Black Box erklärt Verschlüsselung / Digitale Signatur

1. Einleitung

Das Internet – als weltweites Computernetzwerk – bietet fast alles was man sucht: Nachrichten, Lexika, Spiele und andere Software, virtuelle Einkaufszentren, bis hin zur privaten Homepage des Nachbarn. Und es ist für jeden zugänglich – doch gerade das macht das Internet so gefährlich! Jeden Tag belauschen tausende von Hackern die Datenleitungen des World Wide Web. Doch wie kann man sich davor schützen? Eine Möglichkeit hierfür ist die Verschlüsselung. Alle Welt spricht darüber, wenige nutzen sie, noch weniger wissen wie die Verschlüsselung genau funktioniert. Im folgenden Essay wollen wir einen kurzen Einblick in die Welt der Verschlüsselung geben.

2. Historie

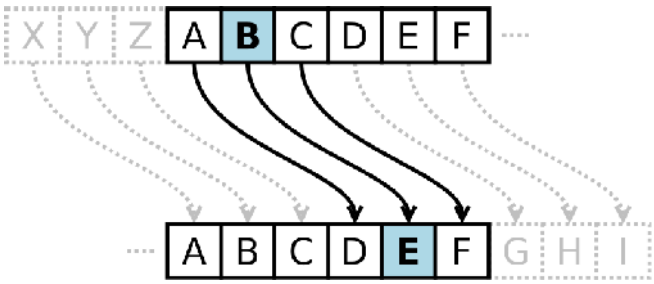
Ursprünglich entstand die Verschlüsselung zu militärischen Zwecken – der Feind, der eine Nachricht abgefangen hatte, konnte damit nichts anfangen, ihm fehlte ja der Schlüssel, um den durch die Verschlüsselung entstandenen Buchstabensalat in Klartext umzuwandeln. Ein einfaches Beispiel:

2.1 Die Cäsar-Verschlüsselung:

Es handelt sich hierbei um eine der einfachsten Verschlüsselungsarten und wird am besten klar, wenn man sich das gesamte Alphabet niederschreibt und betrachtet:

Uns bekanntes Alphabet																									
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
Alphabet um 3 Stellen nach links verschoben																									
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

Wenn man diese Darstellung betrachtet, fällt auf, dass man bereits eine Art Verschlüsselungsschema erstellt hat. Der Buchstabe A wird im obigen Schema als D kodiert, der Buchstabe M beispielsweise als P, anders ausgedrückt: Geht man im Alphabet 3 Buchstaben weiter nach rechts, bekommt man am Ende einen mehr oder weniger sinnlosen Buchstabensalat.



Beispiel für die Cäsar-Verschlüsselung:

Sie möchten folgenden Text verschlüsseln:

„Ich lese gerne die Black Box Wissensdatenbank.“

Unser Klartext																								
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
...wird zu								↓																	
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

Laut unserem Schema wird: I → L, C → F, H →K, usw.

Der Verschlüsselte Satz lautet nun:

„LFK OHVH JHUQH GLH EODFN ERA ZLPPHQVGDWHQEDQN“,
also erstmal völlig unverständlich für denjenigen, der es liest. Hier handelt es sich jedoch um eine sehr einfache Art der Verschlüsselung und mit ein bisschen überlegen und ausprobieren kann man auf die richtige Entschlüsselungsmethode kommen.

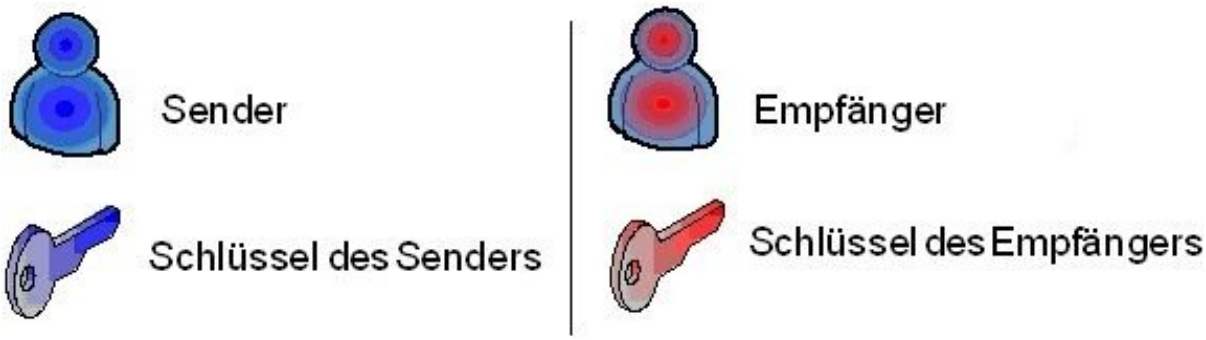
Ein Lösungsansatz ist beispielsweise die Betrachtung der statistischen Buchstabenwahrscheinlichkeit, das heißt, wie oft ein Buchstabe durchschnittlich in einem Text vorkommt. Berechnungen haben ergeben, dass in der deutschen Sprache der Buchstabe „E“ mit einer Wahrscheinlichkeit von 17,40% am häufigsten vorkommt. So kann man zumindest einmal einen Buchstaben entschlüsseln und herausfinden um wie viele „Stellen“ das Chiffre verschoben wurde.

3. Verschlüsselung

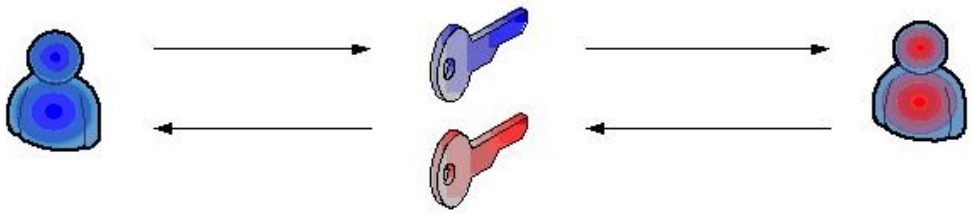
In der heutigen Zeit ist eine Verschlüsselung wie die Cäsar-Verschlüsselung längst überholt und gilt als unsicher und nicht brauchbar für den Einsatz in der Datenkommunikation. Grundsätzlich werden heute 2 Arten von Verschlüsselungen in der Computerwelt verwendet: Die symmetrische und die asymmetrische Verschlüsselung.

3.1 Die Symmetrische Verschlüsselung

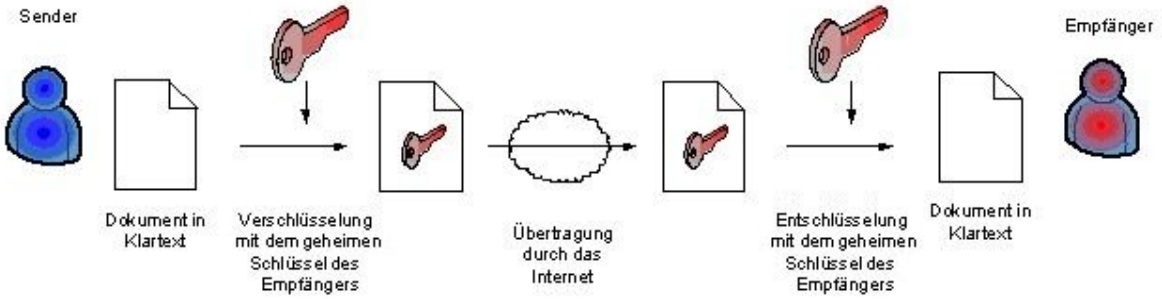
Grundlegende Vorraussetzung für die sichere Kommunikation ist, dass jeder der beiden Kommunikationspartner sich selbst einen Schlüssel generiert hat. Hierzu stehen im Internet Freewareprogramme zur Verfügung. Der Schlüssel ist geheim und darf – ähnlich wie ein Passwort – nicht an jeden, sondern nur an gewünschte Kommunikationspartner weitergegeben werden.



Um nun sicher kommunizieren zu können, brauchen die Kommunikationspartner jeweils den geheimen Schlüssel des anderen. Folglich muss ein Schlüsseltausch durchgeführt werden. Genau hier liegt bereits die erste Schwachstelle der symmetrischen Verschlüsselung, später jedoch mehr dazu. Beide Kommunikationspartner haben nun den Schlüssel des jeweils anderen.



Jetzt kann der verschlüsselte Datenverkehr beginnen. Der Sender verschlüsselt nun die zu versendende Nachricht (Email, etc.) mit dem Schlüssel, den er vom Empfänger bekommen hat. Das Dokument ist nun verschlüsselt und wird über das Internet übertragen. Der Empfänger erhält das verschlüsselte Dokument und entschlüsselt dieses mit seinem Schlüssel. Nun hat er wieder das ursprüngliche Dokument im Klartext vorliegen.



Ein Nachteil, wie bereits erwähnt, ist der Schlüsseltausch. Der bequemste aber gleichzeitig gefährlichste Weg ist, den Schlüssel über das Internet, via Email auszutauschen. Sollte die Mail mit dem Schlüssel von einem Hacker abgefangen werden, ist die gesamte zukünftige Kommunikation nicht sicher, da der Hacker alle zukünftigen Nachrichten wieder abfangen und mit dem gestohlenen Schlüssel entschlüsseln kann. Deshalb sollte der Schlüssel auf einem Datenträger wie z.B. einem USB-Stick, einer Chipkarte, einer Diskette oder einer CD ausgetauscht werden. Die CD sollte anschließend vernichtet, bzw. der Schlüssel sollte vom USB Stick gelöscht werden, um eine unbefugte Verteilung des Schlüssels zu unterbinden.

Bei weiter entfernten Kommunikationspartnern ist auch der Postweg eine Alternative, doch es ist nie sichergestellt, dass nicht doch jemand Einblick in die Sendung und somit Zugang zum Schlüssel hat. Daraus ergibt sich noch das Problem, dass jeder, der den Schlüssel eines Teilnehmers besitzt, jede seiner Nachrichten lesen kann, ob sie nun ursprünglich an ihn adressiert waren oder nicht.

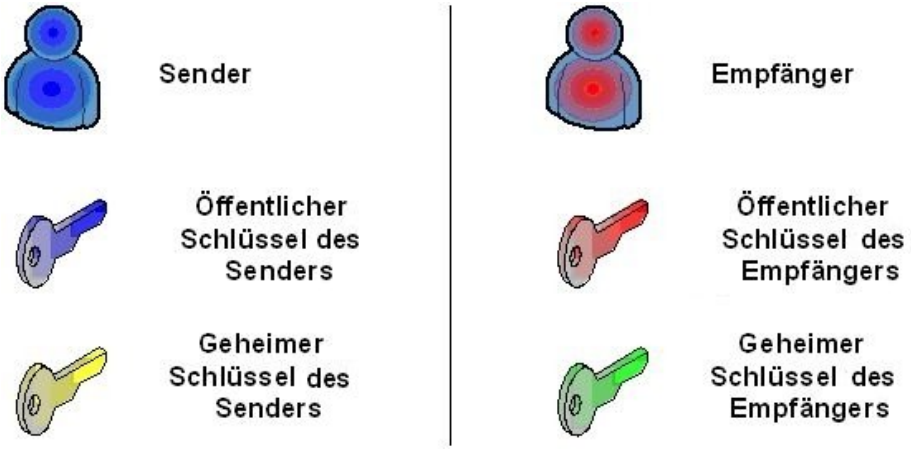
Ein weiterer Nachteil ist, dass jeder Kommunikationspartner den Schlüssel des Empfängers benötigt, an den er eine verschlüsselte Nachricht senden will. Bei einer 50-köpfigen Forschergruppe zum Beispiel, die alle ihre neuesten Erkenntnisse verschlüsselt austauschen wollen, hat jeder der Forscher seinen eigenen plus 49 Schlüssel seiner Kommunikationspartner, macht 50 geheim zu haltende Schlüssel pro Benutzer.
Beispiele für symmetrische Verschlüsselungsverfahren, auf die wir an dieser Stelle nicht genauer eingehen möchten sind:

- Data Encryption Standard (DES / 3DES), seit 1976
- International Data Encryption Algorithm (IDEA), seit 1990
- Advanced Encryption Standard (AES), seit 2000

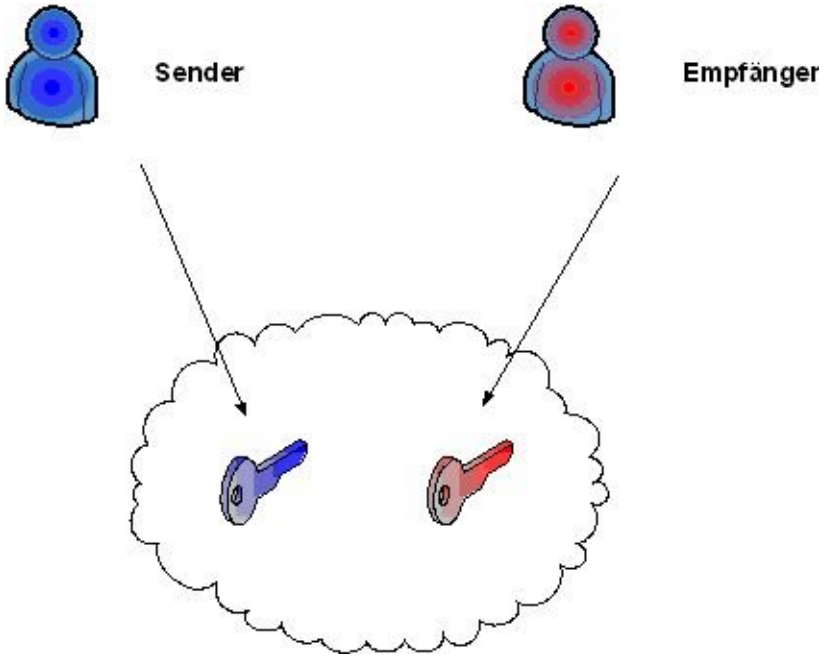
Diese Verschlüsselungsverfahren unterscheiden sich im allgemeinen in der Länge ihrer Schlüssel, meistens angegeben in Bit (64Bit, 128Bit, etc.). Je länger der Schlüssel, desto sicherer ist er und desto länger braucht auch ein möglicher Angreifer, um ihn zu entschlüsseln. Auch spielt der Algorithmus (die mathematische Formel) eine Rolle, mit dem der Schlüssel erzeugt wird. Je komplizierter, desto sicherer. Die AES-Verschlüsselung wird beispielsweise bei der Benutzer-authentifizierung des Black Box ServSwitch DTX oder dem ServSwitch Wizard IP verwendet.

3.2 Die asymmetrische Verschlüsselung

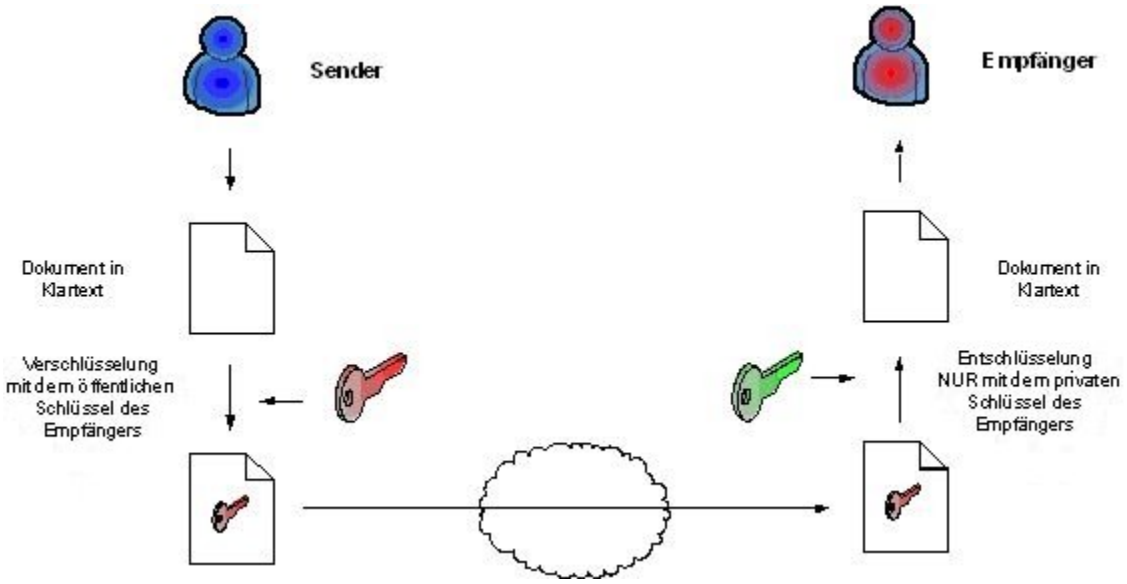
Die Vorraussetzungen für die asymmetrische Verschlüsselung sind etwas umfangreicher als die der Symmetrischen. Hierzu muss sich jeder Teilnehmer ein Schlüsselpaar generieren, bestehend aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel ist – wie der Name schon sagt privat und darf nicht weitergegeben werden, der öffentliche Schlüssel jedoch kann überall verteilt werden. Sie könnten ihn sich sogar auf Ihre Visitenkarte schreiben.
So sieht also die Ausgangssituation der asymmetrischen Verschlüsselung aus:



In unserem Beispiel stellen beide Teilnehmer Ihre öffentlichen Schlüssel im Web zur Verfügung.



Der Sender verschlüsselt jetzt das Dokument, dass er dem Empfänger schicken möchte mit dem öffentlichen Schlüssel des Empfängers. Der öffentliche Schlüssel ist ja allen offen zugänglich, es fällt also das Risiko der unsicheren Übertragung weg, denn jeder darf den öffentlichen Schlüssel haben. Das Dokument wird nun über das Internet übertragen. Der Empfänger entschlüsselt – und das ist der Trick der asymmetrischen Verschlüsselung – mit seinem privaten Schlüssel, den nur er hat. Ein Dokument, das mit dem *öffentlichen* Schlüssel des Empfängers verschlüsselt wurde, kann **nur** mit dem *privaten* Schlüssel des Empfängers wieder entschlüsselt werden. So kann ausschliesslich der eigentliche Empfänger die Nachricht verstehen, da nur er seinen eigenen privaten Schlüssel hat. Nach dem Entschlüsseln liegt dem Empfänger die Nachricht wieder im Klartext vor.

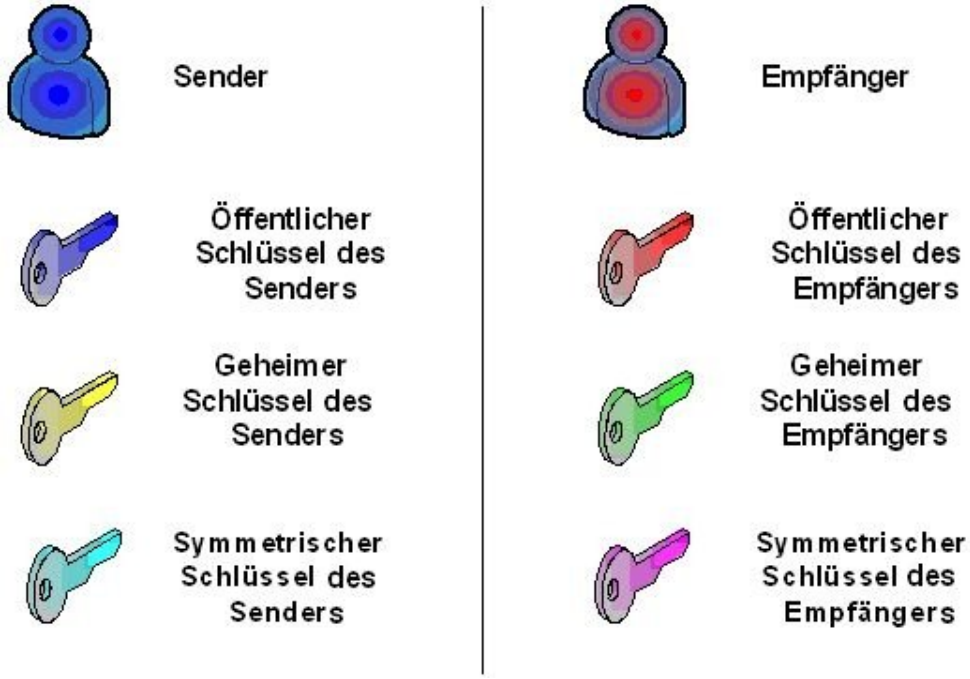


Die Vorteile dieser Verschlüsselung liegen klar auf der Hand: Dadurch, dass der Schlüssel, mit dem entschlüsselt wird, niemals die „Hände des Besitzers“ verlässt, kann ihn auch niemand abfangen und für seine Zwecke missbrauchen. Es ist bis dato auch kein mathematischer Zusammenhang bekannt, um rechnerisch vom öffentlichen Schlüssel auf den privaten Schlüssel eines Schlüsselpaares zu kommen.

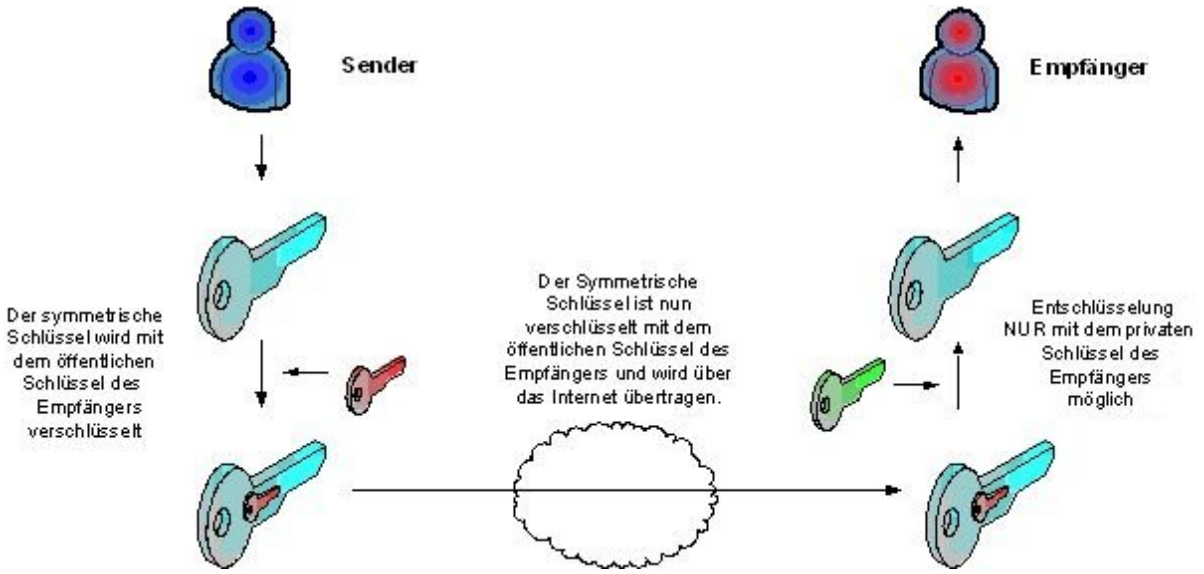
Ein weiterer Vorteil dieser Methode ist, dass nur der eigene private Schlüssel gespeichert werden muss, somit sinkt der Aufwand, viele geheime/private Schlüssel sicher verwahren zu müssen. Alle öffentlichen Schlüssel können entweder nach Bedarf angefordert oder herunter geladen werden, bzw. völlig ungesichert auf dem Rechner oder einem Blatt Papier hinterlegt werden.
Diese Methode bietet jedoch auch einen gewaltigen Nachteil: Die Geschwindigkeit der Ver- bzw. Entschlüsselung ist erheblich langsamer als die der Symmetrischen.
Eine asymmetrische RSA-Verschlüsselung ist mindestens um den Faktor 1000 langsamer als die symmetrische Variante wie z.B. DES oder AES (siehe 3.1 oben).
Wie man sieht, hat auch diese Verschlüsselungsart ihren Nachteil, deshalb kamen findige Tüftler auf einen cleveren Mittelweg – das Hybridverfahren.

3.3 Das Hybridverfahren

Hier werden die Vorteile der symmetrischen und der asymmetrischen Verschlüsselung vereint. Nun haben wir folgende Ausgangssituation:
Sender und Empfänger haben sich je ein asymmetrisches Schlüsselpaar und zusätzlich je einen symmetrischen Schlüssel generiert.



Der öffentliche Schlüssel des asymmetrischen Schlüsselpaares wird wie bei der asymmetrischen Verschlüsselung jedem frei zugänglich gemacht. Der Sender verschlüsselt jetzt statt eines Dokuments seinen Schlüssel von der Symmetrischen Verschlüsselung, den er dann zum Empfänger schickt und umgekehrt.



Auf diese Weise ist die Sicherheitslücke der symmetrischen Verschlüsselung umgangen und man kann zukünftig schnell und zuverlässig mit der symmetrischen Verschlüsselung arbeiten, da sichergestellt ist, dass die Verbreitung des Symmetrischen Schlüssels nicht „abgehört“, oder besser gesagt, nicht entschlüsselt werden kann. Der Aufwand der Schlüsselspeicherung jedoch bleibt.

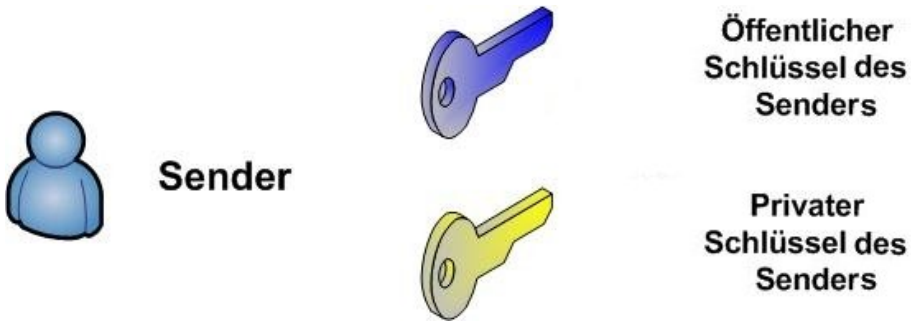
Dieses Hybridverfahren findet beispielsweise bei SSH / SSL statt. Dabei wird ein symmetrischer „Sitzungsschlüssel“, der etwa alle 60min erneuert wird, über eine asymmetrisch verschlüsselte Verbindung getauscht. Die Verbindung unserer Black Box SecureDevice Server (LEB400, LS1001) arbeiten z.B. mit dieser SSL bzw. SSH-Verschlüsselung.

3.4 Die Zukunft der Verschlüsselung

Gerade in der heutigen High-Tech-Generation wird die Vertraulichkeit von Daten immer wichtiger. Längst haben z.B. billige Plagiate und Nachahmungen von IPods, Camcordern, etc. die Weltmärkte überspült – wer weiß, vielleicht fingen die Nachahmungen mit einer unbefugt abgefangenen, unverschlüsselten E-Mail an, die z.B. Baupläne enthielt?
Möchten Sie, dass all Ihre Emails – ob nun mit privaten oder geschäftlichen Inhalten – ungeschützt durchs Internet strömen?
In den USA haben Geheimdienste bereits das Recht zur Überwachung des E-Mail-verkehrs. In Deutschland ist das Durchstöbern von Privatrechnern aktuell Thema im Bundestag.
Wie lange werden die heutigen Verschlüsselungsalgorythmen noch standhalten?
Generell ist damit zu rechnen, dass irgendwann auch die stärkste Verschlüsselung mit Super-Rechnern der neusten Generation geknackt werden kann. Neue Verschlüsselungsalgorythmen werden geschaffen, um wiederum geknackt zu werden.
Fazit: Die Datenkommunikation wird wohl nie zu 100% sicher stattfinden können. Dennoch ist die Verschlüsselung des E-Mailverkehrs ein erster Schritt zur Geheimhaltung sensibler Daten, denn sie erschwert denjenigen die Arbeit, die unauthorisiert Daten im Internet sammeln.

4. Ähnliche Anwendungsgebiete: Digitale Signatur

In den vorangegangenen Beispielen wurden die Schlüssel dazu verwendet, Dokumente verschlüsselt über das Internet zu übertragen, um sie vor Neugierigen zu schützen. Man kann sie jedoch auch dazu verwenden, die Echtheit eines Dokuments nachzuweisen. Dies wird „Digitale Signatur“ oder „Digitale Unterschrift“ genannt. Wir haben folgende Ausgangssituation:



Vergleichen Sie zum besseren Verständnis die einzelnen Schritte mit der nachfolgenden Grafik.

1. Aus einem Dokument wird ein sog. Hash-Wert (auch „Prüfsumme“) errechnet.
   Dazu nutzt man einen Algorithmus, der jedem bekannt ist.

2. Dieser gebildete Wert wird nun mit dem privaten Schlüssel des Absenders verschlüsselt. Ab jetzt nennt man den Wert „digitale Signatur“.

3.Diese Signatur wird nun an das Dokument angehängt und das Dokument verschickt.

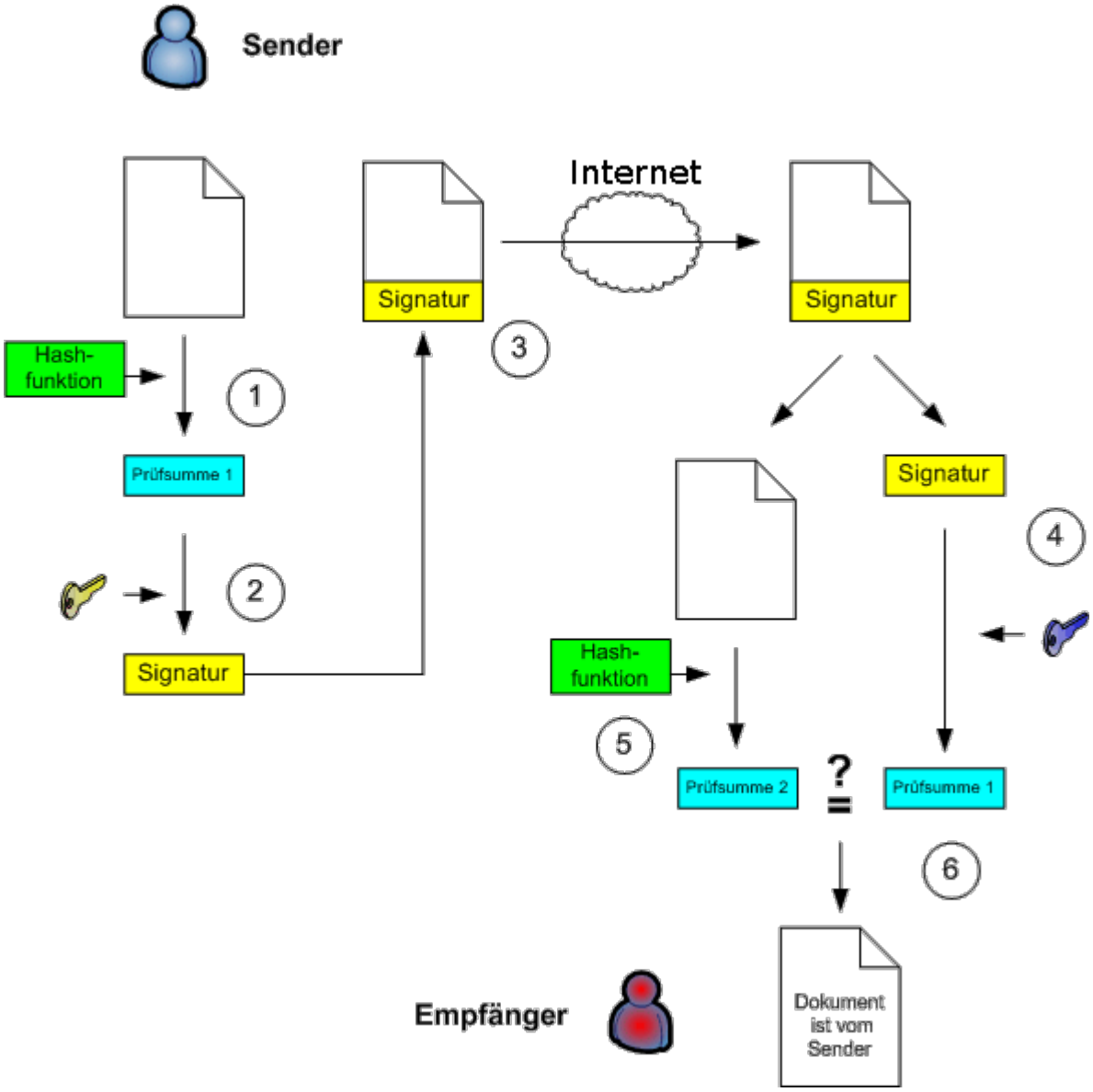
4.Der Empfänger entschlüsselt nun die Signatur mit dem **öffentlichen** Schlüssel des Senders und erhält wieder den Hash-Wert im Klartext.

5.Außerdem bildet er einen eigenen Hash-Wert vom Dokument mit der allen bekannten Hash-Funktion.

6.Wenn diese beiden Werte identisch sind, ist zweifelsfrei nachgewiesen, dass es sich bei dem Absender, um den Besitzer der Schlüssel handelt. Denn nur der wahre Sender konnte den Hash-Wert so verschlüsseln, dass er mit seinem öffentlichen Schlüssel decodiert wieder den richtigen Hash-Wert ergibt. Sollte das Dokument abgefangen und verändert worden sein, passt der vom Empfänger generierte Hash-Wert nicht mehr zum ursprünglich erzeugten Hash-Wert des Senders.

Nehmen wir einmal an, ein Hacker fängt eine digital signierte Nachricht ab. Er könnte jetzt das Dokument beliebig abändern. Er kennt natürlich auch den Hash-Algorithmus, bildet also einen korrekten Hash-Wert passend zum Dokument. Doch was ihm fehlt, ist der private Schlüssel des Senders, denn nur wenn die Prüfsumme mit ihm kodiert wird, ergibt sie entschlüsselt wieder denselben Wert, den der Empfänger mit der Hash-Funktion selbst vom Dokument bildet.

Eine unauthorisierte Änderung des Dokuments fällt dem Empfänger also beim vergleichen der Hash-Werte auf. Üblicherweise findet die Übertragung des Dokuments mit dem Hash-Wert zur Erhöhung der Sicherheit noch verschlüsselt statt. Dies wurde aus Gründen der Übersichtlichkeit in der Grafik weggelassen.



4.1 Sicherheitsstufen der digitalen Signatur

Asymmetrische Schlüsselpaare können auf verschiedenste Weise erstellt werden. Die einfachsten Schlüssel werden per Freeware selbst generiert, für die komplexeren, höherwertigen Signaturen werden Beweise gefordert, die eine Echtheit des Schlüssels bestätigen können.

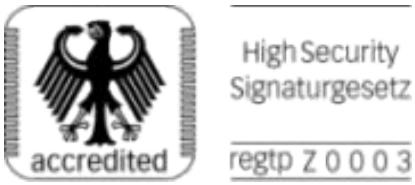
Es gibt drei verschiedene „Sicherheitsstufen“ solcher asymmetrischer Schlüsselpaare:

- Einfache elektronische Signatur
- Fortgeschrittene elektronische Signatur
- Qualifizierte elektronische Signatur

Schlüssel für qualifizierte elektronische Signaturen werden beispielsweise nur ausgestellt, nachdem man sie persönlich unter Vorlage des Personalausweises bei einem als Trustcenter (trust = Vertrauen, center = Zentrum) zertifizierten Anbieter oder dessen Partnern beantragt. Dies gewährleistet später eine sehr hohe Authentizität (=Echtheit) der Daten bzw. des Absenders. Diese Trustcenter unterliegen strengen Regularien, vom Aufbau ihrer Serverräume bis hin zur Ausgabeform der Schlüssel. Die Bundesnetzagentur überwacht die Arbeit der Trustcenter.

Solche Trustcenter sind beispielsweise www.d-trust.de oder www.secrypt.de.

Grundsätzlich lässt sich sagen, je höherwertig die Signatur ist, desto mehr Bedeutung trägt sie auch im Rechtsverkehr. Dies geht soweit, dass vom Gesetzgeber geforderte Dokumente in Papierform durch elektronische Dokumente mit qualifizierter Signatur ersetzt werden dürfen.



Prüfsiegel der Bundesnetzagentur für akkreditierte Anbieter von qualifizierten elektronischen Signaturen.

4.2 Die Zukunft der digitalen Signatur

Dank der digitalen Signatur werden wir uns in naher Zukunft viele Unannehmlichkeiten und Wege ersparen:

- Unsere Finanztransaktionen werden ohne eine lästige TAN-Nummerneingabe vollzogen werden können.
- Medizinische Akten können eindeutig einem Patienten zugewiesen werden, Verwechslungen bleiben aus.
- Die Kommunikation zwischen Ämtern und Bürgern soll künftig voll elektronisch stattfinden, keine lästigen Wartezeiten mehr vor Ort, kein langsamer Briefverkehr mehr.
- Computersoftware kann eindeutig als Original identifiziert werden, das Einschleusen von Dialern/Trojanern/Viren oder Anbieten von manipulierter Originalsoftware ist nicht mehr möglich.

Daniel Brielbeck
Sales Representative
Black Box Deutschland GmbH