Datenschutz und Kryptographie

Theoretische Grundbegriffe der Datensicherheit durch Verschlüsselung und Signatur.

Version 1.10 © Harry Zingel 2000-2001, EMail: HZingel@aol.com, Internet: http://www.zingel.de

Inhaltsübersicht

1. Die drei Aspekte des Datenschutzes

Die mit dem deutschen Wort „Datenschutz“ korrespondierenden englischen Begriffe

- *Privacy*,
- *Safety* und
- *Security*

lassen den Inhalt des Datenschutzbegriffes *wesentlich anschaulicher* werden.

Wir können diese drei Begriffe in der folgenden Art und Weise *visualisieren*.

Dieses Skript befaßt sich *fast ausschließlich mit dem Privacy-Aspekt* des Datenschutzes.

Die umfassende Bedeutung des Datenschutzbegriffes anschaulich demonstriert:

Schutz vor Einsicht Dritter (z.B. Sichtschutz):
Privacy

Sicherheit gegen Unfälle oder Pannen (z.B. Airbag, ABS):
Safety

Schutz vor Einbruch, Diebstahl, Vandalismus oder Kriminalität (z.B. Panzerglas, Wegfahrsperre, Sicherheitsschlösser usw.):
Security

Privacy ist jede Form des Schutzes gegen unbefugte Einsicht Dritter, etwa Codierung oder Signatur von Daten.

Security ist der Schutz gegen Sabotage oder kriminelle Akte, etwa Computerviren, trojanische Pferde oder andere Arten der Spionage.

Safety ist der Schutz vor Datenverlust durch technische Ausfällen von Datenverarbeitungsanlagen etwa durch Datensicherung.

2. Die Inhalte des Privacy-Begriffes

2.1. Kryptographie

Die Kryptographie befaßt sich mit der *Verschlüsselung von Daten*. Durch Verschlüsselung werden Daten in einer Art und Weise verändert, daß nur wer im Besitz eines Schlüssels ist die verschlüsselten Daten wieder entschlüsseln kann.

Die ursprüngliche Information bezeichnet man als *Klartext*; die codierte Information als *Ciphertext*.

2.2. Stageonographie

Die Stageonographie befaßt sich mit der Verschlüsselung von Daten in einer Art und Weise, daß *eine Information so in einer anderen Information verborgen ist*, daß ein Uneingeweihter schon das Vorhandensein der „zweiten“ Information nicht bemerkt. Während durch Kryprographie also eine „offensichtlich“ unlesbare oder mindestens unverständliche Information erzeugt wird, wird eine Information, die selbst codiert sein kann oder auch nicht, durch Stageonographie so in einer anderen Information „versteckt“, daß schon das Vorhandensein der versteckten Information nicht offensichtlich ist.

Die Information, die versteckt wird, bezeichnet man auch als *Payload*, und die Information, in der die Payload-Daten versteckt werden, werden als *Container-Daten* bezeichnet.

Die Container-Daten sind stets *wesentlich umfangreicher* als die Payload-Daten. Stageonographie ist besonders mit Bildern, Video- oder Sounddaten möglich und sinnvoll, weil hier die Containerdaten viel größer als die zu verstek-

kende Payload-Information sind. Die Qualität eines stageonographischen Verfahrens kann hierbei nach *zwei Kriterien* gemessen werden:

- Das *Mindestmaß an Containerdaten*, um eine Payload-Information bestimmter Größe zu codieren und
- Die Fähigkeit des Verfahrens, auch bei Anwendung von *reduzierenden Kompressionsverfahren* auf die Containerdaten (wie JPEG oder MPEG) noch eine Payload-Information zu codieren oder zu decodieren sowie
- Die *Sicherheit* des Verfahrens gegen Entdeckung oder unbefugte Decodierung der Payload-Information.

Dieses Skript befaßt sich ausschließlich mit der eigentlichen Kryptographie.

3. Grundbegriffe der Kryptographie

Dieses Kapitel erläutert Grundbegriffe der Datenverschlüsselung und ist nicht spezifisch auf eine bestimmte Software ausgerichtet.

3.1. Arten von Schlüsseln

Als *Schlüssel* bezeichnet man die Information, die zum Ver- und Entschlüsseln einer anderen Information erforderlich ist. Man unterscheidet symmetrische und asymmetrische Schlüssel.

3.1.1. Symmetrische Schlüssel

Ein *symmetrischer Schlüssel* ist eine Schlüssel, der *sowohl zur Ver- als auch zur Entschlüsselung* von Daten verwendet werden kann. Führt man mit binären Daten beispielsweise eine NOT-Operation durch, so erhält man einen Ciphertext, weil jedes Bit „1“ in „0“ verwandelt wurde, und jede „0“ in eine „1“ vertauscht wurde. Führt man mit diesem die NOT-Operation erneut durch, so entsteht wieder der ursprüngliche Klartext.

Analoge *Pay-TV-Systeme* wie Syster, Nagravision oder VideoCrypt verwenden symmetrische Schlüssel. Codiert man ein codiertes Signal erneut, so erhält man wieder das ursprüngliche Bild. Das hat den Vorteil, daß insgesamt nur ein einziges Codierverfahren erforderlich ist, das auf den Klartext zwei mal in genau gleicher Art und Weise angewandt werden muß, ein Mal zum Ver- und ein weiteres Mal zum Entschlüsseln.

Der große *Nachteil* symmetrischer Schlüssel besteht darin, vor ihrer Anwendung einen *sicheren Übertragungsweg* für die Schlüsselinformation zu benötigen. Bei Pay-TV-Systemen ist dies die vorherige Übergabe einer Berechtigungskarte an den Teilnehmer, die die Schlüsselinformation enthält, vermittels der ein Decoder durch erneutes Codieren eines bereits codierten Signales wieder ein Bild rekonstruiert.

Damit keine unverschlüsselten Signale mit dem Code behandelt und damit verschlüsselt werden, enthält das verschlüsselte Signal eine Zusatzinformation, die dem Decoder sagt, ob das Bild verschlüsselt ist oder nicht, so daß der Decoder „weiß“, wann er in Aktion treten muß.

Aus lizenzrechtlichen Gründen wurden verschiedentlich uncodierte Signale mit der Information versehen, sie seien codiert, so daß der Decoder den Schlüssel auf ein Klarbild anwendet und dieses damit codiert. Auf diese Art sollten etwa Programme, die für den europäischen Kontinent gedacht sind, in England „unsichtbar“ bleiben, weil die dort verbreiteten Videocrypt-Decoder das Programm unsichtbar machen sollen. VH1 war für eine gewisse Zeit auf Astra so ein Fall.

Im Internet sind die Verhältnisse nicht so eindeutig. Da es keine sichere Übertragung im Internet gibt, kann jeder symmetrische Schlüssel an Unberechtigte gelangen, die dann die gesamte codierte Information mitlesen können.

3.1.2. Asymmetrische Schlüssel

Bei einem *asymmetrischen Schlüssel* wird ein Schlüssel zur Codierung einer Information benötigt und ein *anderer* Schlüssel zur Decodierung. Man hat es also stets mit einem Schlüssel*paar* zu tun.

Die erneute Anwendung des Codierschlüssels führt nur zu einem neuen Ciphertext und *nicht* zum Klartext zurück.

Der für die Codierung zu verwendende Schlüssel kann also *unbeschränkt jedermann zur Verfügung gestellt werden* und benötigt keinen sicheren Übertragungsweg, weil er nicht zur Decodierung von Informationen taugt. Er kann also im Internet übertragen werden. Der zur Decodierung erforderliche Schlüssel muß überhaupt nicht übertragen werden. Er bleibt beim Empfänger der Information, der damit die zuvor mit dem Codierschlüssel verschlüsselte Information wieder lesbar machen kann.

3.1.3. One-Time Pads

Ein *One-Time Pad* ist ein Schlüssel, der nur ein einziges Mal verwendet wird. Er kann symmetrisch oder asymmetrisch sein. Ein One-Time Pad ist *stets absolut sicher*, aber *wenig praktikabel*, weil die Anzahl der erforderlichen Schlüssel sehr groß ist (im Extremfall der Menge der zu übertragenden Informationen selbst entspricht).

3.2. Kryptographische Angriffe

Als *kryptographische Angriffe* („cryptoattacks“) bezeichnet man den Versuch, eine codierte Information ohne offiziell im Besitz eines Schlüssels zu sein dennoch zu decodieren. Man unterscheidet *zwei grundsätzliche Typen* von kryptographischen Angriffen:

- den Versuch der *Rekonstruktion des Schlüssels* und
- den Versuch der *Rekonstruktion der ursprünglichen Information ohne Kenntnis des Schlüssels*.

Weiterhin unterscheidet man zwei verschiedene Vorgehensweisen:

- das *Ausprobieren aller möglicher Schlüssel* (die sogenannte „Methode der brutalen Gewalt“) und
- die *gezielte Rekonstruktion* einer Information durch die Anwendung spezifischer Algorithmen.

3.3. Sicherheit vor kryptographischen Angriffen

Ein einfaches Maß für die Sicherheit ist das *Verhältnis zwischen möglichen und richtigen Schlüsseln.*

Im oben dargestellten NOT-Beispiel gibt es nur zwei Möglichkeiten: „1“ und „0“. Mit der Methode der brutalen Gewalt muß man also nicht lange probieren, bis man den richtigen Schlüssel bzw. die ursprüngliche Information herausbekommen hat.

Wäre ein Schlüssel 2 Bit lang, so hätte man schon 2^2=4 verschiedene Möglichkeiten, eine Information zu codieren.

Hängt die Sicherheit eines Schlüssels von dessen *Bitlänge* ab, so wächst die Anzahl der möglichen Codierungen mit der Anzahl der Bits des Schlüssels dramatisch an. Da aber immer nur eine einzige Bitfolge der „richtige“ Schlüssel ist, führt die Methode der brutalen Gewalt bald zu keinem Erfolg mehr:

Bitlänge des Schlüssels und Sicherheit vor kryprographischen Angriffen

Bits	Mögliche Verschlüsselungen
1	2
2	4
4	16
8	256
16	65.536
24	16.777.216
32	4.294.967.296
128	ca. 340.282.366.920.938.000.000.000.000.000.000.000.000
512	ca. 13.407.807.929.942.600.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000

Es leuchtet wahrscheinlich ein, daß selbst in den kommenden Jahrzehnten (wenn nicht Jahrhunderten) kein Rechnersystem in der Lage sein dürfte, mit der Methode der brutalen Gewalt in einen Schlüssel einzubrechen.

Da es aus mathematischen Gründen, die hier nicht näher betrachtet werden keine andere Methode zum kryptographischen Angriff auf einen asymmetrischen Schlüssel gibt, war in den USA die Kryptographiesoftware lange Zeit im *Waffengesetz* geregelt (!) und exportbeschränkt. Die Aufhebung dieses Exportverbotes in 1999 wurde vielfach dahingehend gedeutet, daß nunmehr doch ein von der Schlüsselstärke unabhängiges Verfahren für kryprographische Angriffe zur Verfügung steht, daß dem Staat (oder wenigstens dem US-Geheimdienst) den Einbruch in jeden Schlüssel erlaubt, doch ist dies derzeit völlig unbewiesen. Vielleicht wurde auch einfach nur erkannt, daß ein Export von Software faktisch nicht verhindert werden kann.

3.4. Starke und schwache Kryptographie

Ein kryptographisches Verfahren, das Ehefrauen daran hindert, Vatis EMails mit seinen diversen Freundinnen zu lesen, ist eine „*schwache*“ *Kryptographie* („Low Order Encryption“). Ein Verfahren, das hingegen einen Geheimdienst daran hindert, eine technische Entwurfszeichnung mit der Erfindung eines Unternehmens oder auch nur die Gedanken eines Regimekritikers mitzulesen, heißt „*starke*“ *Kryptographie* („High Order Encryption“).

Dieses Skript befaßt sich ausschließlich mit starker Kryptographie.

Obwohl die Grenze zwischen diesen beiden Bereichen unscharf ist, und auch die Ehefrau einen leistungsfähigen Rechner besitzen kann, hat sich PGP von *Phil Zimmermann* als de-facto-Standard eingebürgert. Die derzeitigen Fassungen von PGP können Schlüssel mit bis zu 4.096 Bits Länge erzeugen.

Bei Browsern und im HomeBanking gelten derzeit 40 Bits als relativ unsicher aber 128 Bits noch als vollkommen sicher. Die 128-Bit-Codierung für Windows 2000 heißt auch „*High Encryption Pack*“. Die Sicherheit eines Schlüssels mit 4.096 Bit kann als *absolut* bezeichnet werden, wenn es keine „Hintertüren“ gibt.

4. Asymmetrische Codierung mit PGP

PGP ist die bekannteste asymmetrische Kryptographiesoftware. PGP verwaltet je einen öffentlichen und einen privaten Schlüssel. Die öffentlichen Schlüssel dienen der Codierung eines Textes und können frei weitergegeben werden, auch über einen unsicheren Kommunikationsweg wie das Internet. Die privaten Schlüssel sollten keinesfalls weitergegeben werden und dienen der Entschlüsselung von Nachrichten.

Bei PGP Freeware 6.x steht der Privatschlüssel eines Anwenders in der Datei SECRING.SKR, die beliebig viele Privatschlüssel enthalten kann. Die öffentlichen Schlüssel, über die ein Anwender verfügt, befinden sich in PUBRING.SKR.

4.1. Der Beispielschlüssel für dieses Skript

Für die in diesem Manuskript folgenden Anwendungsbeispiele wurde mit PGP Freeware ein *Beispielschlüssel* generiert. Er findet sich in der Datei

Mustermann Beispielschlüssel.asc

und ist auf den fiktiven Anwender *Heinz Mustermann* ausgestellt. Heinz Mustermann hat die EMail-Adresse **Mustermann@Beispiel.de**. Die Bitlänge dieses Schlüssels beträgt 4096 Bytes, was der maximalen Sicherheit entspricht. Das Passwort lautet **Mustermann4096**.

Die genannte Datei enthält den zur Ver- und zur Entschlüsselung erforderlichen Schlüssel. Da beide Schlüssel hier bekanntgemacht werden, ist jede „echte“ Verwen-

Muster der Codierung eines Klartextes für verschiedene Empfänger

Klartext (Dateiname: „Beispiel 1 Klartext.txt“):
Wenn der Hahn kräht auf dem Mist, ändert sich das Wetter oder's bleibt wie's ist!

Für Heinz Mustermann codierter Text (Dateiname: „Beispiel 1 Ciphertext A.txt“):

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>

qANQR1DBw04DAlSIa3aPb3oQEADWYRCEVYghUQXkL9fYoGCDcImr/VRQg+TFc9hk
UboitO5hPtHJ/8Sb6Kc43l2WerzBfiiwVHJZOiFOGeyLLa6nzNpa+JGFfB/6Fyy4
QN/nKTrkQDhrUvez1MA0/D1gYH5IQ12NKjOvBL29K3GOQH5O6gL9+UMIGqwtPtfO
LF/1XPLVrpjTVm5fcq0SzP+7vXpTBQQW1/AY88PZdkhEybfX3Ws+wiKXUSUIiASW
5zrNVGtjuaiiGwmFxP5dqQbOSEHaGxIWdnnDq0fwvq/ObIH64Txo0UyAHYe1g+aA
0IEuNhoTA1tHqcOhSH1p0aA/s0IOe/nK2g3f+uWff5hXmDJ157YJACSuYNo3GSI+
iH4AJfsGDZ/1KEmaj9rXzsp/FybNLByaOMLXS5HbgnwuGnA1PkhUSk8WFwhXQt0m
4RMmBgocxiWuHe4eOMZMiPFPdU/DagpIrMVF/wzs+fdqTKkNXMpEMPIVdD3q3EtZ
kpS7O7i8ssaYti50SaWkp1ziABr5DaLRRbxVl+N7c9FAHKPWIgUvJIVS0kclIADN
UL0Ze7meeZjbCJvHTBvyqF8q3UadcBGhTpY3lQ4dut487le8TZuEMVFktwTICwbH
GX4g6zl+88hq5UkXaVgLdsxXUc5IK87UPXSGbAtJTN9xMsjDrGnoLMu5UKeuHTSR
w85NjRAA623LQPeCADHSveew+1bfKyKZPUzHMwN3MRBQrd7r2f5utZb0NQUKJqYS
yEVYNhwwCkAZnk5lXAzbqi33nhucxmQsQcWpm8voU6plaXK6ExiCOYt3lVtmHHqE
/D92tIzTMccpS3bXA5a612w1uFKAbbmvxXS4w9BWUb9DTKjw4VpeiHRO11qkgYpw
F7lsf6as1dHzZ2hwIYYUQjiGoTp6+dZp8jwaMdtoup2TFUQOW8NR8Fkw1w+TRojP
K2XrPKTXxQo0IMjwmPpuaq8nqQ7ZSvK0IPGS9NZcAtVBPFJVXg/j+g0gqzWauDyN
Hpokn7YlcLK1GEysXSrE52q+ETOGBtJC8cWKp9/Ul5XBqnNpD7H98jkD7yEj2mkL
URcCmRS/0LMuc/j5N2C2UGadFlAhegTAZXWaTJdRQbjsPl6c0g4KeQjPtmtThzKX
zvt6+ZhMgktXgG1VK0WJr1ZCYFNPaN20vhZl0hHGPDBMO5m9H+hnPSiLy4PjCFY2
zkrujSbzriM7vNjZsaSICvjhVbwUgsamvRHB2FkwCKyVsrimy07l1uAZtJ6H7i1y
gU422ihWYs1OzCGmTdS5j5Fd7KaRYqUcmRnRKmVbtXUdEXLc/488cK/ndpNZubX8
uOx9kn8z7bRoKDAakafZEQbyRdExFR+tqU6NaEJ6IkbARX9LfZrJZbVPxIIE4+G4
lhrtoYlpagvaPNga1P2VZWtO4sSExCU14f/ovaG4V4RLk/8DaydA4bmipN7JsF2p
n3ain2NACOueI+J+wFymxnpN1qrC13Rnk3J1d9kYQLCAyoXjThnzzfkJ35L4
=wOl5
-----END PGP MESSAGE-----
```

Für H. Zingel codierter Text (Dateiname: „Beispiel 1 Ciphertext B.txt“):

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>

hQCMAw09ONB1L4chAQP/UugApKGs+rUQI73Yb+Bb4VDnuBcUmHF1LV8x4fM4nDtT
pK4hCac22Q/CaRW1HbEIz4nfkvrasfm+bxjJpddmquX5w98e88iiF+8RuDyuPs9i
wsiW6X6yWA6efYENZliHCVVlf4yMnBu91Td/ErhZlMeh+lNiWw+NiWaP2NbYmUOk
ZDTZEq8VeFX8HnQyVWxYwR/Jwu/In+hOEOV2Yz12QVwwX1VH20Hsha7wWfgXTKSw
47v0tAzaEO+tcSFA55pCQ3Q7tiHOIoCullPoyVmuZIFprl6Rm0fTGC90oouaC9+w
pWgGlvA=
=siFi
-----END PGP MESSAGE-----
```

dung wird wirklich geheime Informationen unsicher. Der hier verwendete Schlüssel ist also ausschließlich für Übungszwecke gedacht. Jede Haftung des Autors dieses Manuskriptes bei Mißbrauch ist ausgeschlossen!

Zum Ausprobieren finden Sie außerdem den öffentlichen Schlüssel von *Harry Zingel* in der Datei **HZingel.pgp**.

4.2. Ein Anwendungsbeispiel

In vorstehendem Anwendungsbeispiel wird der oben gezeigte kurze Text *für zwei Empfänger codiert*: Für den fiktiven Herrn Mustermann sowie für den keinesfalls fiktiven Herrn Zingel.

Herr Mustermann verfügt über einen 4096-Bit-Schlüssel, so daß der kurze Klartext die anschließend gezeigte umfangreiche codierte Datei erzeugt. Herr Zingel hingegen benutzt „nur“ einen 1024-Bit-Schlüssel, so daß der für ihn codierte Text *wesentlich kürzer* ist, aber auch „wesentlich“ *unsicherer*. Die Länge der codierten Information hängt also von der Länge des verwendeten Schlüssels ab.

Da Sie über den Privatschlüssel des Herrn Mustermann verfügen, und die Dateien mit dem Original-Ciphertexten diesem Skript anliegen, können Sie die für Herrn Mustermann verschlüsselte Datei decodieren. Sie werden jedoch die für Herrn Zingel codierte Datei nicht mehr in Klartext zurückverwandeln können, weil Herr Zingel seinen Privatschlüssel nicht herausrückt.

5. Echtheitsprüfung per Signatur

Während das von PGP verwendete System als sicher gegen kryprographische Angriffe gilt, eignet es sich in der bislang dargestellten Form nicht für die *Echtsheitszertifizierung* von Inhalten.

Echtsheitszertifizierung ist jedes Verfahren, das die *Urheberschaft einer Datei* von einer bestimmten Person sicherstellt. Die Echtsheitszertifizierung ist ein *Sonderfall der Kryptographie*, weil sie alleine die zu übertragende Information nicht codiert, ihr aber eine digital codierte Unterschrift (Signatur) anhängt, der aus dem Privatschlüssel des Absenders und der unterzeichneten Information selbst errechnet wird.

5.1. Der Grundgedanke der digitalen Signatur

Jede Information, ob Klartext oder nicht, kann gefälscht werden:

- Unter eine Klartextinformation kann ein *falscher Name* geschrieben werden, etwa um einer Person eine schriftliche Äußerung unterzuschieben und sie damit öffentlich zu diskreditieren,
- ein Privatschlüssel kann *im Namen einer anderen Person errichtet werden*, da PGP die Identität eines Anwenders nicht überprüfen kann, und verschlüsselte Informationen können mit einem solchen gefälschten Privatschlüssel im Namen einer anderen Person unberechtigt erstellt werden.

Signaturverfahren verhindern diese beiden Formen der Verfälschung von Informationen unter Verwendung kryptographischer Verfahren.

Grundgedanke ist, daß der wirkliche Absender einer Information unter Verwendung seines echten Privatschlüssels und des fertigen Inhaltes eine Signatur errechnet, die selbst eine codierte Information ist. Dabei lassen sich sowohl codierte als auch unverschlüsselte Informationen und sogar Nicht-Textdateien wie Bilder oder Sounddaten signieren, weil jede beliebige Bytefolge signierbar ist.

Da PGP ein asymmetrisches Verfahren ist, kann jeder beliebige Leser die Echtheit der Signatur überprüfen, aber nicht die Signatur eines beliebigen Absenders neu berechnen.

Im Kern wird in der Signatur nur eine *Prüfsumme* codiert, die aufgrund der asymmetrischen Eigenschaft des Codierverfahrens zwar decodiert, aber nicht neu encodiert werden kann.

Würde ein Unberechtigter den Informationsinhalt ändern, etwa durch Hinzufügungen, Löschungen oder Ersetzen von Daten, so stimmt die Information nicht mehr, und der Leser kann durch Überprüfung der Signatur feststellen, daß die Signatur nicht mehr zu dem Dateiinhalt paßt.

5.2. Anwendungsbeispiel einer digitalen Signatur

Wird beispielsweise die untenstehende signierte Datei überprüft, so erhält man die folgende Meldung:

```
*** PGP Signature Status: good
*** Signer: Heinz Mustermann <Muster-
mann@Beispiel.de>
*** Signed: 21.07.2000 19:19:38
*** Verified: 21.07.2000 19:28:03
```

In der Signatur sind also Name des Unterschreibenden und Datum der Signatur und der Signaturüberprüfung gespeichert. „Signature Status: good“ zeigt an, daß die Information nicht verändert wurde, garantiert also, daß die Information wirklich von dem angegebenen Absender stammt. Freilich hätte auch jede andere Person den Text signieren können, wäre dann aber auch als Signierer

Beispiel für eine gültige PGP-Signatur:

Mit dem Privatschlüssel des Herrn Mustermann wurde die folgende bekannte Textzeile signiert. Während der Text selbst uncodiert ist, ist die anhängende Signatur selbst verschlüsselt. Verwenden Sie zur Überprüfung die Originaldatei „**Beispiel 2 Echte Signatur.txt**“:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Wenn der Hahn kräht auf dem Mist, ändert sich das Wetter oder's
bleibt wie's ist!

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>

iQA/AwUBOXh4G8vnOPU/DSCJEQIv+wCgpPag8U2jCCXqiz3snJDQH1ZfIlUAnRYq
xmXkKh1YOJJOXtr73qpMnVCy
=kyB7
-----END PGP SIGNATURE-----
```

Beispiel für eine durch Fälschung ungültige PGP-Signatur:

Der im vorstehenden Beispiel signierte Text wurde minimal verändert („oder's" wurde gegen „oder es" ausgetauscht). Die Überprüfung offenbart diese Fälschung durch eine Fehlermeldung. Verwenden Sie zur Überprüfung die Originaldatei „**Beispiel 2 Falsche Signatur.txt**":

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Wenn der Hahn kräht auf dem Mist, ändert sich das Wetter oder es
bleibt wie's ist!

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>

iQA/AwUBOXh4G8vnOPU/DSCJEQIv+wCgpPag8U2jCCXqiz3snJDQH1ZfIlUAnRYq
xmXkKh1YOJJOXtr73qpMnVCy
=kyB7
-----END PGP SIGNATURE-----
```

genannt worden. Eine Fälschung der Originalunterschrift ist *nur* durch Stehlen des Originalprivatschlüssels des Signierers aber nicht durch Nachmachen der Unterschrift möglich.

Das obenstehende zweite Beispiel enthält einen nur geringfügig veränderten Text. Überprüft man die (nicht veränderte) Signatur, so erhält man:

```
*** PGP Signature Status: bad
*** Signer: Heinz Mustermann <Muster-
mann@Beispiel.de>
*** Signed: 21.07.2000 19:19:38
*** Verified: 21.07.2000 19:33:40
```

Die Meldung „PGP Signature Status: bad" zeigt an, daß der Textinhalt der Datei *nicht* mit dem Inhalt zur ebenfalls angegebenen Zeit der Signierung übereinstimmt. Der Text wurde also verändert, d.h., *gefälscht*.

5.3. Stärken und Schwächen des Signaturverfahrens

5.3.1. Nachgemachte Privatschlüssel

Ein *kryptographischer Angriff auf eine Signatur einer unverschlüsselte Information* kann darin bestehen, daß der Angreifer auf den Namen des ursprünglichen Privatschlüsselinhabers einen neuen Privatschlüssel nachmacht, die ursprüngliche (echte) Signatur von der Information entfernt, die Information fälscht und dann erneut mit dem nachgemachten Schlüssel signiert.

Dies wäre *prinzipiell unproblematisch*, weil keine Software die wirkliche Identität eines Absenders überprüfen kann, man also problemlos Schlüssel auf die Namen anderer Personen generieren kann.

5.3.2. Gestohlene Privatschlüssel

Wird der Privatschlüssel einer Person *gestohlen*, indem ein Angreifer etwa ein *trojanisches Pferd* auf den Computer des Anwenders schmuggelt und damit die SECRING-Datei entwendet, so kann der Angreifer gültige Signaturen erstellen.

5.3.3. Abhilfen gegen falsche Schlüssel

Man könnte den Text selbst codieren, so daß eine Fälschung des Dateiinhaltes nicht möglich ist. Dies ist jedoch keine Abhilfe, weil mit einem asymmetrischen Schlüssel nur für eine bestimmte Person codiert werden kann. Signaturen werden aber gerade unter uncodierten Dateien angewandt, die allgemein zugänglich sein sollen (wie etwa Readme-Dateien), deren Urheberschaft aber dennoch sicher feststellbar sein soll.

Folgende Schutzmechanismen zur sicheren Feststellung der Urheberschaft einer Signatur bestehen:

- Der Public Key einer Person kann *selbst signiert* werden. Da der Public Key von einem Private Key abhängt, kann er nicht gefälscht werden. Durch Vergleich der Signatur eines Public Keys und der Signatur eines Dokuments kann überprüft werden, ob der zur Signatur des Dokuments verwendete Schlüssel identisch ist mit dem Schlüssel, der zur Signatur des öffentlichen Schlüssels verwendet wurde. Dieses Verfahren schützt nur gegen Nachmachen aber nicht gegen Stehlen des Privatschlüssels.
- Ein signierter öffentlicher Schlüssel kann bei einem *Trust Server* eingereicht werden. Dieser ist ein System, das nur Schlüsseldaten öffentlich zur Verfügung stellt. Das signierte Dokument enthält einen Verweis auf den verwendeten Trust Server. Jeder Leser kann nicht nur die Signatur prüfen, sondern auch die Urheberschaft durch Vergleich der Signatur mit der auf dem Trust Server hinterlegten Signatur. Das schützt zwar auch nicht gegen Siebstahl, doch kann die Tatsache des Verlustes eines Schlüssels ebenfalls in dem Trust Server hinterlegt werden, so daß der Leser weiß, daß ein bestimmter Schlüssel entwendet wurde und daher ungültig ist, auch wenn kein Fehler von PGP gemeldet wird. Enthält ein signierter öffentlicher Schlüssel auch (ebenfalls signierte) Informationen über seinen Urheber, so spricht man von einem sogenannten *digitalen Zertifikat*. Zu diesem Themenkomplex bestehen für Deutschland seit 1997 Rechts-

vorschriften, auf die nachfolgend grundlegend eingegangen wird.

6. Rechtliche Aspekte

Wir wären nicht in Deutschland, wenn es nicht für alles Rechtsvorschriften gäbe, und tatsächlich ist es dem deutschen Gesetzgeber, der etwa für die dringend notwendige Reform des Kaufmannsbegriffes im Handelsrecht fast ein Jahrhundert gebraucht hat und im 21. Jahrhundert noch immer verstaubte Nazigesetze nicht abschaffen kann gelungen, schon 1997 Rechtsvorschriften über die digitale Signatur zu erlassen, die die vorstehend dargestellten technischen Aspekte voraussetzen.

6.1. Allgemeine Übersicht über die Regelungen zum Datenschutz

Der Datenschutz ist ein *recht heterogenes Rechtsgebiet*, das in folgende *Kategorien* unterteilt werden kann:

- Im *Grundgesetz* leitet sich der Datenschutz aus dem Recht auf Information (Art. 5 GG) und dem Persönlichkeitsrecht (Art. 2 Abs. 1 GG) ab. Aus letzterem wird insbesondere das Recht auf informationelle Selbstbestimmung abgeleitet.
- Auf *Bundesebene* ist der Datenschutz allgemein im *Bundesdatenschutzgesetz* (BDSG) geregelt.
- Auch die *Länder* verfügen über *eigene Datenschutzgesetze*, da eine bundeseinheitliche Regelung offensichtlich zu einfach wäre.
- Viele *Einzelgesetze* enthalten *verstreute datenschutzrechtliche Einzelvorschriften*, etwa im Steuer-, Straf- oder Handelsrecht.
- Das *Signaturgesetz* ist die spezielle Rechtsquelle für technische Vorschriften zu digitalen Signaturen.

Das vorliegende Skript befaßt sich auf juristischer Ebene *ausschließlich* mit dem Signaturgesetz (SigG). Allgemeines Datenschutzrecht ist nicht Gegenstand dieser Erörterungen.

6.2. Grundriß des Signaturgesetzes

Das Signaturgesetz (SigG) ist die *grundlegende Rechtsquelle* zur Anwendung von elektronischen Signaturen und verwandten mathematisch-softwarebezogenen Verfahren in Deutschland. Es trat zunächst zum 22.07.1997 in Kraft und war die Vorlage für eine entsprechende EU-Richtlinie. Deutschland war insofern Vorreiter in Europa. Nunmehr wurde dieses Gesetz zum 22.05.2001 *in neuer Form in Kraft gesetzt* und dient jetzt als Grundlage für die Einführung der elektronischen Form in das bürgerliche Gesetzbuch bei Willenserklärungen in der sogenannten Textform).

Dieser Artikel stellt nur noch die neue Version des Gesetzes dar.

6.2.1. Wichtige Begriffsbestimmungen

Zunächst definiert das Gesetz in §2 die elektronische Signatur und die mit ihr verwandten und für sie relevanten Begriffe (in Anlehnung an den Gesetzeswortlaut):

1. **elektronische Signaturen** sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur *Authentifizierung* dienen.
2. **fortgeschrittene elektronische Signaturen** sind elektronische Signaturen im vorstehenden Sinne, die jedoch *ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind*, die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und mit den Daten, auf die sie sich beziehen, so verknüpft sind, daß eine nachträgliche Veränderung der Daten erkannt werden kann. Anders als „einfache“ elektronische Signaturen, die etwa auch in

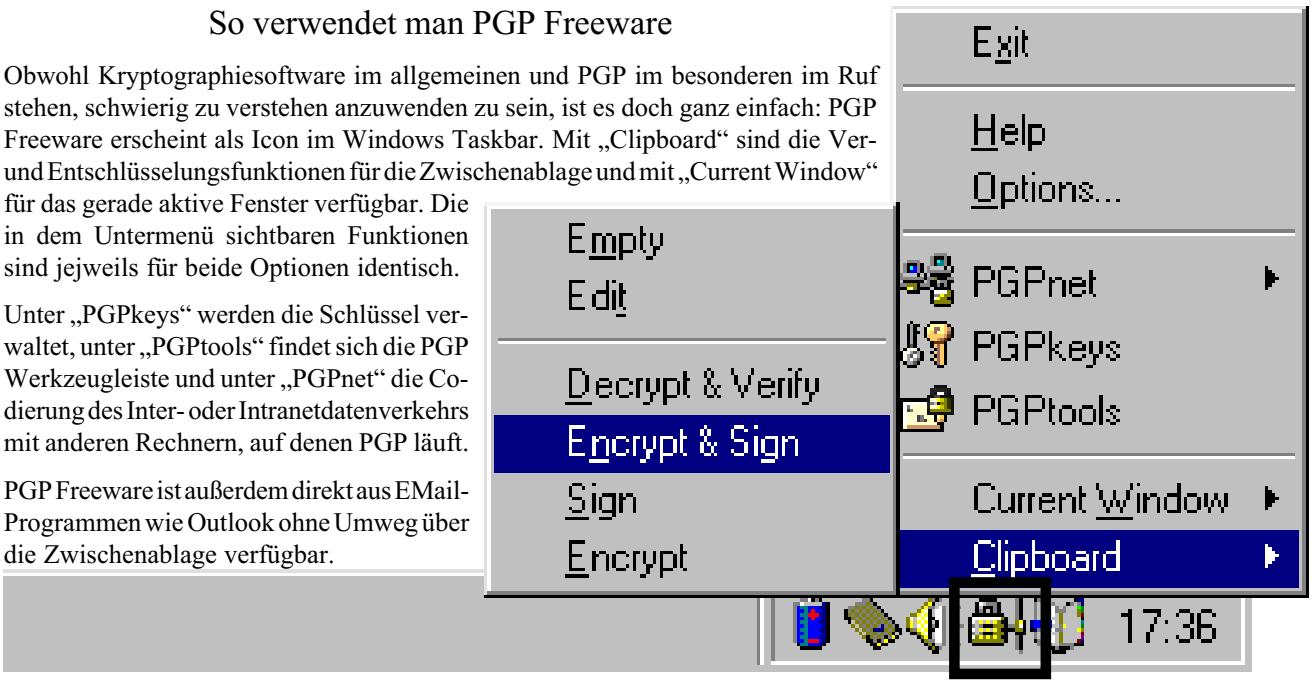
---

So verwendet man PGP Freeware

Obwohl Kryptographiesoftware im allgemeinen und PGP im besonderen im Ruf stehen, schwierig zu verstehen anzuwenden zu sein, ist es doch ganz einfach: PGP Freeware erscheint als Icon im Windows Taskbar. Mit „Clipboard“ sind die Ver- und Entschlüsselungsfunktionen für die Zwischenablage und mit „Current Window“ für das gerade aktive Fenster verfügbar. Die in dem Untermenü sichtbaren Funktionen sind jeweils für beide Optionen identisch.

Unter „PGPkeys“ werden die Schlüssel verwaltet, unter „PGPtools“ findet sich die PGP Werkzeugleiste und unter „PGPnet“ die Codierung des Inter- oder Intranetdatenverkehrs mit anderen Rechnern, auf denen PGP läuft.

PGP Freeware ist außerdem direkt aus EMail-Programmen wie Outlook ohne Umweg über die Zwischenablage verfügbar.



Geräten Anwendung finden könnten (wo sie nicht einmalig sind) sind „fortgeschrittene“ Signaturen einer Person zugeordnet und entsprechen im wesentlichen dem zuvor dargestellten Schlüsselbegriff.

3. **qualifizierte elektronische Signaturen** sind elektronische Signaturen nach Nummer 2, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten *Zertifikat* beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden, also eine *noch weiter differenzierte Form* der Signatur.

4. **Signaturschlüssel** sind *einmalige* elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden, was mit dem allgemeingültigen *Begriff des privaten Schlüssels* deckungsgleich ist.

5. **Signaturprüfschlüssel** sind elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden, was sich mit dem allgemeinen *Begriff des öffentlichen Schlüssels* deckt.

6. **Zertifikate** sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person *zugeordnet* werden und die Identität dieser Person *bestätigt* wird,

7. **qualifizierte Zertifikate** sind elektronische Bescheinigungen nach Nummer 6 für natürliche Personen, die bestimmte *Mindestinhalte* aufweisen (vgl. weiter unten) und von Zertifizierungsdiensteanbietern, die das Gesetz einführt, und die ebenfalls bestimmte Mindestanforderungen hinsichtlich gewerberechtlicher Größen wie Sachkunde und Zuverläsigkeit sowie eine Haftpflichtversicherung besitzen müssen.

8. **Zertifizierungsdiensteanbieter** im vorstehenden Sinne sind natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel *ausstellen* (dürfen).

9. **Signaturschlüssel-Inhaber** ist jede natürliche Personen, die Signaturschlüssel *besitzen* und denen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate *zugeordnet* sind.

10. **sichere Signaturerstellungseinheiten** sind Software- oder Hardwareeinheiten zur *Speicherung und Anwendung des jeweiligen Signaturschlüssels*, die wiederum bestimmten Mindestanforderungen hinsichtlich *Sicherheit* und *Überwachung* genügen müssen, und die für qualifizierte elektronische Signaturen bestimmt sind.

11. **Signaturanwendungskomponenten** sind Software- und Hardwareprodukte, die dazu bestimmt sind, Daten dem Prozeß der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder qualifizierte elektronische Signaturen zu *prüfen* oder qualifizierte Zertifikate *nachzuprüfen* und die Ergebnisse *anzuzeigen*,

12. **technische Komponenten für Zertifizierungsdienste** sind Software- oder Hardwareprodukte, die dazu bestimmt sind, Signaturschlüssel zu *erzeugen* und in eine sichere Signaturerstellungseinheit zu *übertragen*, qualifizierte Zertifikate öffentlich *nachprüfbar* und gegebenenfalls *abrufbar* zu halten oder qualifizierte *Zeitstempel* zu erzeugen.

13. **Produkte für qualifizierte elektronische Signaturen** sind sichere *Signaturerstellungseinheiten*, *Signaturanwendungskomponenten* und *technische Komponenten* für Zertifizierungsdienste.

14. **qualifizierte Zeitstempel** sind *elektronische Bescheinigungen* eines Zertifizierungsdiensteanbieters, der den Anforderungen des Gesetzes genügt und der die sich darauf beziehenden Vorschriften der Rechtsverordnung erfüllt, darüber, daß ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

15. **freiwillige Akkreditierung** ist ein Verfahren zur *Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes*, mit der besondere Rechte und Pflichten verbunden sind.

6.2.2. Der Zertifizierungsdiensteanbieter

Dieses vom Gesetz neu eingeführte Gewerbe ist zwar *an sich genehmigungsfrei* (dem in vielen Berufen kaum noch wahrnehmbaren Grundsatz der *Gewerbefreiheit* wird also nocht entsprochen), aber an *restriktive Auflagen* gebunden. Diese sind gemäß §4 Abs. 2 SigG:

- gewerberechtliche *Zuverlässigkeit*,
- *Sachkundenachweis*,
- die Gewähr, die relevanten *Rechtsvorschriften einzuhalten*,
- ein in die Praxis umgesetztes und nachweisbar angewandtes *Sicherheitskonzept*.

Insofern liegen doch recht *restriktive Regelungen* vor, die eine enge Kontrolle der zuständigen Behörden (§3 SigG) ermöglichen. Zu den besonderen Pflichten des Zertifizierungsdiensteanbieters, die der Kontrolle der Behörde unterliegen, gehören

- eine besondere *Dokumentationserfordernis* mit der Verpflichtung, auf Verlangen in die angewandten Verfahren *Einblick* zu gewähren (§10 SigG),
- Verpflichtungen hinsichtlich des *Datenschutzes* (§14 SigG),
- eine besondere *Haftung* (§11 SigG), für die eine *Deckungsvorsorge* als Zwangshaftpflichtversicherung in Höhe von mindestens zu 250.000 € vorgeschrieben ist (§12 SigG),
- diverse *Unterrichtungs- und Anzeigepflichten* im Rahmen derer der Behörde relevante Änderungen anzuzeigen sind, etwa der Eintritt von Umständen, die den gewerberechtlichen Anforderungen nach §4 entgegenstehen (§4 Abs. 4 SigG) oder die EInstellung der Tätigkeit des Zertifizierungsdiensteanbieters (§19 SigG).

Die Überwachungsmaßnahmen der zuständigen Behörde sind in §19 SigG näher geregelt. Nach dieser Vorschrift hat die Behörde dem Zertifizierungsdiensteanbieter den

Betrieb vorübergehend, teilweise oder ganz zu untersagen, wenn Tatsachen die Annahme rechtfertigen, daß er

1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche *Zuverlässigkeit* besitzt,
2. nicht nachweist, daß die für den Betrieb erforderliche *Fachkunde* vorliegt,
3. nicht über die erforderliche *Deckungsvorsorge* verfügt,
4. *ungeeignete Produkte* für qualifizierte elektronische Signaturen verwendet oder
5. die *weiteren Voraussetzungen* für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Signaturverordnung nicht erfüllt.

Vor einer Gewerbeuntersagung sind jedoch „Maßnahmen“ zu treffen, die das Gesaetz jedoch nicht näher spezifiziert.

6.2.3. Deutschland und die Kryptographie

Hauptzweck dieser Regelungen ist offensichtlich, die Erstellung und Verwaltung von Signaturschlüsseln und entsprechenden Zertifikaten zu *zentralisieren* und damit sicherer aber offensichtlich auch *überwachbarer* zu halten. Anscheinend wird hier ein *staatsnahes Gewerbe mit Kontroll- und Lenkungsfunktion* installiert. Inwieweit dies in die Rechte der Bürger eingreifen wird, muß sich zeigen; im wesentlichen dürfte dies wohl davon abhängen, inwieweit der Besitz und die Verwendung elektronischer Schlüssel vorgeschrieben wird. Nach dem Signaturgesetz ist die Verwendung *freigestellt* (§1 Abs. 2 SiG), kann aber durch Gesetz *angeordnet* werden.

Da die zuständige Behörde *die nach §66 des Telekommunikationsgesetzes zuständige Behörde* ist, und da nach diesem Gesetz der Betreiber einer Telekommunikationsanlage die Überwachung der über die Anlage geführten Kommunikation sicherstellen muß, ist die *indirekte Überwachung* von Schlüsseln und verschlüsselten Kommunikationen mit dem neuen Signaturgesetz sichergestellt.

6.2.4. Qualifizierte Zertifikate

Zertifikate dienen der Zuordnung von Schlüsseln zu Personen. Sie wereen von Zertifizierungsdiensteanbietern ausgestellt und verwaltet und stellen sicher, daß der Gebrauch digitaler Signaturen nicht unkontrollierbar „ausufert“, d.h., machen die Kryptographie *überwachbar*.

Während ein „einfaches“ Zertifikat „nur“ einen Schlüssel einer Person zuordnet, muß ein „qualifiziertes“ Zertifikat gemäß §7 Abs. 1 mindestens folgenden Inhalt aufweisen:

1. den *Namen des Signaturschlüssel-Inhabers*, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,
2. den zugeordneten *Signaturprüfschlüssel*,
3. die *Bezeichnung der Algorithmen*, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
4. die *laufende Nummer* des Zertifikates,
5. *Beginn und Ende der Gültigkeit* des Zertifikates,
6. den *Namen des Zertifizierungsdiensteanbieters* und des *Staates*, in dem er niedergelassen ist,
7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang *beschränkt* ist,
8. Angaben, daß es sich um ein *qualifiziertes Zertifikat* handelt, und
9. nach Bedarf *Attribute des Signaturschlüssel-Inhabers*.

Solche Attribute können auch in ein gesondertes qualifiziertes Zertifikat aufgenommen werden, das als qualifiziertes Attribut-Zertifikat bezeichnet wird (§7 Abs. 2 SigG).

6.2.5. Technische Sicherheit

Auch hierzu enthält das Gesetz *umfangreiche Regelungen*. Insbesondere sind für die Überprüfung signierter Daten Signaturanwendungskomponenten erforderlich, die feststellen lassen, auf welche Daten sich die Signatur bezieht, ob die signierten Daten unverändert sind, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und zu welchem Ergebnis die Nachprüfung von Zertifikaten geführt hat (§17 Abs. 2 SigG). Die technischen Komponenten für Zertifizierungsdienste bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit ausschließen, qualifizierte Zertifikate vor unbefugter Veränderung und unbefugtem Abruf zu schützen und bei Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen ausschließen (§17 Abs. 3 SigG).

7. Mathematische Ergänzung: RSA Codierung

Das erinfachste Codierverfahren basiert auf dem RSA-Schlüssel. RSA steht für die Initialen der Nachnamen von Ron Rivest, Adi Shamir und Len Adleman. Ironischerweise war es niemals verboten, den nachfolgenden Algorithmus zu exportieren, sondern nur Programme, die ihn in ausführbarer Form enthalten:

1. Man berechne P und Q, zwei große Primzahlen. Die Größe dieser Primzahlen ist durch die Anzahl der Bits gekennzeichnet, etwa 1024 Bits.

2. Man wähle die Zahl E so, daß E und (P-1)(Q-1) are relative Primzahlen, d.h., keine gemeinsamen Primfaktoren mehr besitzen. E selbst muß keine Primzahl sein, aber es muß eine ungerade Zahl sein. (P-1)(Q-1) kann keine Primzahl sein, weil es stets eine gerade Zahl ist.

3. Man berechne D so, daß (DE - 1) ohne Rest teilbar ist durch (P-1)(Q-1). Mathematiker schreiben dies in der Notationsform DE = 1 MOD (P-1)(Q-1) und bezeichnen D als die multiplikative Inverse von E.

4. Die Verschlüsselungsfunktion ist ENCRYPT(T) = (T^E) MOD PQ. Hierbei steht „T“ für den zu verschlüsselnden Text.
5. Die Entschlüsselungsfunktion ist DECRYPT(C) = (C^D) MOD PQ, wobei C für den Ciphertext, also die verschlüsselte Information T steht.

Der öffentliche Schlüssel besteht aus den Werten PQ und E. Der Privatschlüssel ist D.

Das Produkt aus P und Q ist der Modulus. E ist der öffentliche Exponent und D ist der geheime Exponent.

Da D und E ungleich sind, handelt es sich um ein asymmetrisches Verfahren. E kann beliebig weitergegeben werden, ohne E bloßzulegen.

Dieses Verfahren gilt derzeit als vollkommen sicher, wenn nur die Bitzahl von P und Q ausreichend ist. Einen endgültigen Beweis, daß D nicht zurückgerechnet werden kann, hat jedoch noch niemand erbracht, so daß der Verdacht besteht, daß die Freigabe des Exports von Kryprosoftware durch die US-Regierung auf der Entdekkung einer solchen Rechenmethode beruht. Da jedoch auch zu Zeiten des Bestehens des Exportverbotes Software in wenigen Sekunden illegal heruntergeladen werden konnte, kann diese Neuregelung auch einfach nur der Ausdruck der Erkenntnis sein, daß im Informationszeitalter eine wirksame Exportsperre für Software unmöglich ist.

8. Glossar

Akkreditierung, freiwillige [Gesetzesdefinition aus §2 SigG]: Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind. → Zertifizierungsdiensteanbieter.

Algorithmus: Jede mathematische Folge von Rechen- oder anderen Arbeitsanweisungen.

Asymmetrische Verschlüsselung: Jedes Codierverfahren, bei dem für die Verschlüsselung ein anderer → Schlüssel benötigt wird als für die Entschlüsselung. Der Schlüssel zur Verschlüsselung ist der öffentliche Schlüssel (→ Öffentlicher Schlüssel). Er kann unbeschränkt weitergegeben werden, weil er nicht zur Entschlüsselung taugt. Hierfür eignet sich nur der Privatschlüssel. Beide Schlüssel zusammen heißen auch → Schlüsselpaar.

Attribut-Zertifikat: Ein digitales → Zertifikat, das mehr Informationen als die in §7 Abs. 1 SigG aufgezählten Mindestinformationen enthält. Die Aufnahme von Daten üner Vertretungsverhältnisse und berufsrechtliche oder sonstige Zulassungen des Inhabers sind möglich; weitere Angaben sind nur mit Zustimmung des Betroffenen möglich (§7 Abs. 2 SigG). → Signaturschlüssel-Zertifikat.

Bit: Binary Digit, kleinste Informationseinheit, bestehend nur ein „0“ und „1“. Das Bit ist das Maß für → Schlüssellänge.

Brutale Gewalt: → Methode der brutalen Gewalt.

Ciphertext: Eine verschlüsselte Information.

Container: Die Information, in der eine andere Information (→ Payload) durch → Stageonographie versteckt wird.

Containerdaten: → Container.

Datenschutz: Sicherheitskonzept, das aus → Privacy, → Safety und Security besteht.

Dictionary Attack: Versuch, ein → Password durch Ausprobieren aller Einträge in einem Wörterbuch (Dictionary) herauszufinden. Der einzige sichere Schutz gegen diese Form des Angriffes ist es, als Password keine sinnvolle Zeichenfolge, d.h., kein Wort aus irgendeinem Wörterbuch zu verwenden.

DSA: Abk. für Digital Signature Algorithm, ein Verfahren zur digitalen → Signatur.

DSS: Abk. für Digital Signature Standard, ein auf → DSA aufbauendes Verfahren der digitalen → Signatur.

elektronische Signaturen: → Signatur, elektronische, → Signatur.

Entropie: Das mathematische Maß für den Grad an Unordnung in einem System. Verschlüsselung basiert im wesentlichen auf der kontrollierten Steigerung von Entropie, so daß dem Betrachter der verschlüsselten Information die Erkenntnis ihres eigentlichen (nach bestimmten anderen Mustern geordneten) Inhaltes unmöglich wird. Entschlüsselung ist die Reduktion von Entropie in der Art und Weise, daß nur die zuvor bestehende Ordnung zurückbleibt, d.h., die eigentliche, zuvor verschlüsselte Information wieder zugänglich wird.

Entropy Deconvolution: Mathematisches Verfahren, das „versteckte“ Ordnungen in Daten erkennt und wiederherstellt. Ursprünglich wurde die Methode der Entropy Deconvolution entwickelt, um versteckte feindliche Einrichtungen auf Luftbildern von natürlichen Mustern zu unterscheiden, also etwa versteckte Panzer in Wäldern zu finden. Die Methode eignet sich aber auch, unbekannte archäologische Strukturen in Luftaufnahmen zu finden oder fast ausgelöschte praktisch unsichtbare Schriftzüge auf Pergament, Wänden oder anderen Beschreibstoffen wieder lesbar zu machen.

fortgeschrittene elektronische Signaturen: → Signatur, elektronische, fortgeschrittene.

freiwillige Akkreditierung: → Akkreditierung, freiwillige.

Hash-Funktion: Mathematische Funktion, die aus einer Information eine Art von Prüfsumme errechnet, aus der die ursprüngliche Information nicht wieder zurückgewonnen werden kann. Die Hash-Funktion ist die Grundlage zur Berechnung einer digitalen → Signatur.

Key: → Schlüssel.

Key Server: System im Internet, auf dem öffentliche Schlüssel (→ Öffentlicher Schlüssel) oder Zertifikate (→ Zertifikat) hinterlegt sind.

Klartext: Eine entschlüsselte (oder unverschlüsselte) Information.

Kryptoanalyse: → Kryptographischer Angriff.

Kryptographie: Die Kunst der Verschlüsselung von Informationen.

Kryptographischer Angriff: Der Versuch, einen → Schlüssel aus einer verschlüsselten Information zurückzugewinnen oder auch die verschlüsselte Information ohne Schlüssel zu entschlüsseln.

Methode der brutalen Gewalt: Diejenige Art des kryptographischen Angriffes (→ Kryprographischer Angriff), bei der sämtliche möglichen Schlüssel ausprobiert werden, bis der richtige Schlüssel gefunden wird. Da die Anzahl der möglichen Schlüssel bei großer → Schlüssellänge dramatisch ansteigt, ist diese Methode zumeist ungeeignet.

Öffentlicher Schlüssel: Der → Schlüssel, der nur zum Ver- aber nicht zum Entschlüsseln einer Information geeignet ist. Der öffentliche Schlüssel kann unbeschränkt weitergegeben werden, um anderen die Verschlüsselung von Informationen zu erlauben. Zu jedem öffentlichen Schlüssel gehört ein → Privatschlüssel.

One-time pad: Ein → Schlüssel zur einmaligen Verwendung, der als absolut sicher gilt, gerade weil er durch Singularität kryptographische Angriffe (→ Kryptographische Angriffe) unmöglich macht. One-time pads wurden 1917 von Major J. Mauborgne und G. Vernam erfunden.

Passphrase: In → PGP das → Password für den → Privatschlüssel.

Password: Kombination aus Zeichen, die einem Anwender Zugang zu einem Dienst oder System ermöglichen soll. Um es einem Dritten zu erschweren, Kenntnis von einem Password zu erlangen, sollte es auch Ziffern und Buchstaben bestehen, eine bestimmte Länge besitzen und keinen Sinn haben, der in Zusammenhang mit einer Person gebracht werden kann.

Payload: Die durch → Stageonographie in einem → Container versteckte Information.

PGP: Abk. für Pretty Good Privacy, von Phil → Zimmermann entwickeltes Asymmetrisches Verschlüsselungsprogramm.

Pretty Good Privacy: → PGP.

Privacy: Der Schutz vor unbefugter Einsichtnahme Dritter in Daten. Ein Aspekt des Datenschutzes (→ Datenschutz).

Privatschlüssel: Der → Schlüssel, der nur zum Ent- aber nicht zum Verschlüsseln einer Information geeignet ist. Der Privatschlüssel darf keinesfalls an Dritte weitergegeben werden. Gegenteil: → Öffentlicher Schlüssel.

Public Key: → Öffentlicher Schlüssel.

PUBRING.PGP: Datei bei → PGP, die öffentliche Schlüssel enthält (→ Öffentlicher Schlüssel).

PUBRING.PKR: Datei bei → PGP, die öffentliche Schlüssel enthält (→ Öffentlicher Schlüssel).

qualifizierte elektronische Signaturen: → Signatur, elektronische, qualifizierte.

qualifizierte Zeitstempel: → Zeitstempel, qualifizierte.

qualifizierte Zertifikate: → Zertifikat, qualifiziertes.

RSA: Abk. für Ron Rivest, Adi Shamir und Len Adleman, drei Entwickler von Verschlüsselungssystemen.

Safety: Schutz vor technischem Versagen von Datenverarbeitungssystemen, ein Konzept des Datenschutzes (→ Datenschutz).

Schlüssel: Zum Ver- oder Entschlüsseln benötigte Information. → Öffentlicher Schlüssel, → Privatschlüssel.

Schlüssellänge: Die Anzahl der Bits (→ Bit) in einem Schlüssel und damit ein wesentliches Maß für die Anzahl der möglichen Schlüssel und damit die „Stärke" eines Schlüssels. Ein genügend langer Schlüssel ist die Voraussetzung für → Starke Kryptographie.

Schlüsselpaar: Ein → Öffentlicher Schlüssel mit zugehörigem → Privatschlüssel. Ein Schlüsselpaar wird immer gemeinsam erzeugt, aber nur der öffentliche Schlüssel darf weitergegeben werden.

Schwache Kryptographie: Jede Form der → Kryptographie, die relativ leicht zu brechen ist (→ Kryptographischer Angriff). Gegenteil: → starke Kryptographie. Die Grenze zu „stark" ist recht unscharf definiert.

Secret Key: → Privatschlüssel.

SECRING.PGP: Datei bei → PGP, die→ Privatschlüssel enthält.

SECRING.SKR: Datei bei → PGP, die→ Privatschlüssel enthält.

Security: Schutz vor Sabotage von Daten oder Datenverarbeitungssystemen, ein Konzept des Datenschutzes (→ Datenschutz).

Sicherer Kanal: Übertragungsweg, auf dem uneingeschränkter → Datenschutz gewährleistet ist. Bei symmetrchen Schlüsseln (→ Symmetrisches Codierverfahren) ist ein sicherer Kanal zunächst erforderlich, bevor verschlüsselte Daten ausgetauscht und wieder entschlüsselt werden können. Im Internet gibt es keinen sicheren Kanal.

SigG: Abk. für → Signaturgesetz.

SigVO: Abk. für → Signaturverordnung.

Signatur [Allgemeine Definition]: Digitale Unterschrift unter einer Information zur eindeutigen Feststellung der Urheberschaft der Information.

Signatur, elektronische [Gesetzesdefinition aus §2 SigG]: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

Signatur, elektronische, fortgeschrittene [Gesetzesdefinition aus §2 SigG]: elektronische Signaturen, die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und mit den Daten, auf die sie sich beziehen, so verknüpft sind, daß eine nachträgliche Veränderung der Daten erkannt werden kann.

Signatur, elektronische, qualifizierte [Gesetzesdefinition aus §2 SigG]: elektronische Signaturen, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Signaturanwendungskomponenten: im Sinne des Signaturgesetzes Software- und Hardwareprodukte, die dazu bestimmt sind, Daten dem Prozeß der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen (→ Signatur; → Signatur, elektronische) zuzuführen oder qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,

Signaturgesetz: Seit 1997 geltendes Gesetz über die digitale Signatur, im Mai 2001 neu gefaßt.

Signaturprüfschlüssel: der vom Signaturgesetz verwendete Begriff für öffentliche Schlüssels. → Privatschlüssel.

Signaturschlüssel: der vom Signaturgesetz verwendete Begriff für private Schlüssels. → Öffentlicher Schlüssel.

Signaturschlüssel-Inhaber: im Signaturgesetz jede natürliche Personen, die einen → Signaturschlüssel besitzen und denen die zugehörigen → Signaturprüfschlüssel durch qualifizierte Zertifikate (→ Zertifikat, qualifiziertes) zugeordnet sind.

Signaturschlüssel-Zertifikat: Ein digitales → Zertifikat, das die Mindestinhalte des §7 Abs. 1 SigG enthält. → Attribut-Zertifikat.

Signaturverordnung: Im Oktober 1997 aufgrund von §16 SigG erlassene Rechtsverordnung, die die Details über Zertifizierungen und Zertifizierungsdiensteanbieter enthält. → Zertifizierungsstellen nach §4 SigG.

Stageonographie: Die Kunst, Daten in anderen Informationen so zu verstecken, daß das Vorhandensein der versteckten Daten dem Betrachter der Information, in welcher die Daten versteckt sind nicht ohne weiteres offensichtlich wird.

Starke Kryptographie: Jede Form der → Kryptographie, die auch etwa staatlichen Stellen wie Geheimdiensten widersteht. Gegenteil: → schwache Kryptographie. Die Grenze zu „stark" ist recht unscharf definiert.

Symmetrisches Codierverfahren: Jedes Verschlüsselungsverfahren, das für die Ver- und die Entschlüsselung denselben → Schlüssel verwendet. Wer diesen Schlüssel besitzt, kann also sowohl ver- als auch entschlüsseln, so daß für den Schlüssel zunächst ein sicherer Übertragungsweg erforderlich ist.

Trust-Center: Organisation, die digitale Signaturen oder Zertifikate verwaltet und für deren Echtheit bürgt. In Deutschland der → Zertifizierungsdiensteanbieter nach §4 SigG. → Zertifikat.

Unterrichtungspflicht: Die Verpflichtung der → Zertifizierungsdiensteanbieter nach §4 SigG, Antragsteller über technische und rechtliche Aspekte der Anwendung von Signaturen zu informieren.

Unterschrift: → Signatur.

Verifikation: Die Überprüfung einer → Signatur.

Zeitstempel: Angabe über den Zeitpunkt der Errichtung einer → Signatur. Der Z. soll verhindern, daß ein Unbefugter eine Signatur auf einen anderen Namen errichtet. Im deutschen Recht wird der Z. von den → Zertifizierungsdiensteanbietern nach §4 SigG vergeben (§§9 SigG).

Zeitstempel, qualifizierte [Gesetzesdefinition aus §2 SigG]: elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der den Anforderungen des Gesetzes genügt und der die sich darauf beziehenden Vorschriften der Rechtsverordnung erfüllt, darüber, daß ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

Zertifikat: → Öffentlicher Schlüssel mit zusätzlichen Informationen über seinen Urheber und einer digitalen → Signatur. Vgl. insbes. §§5, 7, 8 SigG mit der Aufzährung von Mindestinhalten. Die beiden vom SigG unterschiedenen Typen von Zertifikaten sind das → Signaturschlüssel-Zertifikat und das → Attribut-Zertifikat.

Zertifikat, qualifiziertes: Zertifikate mit bestimmten Mindestinhalten (§7 Abs. 1 SigG).

Zertifizierungsdiensteanbieter nach §4 SigG: Durch eine Behörde nach §66 des Telekommunikationsgesetzes zugelassene privatrechtliche oder öffentlich-rechtliche Organisation, die digitale Zertifikate verwaltet (→ Zertifikat), d.h., durch Rechtsvorschriften für Deutschland vorgeschriebene → Trust Center.

Zimmermann, Phil: Schöpfer von → PGP, einem Verschlüsselungsprogramm für → starke Kryptographie, und von vielen als eine Art Held betrachtet.