsselungsverfahren

Mit den **modernen Möglichkeiten** und den veränderten Ansprüchen der Kommunikation wurde eine **neue Methode der Sicherung** gebraucht. Damit wurden **mathematische Verfahren** zur Verschlüsslung interessant.

Noch lange vor der **massenhaften Verbreitung von Computern** wurde Verschlüsselung in Europa immer wichtiger in den vielen Kriegen des vormodernen Europa wurde nicht nur die **Waffentechnologie** sondern auch die Nachrichtenübermittlung weiterentwickelt und musste sich bald an die **Bedürfnisse der Telegraphie** anpassen.

Mit **kabelgebundenen Nachrichten** wurde Abhören auf technischer Ebene leichter. Im gleichen Maß entwickelte sich auch die **Verschlüsselungstechnik**. Anfangs stützte sich die gesamte geheime Kommunikation auf den **Funker**. Dieser Fachmann war mit einem Codebuch ausgestattet und **übersetzte synchron** die Nachrichten, die verschlüsselt übertragen wurden. Wieder entbrannte ein **Wettrennen** zwischen Verschlüsslungsschaffenden (codemaker) und den Verschlüsselungsknackern (codebreaker). →



Als die deutschen Streitkräfte **nach dem ersten Weltkrieg** begannen, verschlüsselte Nachrichten zu versenden, standen **die Kryptographen Europas** vor einer Herausforderung, die unlösbar schien. Mit der ENIGMA-Maschine gelang es **deutschen Ingenieuren** eine Verschlüsselungsmaschine zu bauen, die äußerlich **wie eine Schreibmaschine** funktionierte. Mit einer Schlüsseleinstellung wurde **die Ausgabe beeinflusst** und konnte erst durch Eingabe in eine zweite ENIGMA mit **gleicher Schlüsseleinstellung** wieder entschlüsselt werden.

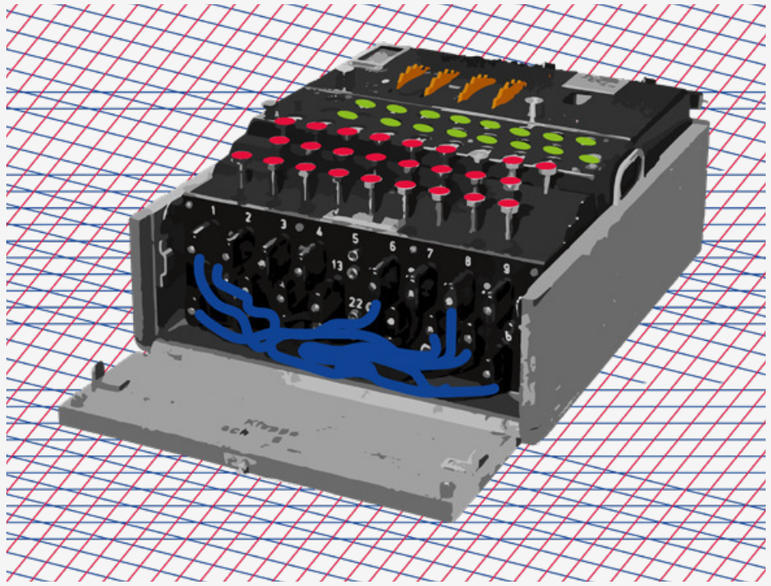
Lange Zeit galt diese Technologie als **unbezwingbar**. Doch sowohl in Polen als auch in Großbritannien gelang es Kryptographen **das gesamte System zu entschlüsseln**. Damit war die Kommunikation der Deutschen korrumpiert. Dieser Fall zeigt wieder einleuchtend, was **eine der Grundannahmen der modernen Verschlüsselung** ist. Sicherheit erwächst nicht aus der **Unkenntnis des Verschlüsselungssystems** (security-by-oscurity). Sicherheit kann nur **in einem sicheren System** geschaffen werden (security-by-design).

In der Zeit des **kalten Krieges** explodierte das Interesse an kryptographischen Verfahren. Da **Telefonsysteme** aber zum größten Teil in **zentral staatlicher Hand** waren, erlebte auch die Steganographie eine Renaissance. Doch immer noch war Ver- und Entschlüsseln eine **aufwändige Handarbeit**, die zwar durch Maschinen erleichtert werden konnte, aber immer einen Menschen brauchte, der das Ergebnis auswertet.

Das änderte **die Verbreitung von Computern** im Alltag der Zivilbevölkerung und die mit dem Internet verbundene **massenhafte Bereitstellung** von Rohdaten. Mit der Geschwindigkeit von Computern können zwar **große Datenmengen** schnell verarbeitet, also auch verschlüsselt werden, jedoch ist es auch für Computer möglich mit roher Gewalt (brute force) zu versuchen, eine **Verschlüsselung zu knacken**.

Dabei werden **alle möglichen Verfahren und Schlüssel** ausprobiert, bis ein sinnvolles Ergebnis ausgegeben wird. Klassische Verfahren sind damit **wirkungslos**. Um diese Attacken **unwirtschaftlich** zu machen, verlässt sich moderne Verschlüsselung beispielsweise auf **das mathematische Verfahren** der Primfaktorzerlegung. Dabei **steigt der Aufwand**, um das Problem mathematisch zu lösen, schnell **ins Unermessliche**.

Generell werden die großen und aufwändigen **Probleme der algorithmischen Zahlentheorie** verwendet, um Rechner ohne die notwendigen Informationen **lange genug beschäftigt** zu halten, damit sich der Angriff **nicht lohnt**. Die so verschlüsselten Daten gelten **nach den Maßstäben** heutiger Rechentechnik als nicht **in einer sinnvollen Zeitspanne** knackbar.



### *Asymmetrische Verschlüsselung*

Bei den klassischen Verfahren muss sowohl **die Geheimnachricht als auch der Schlüssel** zwischen Sender und Empfänger ausgetauscht werden. Dann kann die Nachricht **mit demselben Schlüssel** wieder entschlüsselt werden, mit dem sie **zuvor verschlüsselt** wurde. Eine solche Verschlüsselung wird als symmetrisch bezeichnet, da die **Schlüssel zum Ver- und Entschlüsseln** deckungsgleich sind.

In den 1970er Jahren entwickelten **die US-amerikanischen Kryptographen** Martin Hellman und Whitfield Diffie ein neues **System zum Schlüsseltausch**. Damit musste nicht mehr der vollständige Schlüssel übertragen werden. Stattdessen wurden die Verschlüsselung und die Entschlüsselung **mit unterschiedlichen Schlüsseln** vorgenommen.(3)

Das legte den Grundstein für den aktuellen **Verschlüsselungsstandard**. Im Prinzip funktioniert diese Art der Kryptographie über **mathematische Falltürfunktionen** bzw. Falltürpermutation. Diese zeichnen sich dadurch aus, dass sie von einer Seite aus leicht berechenbar sind, aber zur Rückrechnung fehlen **elementare Werte**, die dann kein eindeutiges Ergebnis zulassen. Diese Werte sind elementare Bestandteile der **Schlüsselpaare** für die asymmetrische Verschlüsselung.

### *Mathematische Grundlagen*

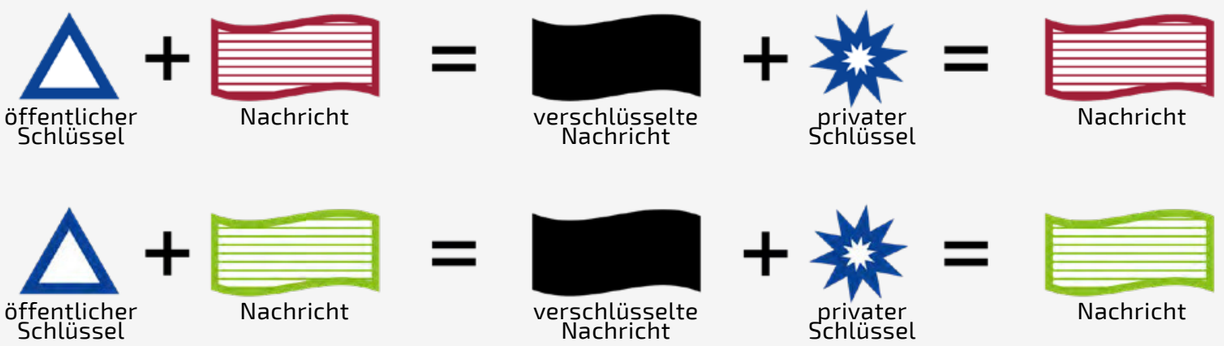
An dieser Stelle soll ein **kurzer Überblick** über den mathematischen Hintergrund der modernen Verschlüsselung gegeben werden. Mit der rasanten **Verarbeitungsgeschwindigkeit**, mit welcher Computer große Datenmassen bearbeiten, ist klassische Kryptographie untauglich, um die heutzutage **meist digital vorliegenden Datenmassen** zu schützen.

Jedoch hat diese **Art der Datenverarbeitung** einen Vorteil. Alle Daten sind irgendwann **binär** und somit mathematisch bearbeitbar. Dann muss **das mathematische Problem**, das der Verschlüsselung zu Grunde liegt, nur noch **ausreichend komplex** sein, damit auch ein schneller Rechner im Mittel **eine astronomisch lange Zeit** braucht, um den richtigen Schlüssel zu finden.

Das Verfahren, das sich dafür **als brauchbar erwiesen hat** ist die sogenannte Primfaktorzerlegung. Dabei werden zwei **sehr große Primzahlen** miteinander multipliziert. Da umgekehrt **kein effizientes Verfahren** existiert, mit dem die Primfaktoren ermittelt werden können (Faktorisierung), hebt dieses Verfahren **den Geschwindigkeitsvorteil** der Computer auf. Aus den beiden Primzahlen werden dann **die kryptographischen Schlüsselpaare** erzeugt, die nötig sind, um eine **nach modernen Maßstäben** sichere Verbindung zu haben.

→

3.

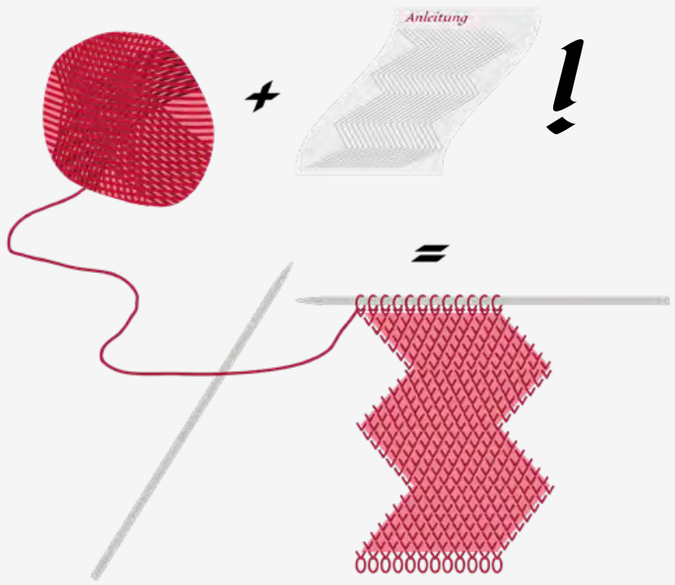


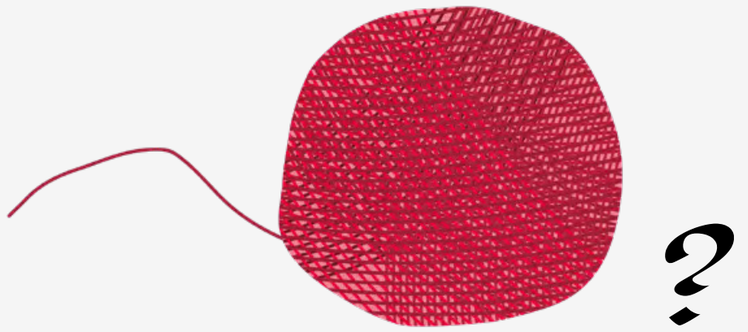
### *Das Schlüsseltausch-Problem*

Ein weiterer **zentraler Schwachpunkt** der klassischen Verschlüsselungsverfahren ist der **Schlüsselaustausch**. Neben dem Geheimtext musste auch der Schlüssel **übermittelt** werden. Denselben Schlüssel öfter zu verwenden, birgt immer die Gefahr, dass Dritte den Schlüssel kennen und die Kommunikation **unbemerkt belauschen** könnten. Andererseits müssen die Teilnehmer an der Kommunikation sich **auf einen Schlüssel** einigen. All diese Prozesse machen Kommunikation wenigstens **für gezielte Angriffe** verwundbar.

Dieses Dilemma wird **mit der asymmetrischen Verschlüsselung** umgangen. Bei diesem System besitzt jeder Teilnehmer zwei Schlüssel, die ähnlich der oben beschriebene **Falltürfunktion** verbunden sind. Einer der Schlüssel ist **öffentlich** und kann von jedem eingesehen werden. Der andere ist **geheim** und verbleibt beim Besitzer.

Soll nun eine **verschlüsselte Kommunikation** stattfinden wird nicht jede Nachricht mit demselben Schlüssel ver- und entschlüsselt. Für die Verschlüsselung verwendet der Sender **den öffentlichen Schlüssel** des Empfängers. Selbst mit dem öffentlichen Schlüssel ist es nicht möglich die Nachricht wieder eindeutig zu entschlüsseln. Für diese Berechnung wird **der private Schlüssel** benötigt, den nur der Empfänger besitzt. Damit müssen keine sensiblen Schlüssel ausgetauscht werden und **das Schlüsseltausch-Dilemma** ist überwunden.



# Gründe für und gegen moderne Verschlüsselung

Seit den **Enthüllungen von Edward Snowden** ist der Menschheit schlagartig klar geworden, wie gefährlich **unverschlüsselte digitale Kommunikation** sein kann. Nicht nur der Inhalt einer Nachricht enthält Informationen, die für **Geheimdienste und Werbetreibende** lukrativ sind. Auch die sogenannten **Metadaten** enthalten Informationen, die einzeln wertlos erscheinen. Über längere Zeit gesammelt ermöglichen sie jedoch Analysen, die **den Grundsatz der informationellen Selbstbestimmung** in Frage stellen.

Aber auch **empfindliche persönliche Vorgänge** wie Banküberweisungen, der Transfer medizinischer Daten oder Steuer- und Einkommensunterlagen sollten nicht **ungeschützt** übertragen werden. Während früher **Berge von Papier** an Ämter übermittelt werden mussten, sind es heute wenige **Dateien und Ordner**. Aber die Informationen darin sind immer noch empfindlich und müssen **gegen Manipulation geschützt** werden.

Schon heute wird ein großer Teil der **Lohn- und Steuerabrechnung** via Internet abgewickelt, genauso ist es bei Bankgeschäften. Zahlreiche Transaktionen werden heutzutage **digital** abgewickelt. Ohne eine sichere Verschlüsselung wäre jede Art der **vertraulichen Datenübermittlung** undenkbar.

## Gründe für Verschlüsselung

Für sichere Verschlüsselung spricht:

- Das Recht auf informationelle Selbstbestimmung auch bei der digitalen Kommunikation
- Schutz des Rechts auf Privatsphäre
- Schutz des Briefgeheimnis und der vertraulichen Kommunikation
- Schutz der Verschwiegenheitsrechte von Anwälten, Ärzten, Seelsorgern etc.
- Schutz des Eigentums, beispielsweise bei digitalen Bildern

All diese Gründe basieren auf dem Wunsch, das **Recht auf Privatsphäre** zu schützen und eine Situation anzustreben, in der jedes Individuum **frei von Kontrolle und Verfolgung** leben kann, solange nicht gegen geltendes Recht verstoßen wird. Vergangene Ereignisse, wie die **anlasslose und massenhafte Speicherung** und Auswertung von Daten durch ein Bündnis verschiedener Geheimdienste, haben gezeigt, dass **Verschlüsselung scheinbar notwendig** ist, wenn im Internet solche Maßnahmen gefahren werden, deren rechtlicher Status wenigstens fraglich ist.

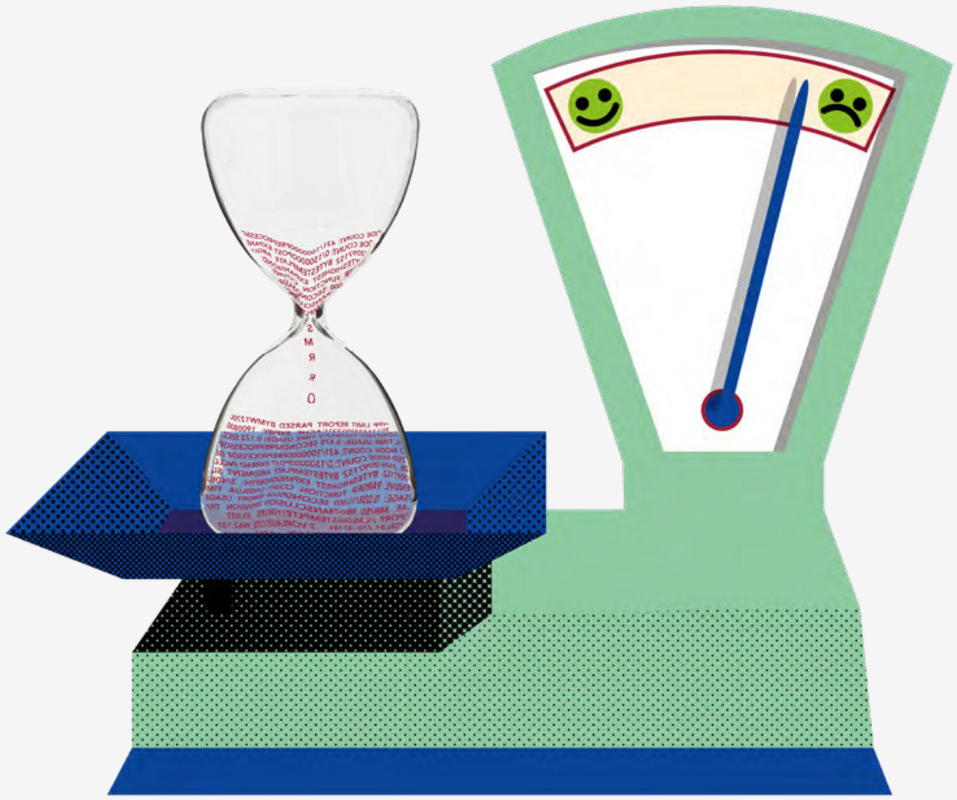
## Gründe gegen Verschlüsselung

Gegen sichere Verschlüsselung spricht:

- Bedenken seitens der Sicherheitsbehörden und Geheimdienste, der Aufwand für Überwachung (sowohl gezielt als auch flächendeckend) steige zu einem Punkt an dem sich der Aufwand nicht mehr wirtschaftlich rechtfertigen lasse.
- Konsequente Verschlüsselung ist kompliziert und nicht anwenderfreundlich
- Der Nutzen ist für den Laien nicht zu erkennen, die Leistungseinbuße des Rechners ist zu spüren

Die Gründe die sich **gegen Verschlüsselung** richten, kritisieren weniger Verschlüsselung an sich als den Sinn und **das Aufwand-Kosten-Verhältnis**, das der Prozess mit sich bringt. Die Spezialwissenschaft ist für Menschen, die **den Rechner im Alltag benutzen**, sich aber nicht professionell mit Datenverarbeitung auseinandersetzen, undurchsichtig. Diese Nutzer sind gezwungen, den Aussagen von Spezialisten zu glauben, deren **Kompetenz** sie nicht bewerten können.

Behörden, die ihre **Arbeit durch Überwachung massiv vereinfachen** können, möchten sich diese Tür natürlich offenhalten. Obwohl die Logik dahinter nicht von jedem geteilt wird, ist es **nachvollziehbar**, dass eine sichere Verschlüsselung **die Arbeit der Ermittlungs- und Sicherheitsbehörden verlangsamen** würde. Jedoch ist der gesamte Themenkomplex kontrovers und von **verschiedenen Auffassungen** über hoheitliche Rechte und Pflichten durchzogen.



# Kryptographie in Deutschland

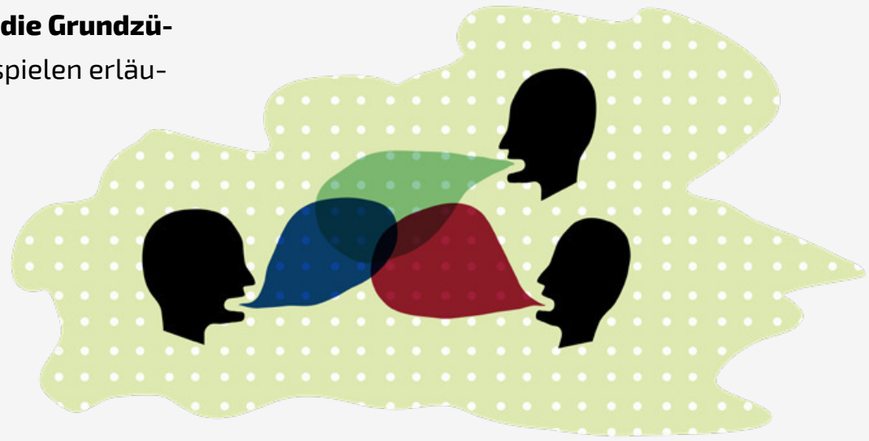
In der Bundesrepublik Deutschland herrscht auf Grund der Debatte um Überwachung, Verschlüsselung, Bürger- und Staatsschutz eine gespaltene Stimmung in Bezug auf die moderne Verschlüsselung von Daten. Auf verschiedenen Ebenen haben sich Argumentationsmuster entwickelt, die die Bedürfnisse ihrer Vertreter gut darstellen. In der Diskussion haben sich drei Pole entwickelt, die sich in Motivation und Stoßrichtung unterscheiden lassen.

Auf der einen Seite stehen **Staat, Regierung und Sicherheitsbehörden**. Diese haben zum einen den Willen, die **Bürger zu schützen** und verpflichten Unternehmen dazu, für den Datenschutz Personal abzustellen und strenge Regeln zu befolgen, wenn es um **die Erfassung, Speicherung und Verarbeitung von Daten** geht. Auch umfassende Auskunftsrechte und informationelle Selbstbestimmungsrechte wurden etabliert. Die Versuche vom Staat **Dienste für sichere Kommunikation** anzubieten, wurden jedoch von der Seite der Spezialisten regelmäßig als untauglich oder als „mit Absicht schlecht programmiert“ bezeichnet. Hier zeigt sich **das Spannungsverhältnis** zwischen Bürgerschutz- und Staatsschutzbedürfnissen.

Darin schwingt auch **die offensive Unterstellung der Spezialisten** mit, die auch Grundlage ihrer Argumentation darstellt. Die Unterstellung ist, dass Sicherheitsbehörden **alles tun werden, was sie können**, um die Sicherheit zu gewährleisten. Dabei spielen laut der IT-Fachleute auch Freiheitsrechte für die Behörden **eine untergeordnete Rolle**. Daraus resultiert für den versierten Computernutzer der **Imperativ der passiven digitalen Selbstverteidigung**. Verschlüsselung sei die **logische Konsequenz der Sammelwut** von nationalen und internationalen Behörden.

Auf der dritten Seite steht **der Bürger**. Verunsichert von den Aussagen der Spezialisten und enttäuscht von Staat und Regierung, steht dieser vor einem System, das er **nicht vollständig versteht**. Doch was der Bürger weiß ist, dass private Dateien wie Bilder oder Videos **nicht in fremde Hände** gelangen sollen. Ob jedoch **selbst verschlüsselt** werden soll oder ob die Dienstanbieter **in die Pflicht genommen** werden sollen, sicher und transparent mit den Daten umzugehen, ist unklar. Hierzu existiert **keine klare Linie**. Doch das Vertrauensproblem bleibt bestehen. Erst in Zukunft wird sich zeigen, ob die Datenschutzgesetzgebung **den Ansprüchen** an ein Sicherheitsgefühl gerecht wird oder ob **die Kassandrarufe** der IT-Fachleute eine andere Lösung begünstigen.

Die moderne Kryptographie an sich ist in Deutschland **auf fruchtbaren Boden** gestoßen. Durch die großen naturwissenschaftlichen Kapazitäten hat die Disziplin **in den mathematischen Fakultäten** schnell einen festen Platz gefunden. Die Kreise der Interessierten wachsen hier schnell und selbst in der Kindererziehung werden bereits **die Grundzüge der Verschlüsselung** mit klassischen Beispielen erläutert.

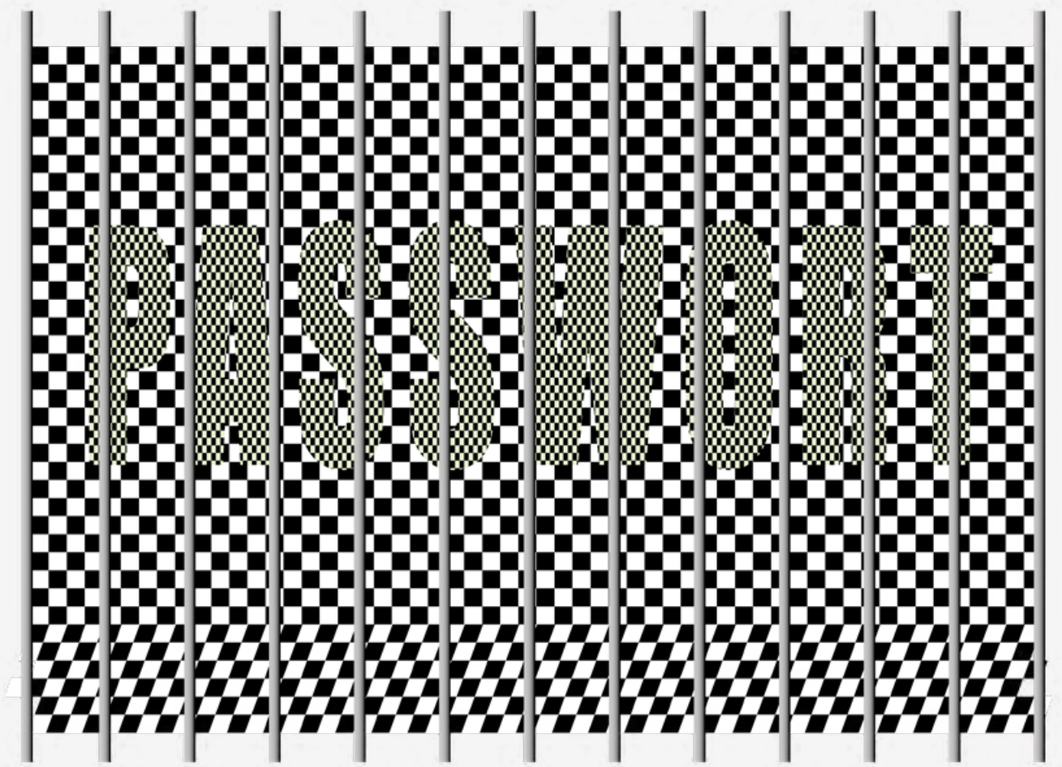


# Kryptographie im Ausland

Da in Deutschland **die Aussage verweigert** werden darf, wenn die Gefahr besteht, sich selbst zu belasten, muss auch ein Passwort nicht herausgegeben werden. In anderen Ländern jedoch **sieht das anders aus**. Auch innerhalb der EU ist in diesem Fall **die Rechtslage unterschiedlich**. In Frankreich und Großbritannien kann **zur Erlangung eines Passwortes** Haft angeordnet werden.

In den USA können **biometrische Schlüsse**l wie der Fingerabdruck auch **gegen den Willen** des Eigentümers genommen werden. In Staaten wie Südafrika steht auf die Verweigerung der Herausgabe eines Passworts eine **Haftstrafe von bis zu 10 Jahren**. Ähnlich ist es in Indien, wo eine Weigerung eine Verschlüsselung zu lösen mit bis zu 7 Jahren Haft bestraft werden kann. Dabei kann jeder, der **befähigt** ist, die Verschlüsselung zu lösen, sich aber weigert, haftbar gemacht werden.

Solche Gesetze können sehr schnell mit **Datenschutzklauseln in Arbeitsverträgen** und Belehrungen zu Dienstreisen kollidieren. Oftmals werden Angestellte mit **firmeneigener Hardware** ausgestattet, so dass eine sichere Verschlüsselung gewährleistet ist. Die Herausgabe der Schlüssel jedoch ist meist unter **Vertragsstrafe** verboten. An dieser Stelle gerät der Angestellte **am Zoll in Verlegenheit**, wenn er aufgefordert wird, den Rechner **für eine Überprüfung** zu entschlüsseln. Die Rechtslage im Zielland sollte unbedingt vorher abgeklärt werden, da ansonsten **Zwickmühlen** entstehen können.



# Wichtige Informationen zu Verschlüsselungen

- Unverschlüsselte Kommunikation gibt nicht nur widerstandslos den Inhalt der Nachricht Preis sondern mit den Metadaten auch ein Puzzleteil zu einem Verhaltensprofil.

- Verschlüsselung muss nicht unknackbar sein, um einem Mithörer die Lust zu nehmen, sich mit genau diesen Daten zu beschäftigen.

- Betrieblicher Datenschutz fordert Verschlüsselung zum Schutz von Kunden und Angestellten, das kann bei internationalen Geschäftsreisen mit verschlüsseltem Laptop zu Problemen mit dem Zoll führen.
  In einigen Ländern wird die Herausgabe von Passwörtern für verschlüsselte Systeme erzwungen.

- Cloud-Computing speichert Daten auf Servern, die dadurch zu attraktiven Zielen für Hacker werden.

- Daten können auch im verschlüsselten Zustand kopiert werden. Danach hat ein Entschlüsselungsprogramm alle Zeit, die es braucht um die Verschlüsselung zu knacken.

- Inzwischen sind ganze Bereiche des Internet verschlüsselt und basieren auf geschlossenen kryptographischen Netzwerken. Ein prominentes Beispiel ist das Onion-Netzwerk, das durch den Tor-Browser erreichbar ist.

- Kryptographie stellt die Grundlage für virtuelle Krypto-Währung dar. Die Verteilung der sogenannten Bitcoin (nach dem prominentesten System) wird vollständig über kryptographische Schlüssel vollzogen.

- Auf Grund der linearen Arbeitsweise von Computern werden Passwörter schwerer zu knacken, wenn sie aus vielen unterschiedlichen Zeichen bestehen.
  Die Dauer, die ein Angriff auf ein Passwort mit Buchstaben, Zahlen und Sonderzeichen braucht, steigt exponentiell mit der Länge des Passworts. Daraus ergeben sich durchschnittliche Zeiten zum Überwinden mit brute force von 10.000 Jahren.

- Asymmetrische Verschlüsselung gilt als ausreichend sicher. Diese Sicherheit wird laut Experten erst bedroht, wenn Quantencomputer in annehmbarer Rechenleistung zur Verfügung stehen.

# Impressum

Unter diesem Link gelangen Sie zu unserem Impressum:

***https://www.anwalt.org/impressum/***