Facharbeit Informatik

Public Key Verschlüsselung Speziell: PGP

Ole Mallow
Basiskurs Informatik

Inhaltsverzeichnis

Inhaltsverzeichnis 2

1. Allgemein 3
   1.1 Was ist Public Key Verschlüsselung? 3
   1.2 Warum Public Key Verschlüsselung ? 3
   1.3 Wo werden diese Verfahren eingesetzt? 3

2. PGP 4
   2.1 Was ist PGP? 4
   2.2 Keys („Schlüssel“) 4
   2.3 Digitale Signaturen 5
      Allgemein 5
      Einsatz in PGP 5
      Beispiel 5
   2.4 Ver- und Entschlüsselung 6
      Allgemein 6
      Verschlüsselung 7
      Schema 7
      Entschlüsselung 7
      Schema 7
   2.5 Vor und Nachteile 8

3. Begriffserläuterungen und Anhänge 9
   3.1 Symmetrische und Asymmetrische Verschlüsselung 9
   3.2 Quellennachweis 9

1. Allgemein

1.1 Was ist Public Key Verschlüsselung?

Public Key Verschlüsselung dient zur Weitergabe von Information im Internet unter Verwendung bestimmter Schlüssel, die nur demjenigen, der die Nachricht erhalten soll, bekannt sind. Bei einer Verschlüsselung mit diesem Verfahren werden genau 2 Schlüssel verwendet: ein so genannter *Public Key* („öffentlicher Schlüssel“) und ein *Private Key* („privater oder individueller Schlüssel“). Da zwei verschiedene Schlüssel existieren, wird diese Methode auch als asymmetrisch bezeichnet. Aufgrund mathematischer Zusammenhänge kann eine verschlüsselte Nachricht immer nur mit dem zu einem bestimmten Paar dazugehörigen Schlüssels wieder entschlüsselt werden. Es gibt verschieden *Public Key* Verschlüsselungsvarianten: RSA, die den Industriestandard darstellt; PGP, eine weit verbreitete Mailverschlüsselungsvariante und SET, welche bei E-Commerce verwendet wird.

1.2 Warum Public Key Verschlüsselung ?

Public Key Verschlüsselung wird eingesetzt um das Risiko beim Austausch bestimmter, einmaliger Schlüssel zu minimieren. Mit diesen symmetrischen („gleichen“) Schlüsseln kann genauso gut etwas chiffriert werden, allerdings besteht das Risiko, dass beim Austausch dieses Codes ein Dritter Einsicht erhält. Die Chance, dass ein Dritter Informationen über den Schlüssel erhält, steigt, umso mehr Individuen diesen Schlüssel erhalten. Bei den Verfahren mit dem öffentlichen Schlüssel wird dies gänzlich vermieden, da jeder ein öffentlichen und einen geheimen Schlüssel besitzt und nur mit dieser Kombination kann chiffriert oder später dechiffriert werden.

1.3 Wo werden diese Verfahren eingesetzt?

Diese Verfahren werden im Internet angewendet, beispielsweise um Mails zu verschlüsseln oder um Kreditkarteninformationen bei Onlinekaufhäusern oder Online-Banking zu verschlüsseln. In der Zukunft sollen diese Verfahren oder werden sie zum Teil heute auch schon eingesetzt, um Chipkarten zu codieren, damit mit diesen irgendwo bezahlt werden kann oder um einfach Zugriff auf bestimmte, gesicherte Informationen zu haben.

2. PGP

2.1 Was ist PGP?

PGP wurde im Jahre 1991 von Phil R. Zimmermann in den USA entwickelt. Der Entwicklung von PGP geht die Fin- und Erfindung des *Puplic Key* Verfahrens voran. Diese ist auf Whitfield Diffie und Martin Hellman zurückzuführen, die diese im Jahre 1976 tätigten. Ein Jahr später legten Ron Rivest, Adi Shamir und Len Adleman weitere Grundsteine, indem sie ein *Puplic Key* Verfahren mit dem Namen RSA gründeten.
PGP (Pretty Good Privacy) ist eine Kombination aus 2 Methoden um die Sicherheit möglichst hoch zu halten: Konventionelle Verschlüsselung und *Public Key* Verschlüsselung.

2.2 Keys („Schlüssel“)

Keys sind die Bestandteile des PGP-Verfahrens, die dazu dienen einen Text in einen neuen Geheimtext zu übersetzen. Sie sind der eigentliche Kern des Verfahrens und von ihnen hängt auch die Sicherheit ab. Keys sind normalerweise sehr große Zahlen. Sie werden in Bits angegeben und eine 1024Bit Schlüssel ist eine sehr große Zahl. Umso größer so ein Schlüssel ist, umso sicherer sind auch die mit ihm verschlüsselten Daten; allerdings dauert der Verschlüsselungs- bzw. Entschlüsselungsprozess umso länger, wenn der Schlüssel entsprechend groß ist. Bei den Schlüsseln kann man die der konventionellen, also symmetrischen, Verschlüsselungsmethodik nicht mit denen des *Public Key* Verfahrens vergleichen, da zum Beispiel ein 80Bit Schlüssel der konventionellen Methodik, dem eines 1024Bit Schlüssels der asymmetrischen Methodik entspräche.
Auch die 100 % Sicherheit eines enorm langen Schlüssels ist nicht gewährleistet, da die Möglichkeit besteht, nur anhand eines *Public Keys* den zugehörigen *Private Key* mathematisch zu errechnen und zu erfassen. Da aber angenommen wird, dass der Rechenaufwand dafür so enorm ist, dass kein Mensch mit den heutigen Computern in der Lage ist, so einen Schlüssel in der Zeit seines Lebens zu errechnen, gelten adäquate Schlüssellängen als sicher. Bei der Wahl seiner Schlüssellänge sollte man also immer darauf achten, welche kriminelle Energie mit welchen Ressourcen und welcher Zeit darauf bedacht sein könnte, den Schlüssel zu knacken.
Alle Schlüssel, die ein Anwender besitzt, werden in 2 verschiedenen Dateien auf der Festplatte gespeichert. Diese Dateien und die darin enthaltenen Schlüssel werden als *Key-Ring* bezeichnet. In der einen Datei wird der *Private Key* gespeichert (*Private Key-Ring*) und in der anderen werden alle *Public Keys* gespeichert, die dem Anwender bekannt sind. Da die *Public Keys* zugänglich sein müssen, häufen sich über die Zeit viele verschiedene Schlüssel in dieser Datei an. Die *Private Key-Ring* Datei wird mit einem eigenen Passwort geschützt, das jedes Mal bei Gebrauch eingegeben werden muss.

2.3 Digitale Signaturen

Allgemein

Digitale Signaturen sind keine eingescannten Unterschriften, die als Bild an eine Nachricht angehängt werden, um deren Gültigkeit zu Gewährleisten, sondern mathematischen Routinen, mit denen Signaturen generiert werden, die einmalig sind und die nicht verändert werden können.

Einsatz in PGP

Digitale Signaturen werden in PGP eingesetzt, um zu kontrollieren, ob:

1. die empfangene Nachricht wirklich vom Absender stammt.
2. die Nachricht auf dem Wege verändert worden ist.

Mittels mathematischen Operationen wird anhand des zu verschickenden Textes ein so genannter *Hash-Wert* generiert. Dieser Wert ist für jeden Text einmalig und wird mit dem *Private Key* des Absenders verschlüsselt, in den normalen Zeichensatz (ASCII-Code) umgewandelt und an die Nachricht angehängt. Der Empfänger kann anschließend mit Hilfe des *Public Keys* des Absenders diesen *Hash-Wert* dechiffrieren PGP bildet nun beim Empfänger ebenfalls einen *Hash-Wert* anhand der angekommenen Nachricht und vergleicht beide Werte miteinander. Nur wenn beide Werte übereinstimmen, kann gewährleistet sein, dass die Nachricht auch vom Absender stammt und dass sie zwischendurch nicht verändert wurde. Diese Signatur-Methode kann mit unchiffrierten Texten verwendet werden oder ebenso gut mit chiffrierten, sie stellt nur sicher, dass die Nachricht nicht verändert wurde und mit dem zum *Public Key* gehörigen *Private Key* verschlüsselt wurde.

Beispiel


```
-----BEGIN PGP SIGNED MESSAGE-----

Dies ist eine digital signierte Nachricht.

-----BEGIN PGP SIGNATURE-----
Version: 2.6.2

iQCVAwUBMwn2/4r9AZDvOhHZAQFLKgP+O2YkTkUy4lOUWaFjBJUho9VOL+vWRFGc
KlZe2x11h41Z1jNpfDcrgv08dDf1fGAHbBFTfUFZN4hKbM5xp176huLnn2ogqkog
rc0iTWgoAQNSfH9V+56zfhUujA7dN+IwCbE0Tg1+i+VM79xP1LdwEP6HH9UAynWE
T0cJfFprKos=
=p19E
-----END PGP SIGNATURE-----
```


Abb. 1

2.4 Ver- und Entschlüsselung

Allgemein

Jeder PGP-Benutzer verfügt über ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Daten, die mit dem öffentlichen Schlüssel kodiert werden, können nur mit dem privaten Schlüssel dekodiert werden. Andrerseits können digitale Unterschriften nur mit dem privaten Schlüssel erstellt werden und mit dem zugehörigen öffentlichen Schlüssel auf Ihre Echtheit überprüft werden.
Der öffentliche Schlüssel (*Public Key*) kann allen Mailpartnern mitgeteilt werden, die diesen, bildlich gesprochen, an ihrem öffentlichen Schlüsselbund (*Public Key* Ring) hängen. Der private Schlüssel (*Private Key*) befindet sich an eines jeden privatem Schlüsselbund (*Private Key* Ring), wird aber niemals jemandem ausgehändigt.
Möchten Sie nun eine verschlüsselte Mail verschicken, so benötigen Sie die öffentlichen Schlüssel (*Public Key*) des Empfängers, verschlüsseln damit die Daten und schicken diese auf die Reise. Der Empfänger -und nur dieser- kann jetzt mit seinem privaten Schlüssel (*Private Key*) die Mail wieder entschlüsseln. Nicht einmal Sie selbst als Absender dieser Mail könnten Sie wieder entschlüsseln.
Um es abschließend zu verdeutlichen: Es existieren für ein Schloss jeweils 2 Schlüssel. Einer dient zum Abschließen des Schlosses – *Public Key*; der Andere wird verwendet, um das Schloss wieder aufzuschließen – *Private Key*.

Verschlüsselung

Wenn ein Benutzer einen Klartext verschlüsseln möchte, dann komprimiert PGP diesen Text erstmal. Das Komprimieren hat den Vorteil, dass Kryptoanalytiker (besser bekannt als „Hacker“) den Text nicht mit so genannten Häufigkeitsanalysen bearbeiten können Anschließend wird der komprimierte Text mit einem Schlüssel codiert der per Zufall generiert wird. Den Zufall bestimmen hierbei die Bewegungen mit der Maus bzw. die Anschläge mit der Tastatur, die in einer bestimmten Zeit verübt werden. Dieser „Zwischenschlüssel“ wird als *Session Key* bezeichnet und ist ein einmaliger Schlüssel, der nie wieder benutzt wird. Nach diesem chiffrieren des Textes zu dem Geheimtext wird der *Session Key* mit dem öffentlichen Schlüssel des Empfängers chiffriert und mit dem Geheimtext mitgesendet.

Schema

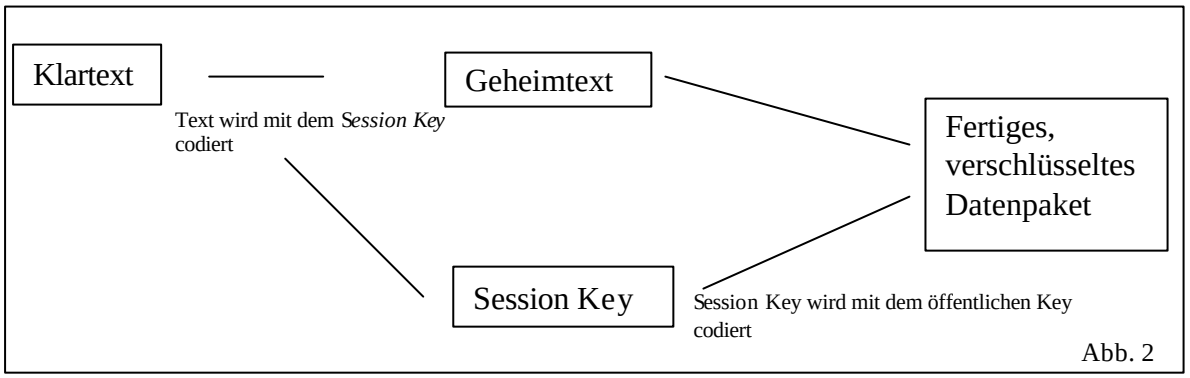

Abb. 2

Entschlüsselung

Um den erhaltenen Geheimtext wieder zu entschlüsseln, wird das Verfahren umgedreht und angewandt. Die Person, die das verschlüsselte Datenpaket erhält kann mit dem eigenen *Private Key* das Datenpaket entschlüsseln. Die erhaltenen beiden Teile werden nun unterschiedlich behandelt. Der verschlüsselte *Session Key* dient nun zur Entschlüsselung des Geheimtextes. Abschließend wird der entschlüsselte Texte noch dekomprimiert, also „entpackt“, und kann dann vom Anwender gelesen werden.

Schema

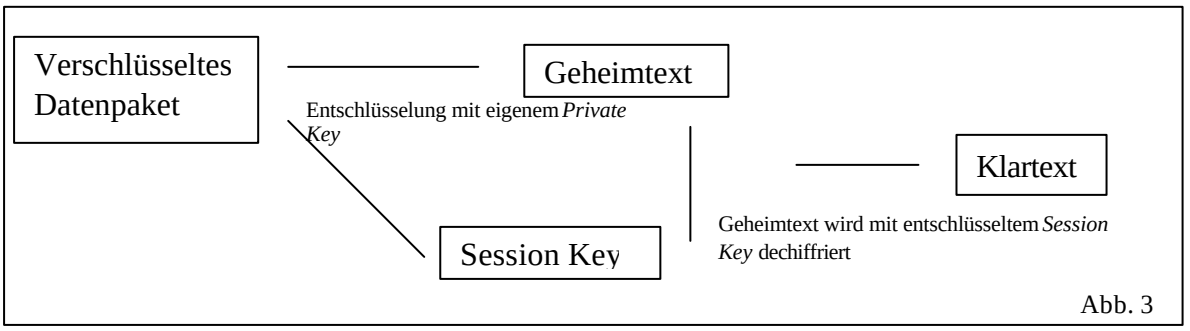

Abb. 3

2.5 Vor und Nachteile

Die Vorteile des in dieser Arbeit vorgestellten Verfahrens sind klar in der Sicherheit im Vergleich zur Symmetrischen Verschlüsselung zu sehen. Denn 1. muss der Schlüssel nicht auf umständlichen Wege (persönlich oder brieflich) übergeben oder übertragen werden, sondern kann ganz einfach veröffentlich werden und 2. muss dieser Schlüssel nicht sehr aufwendig verwaltet werden. Das heißt, dass man ihn einfach in einer mit einem simplen Passwort-Geschützten Datei speichern kann und er dort sicher ist. Und dies kann an einem einzigen Ort geschehen, da keine weiteren Kopien dieses Schlüssels vorhanden sind.
Des Weiteren eignet sich diese Methodik ideal für die Verwendung digitaler Signaturen, sodass auch die Echtheit eines Dokuments garantiert werden kann. Als letzter Punkt sei die kryptologische Unangreifbarkeit zu nennen, die diesem Verfahren weitere Sicherheitsmerkmale gutschreibt. Kryptologische Unangreifbarkeit heißt in diesem Falle, dass es unmöglich ist, den Geheimtext mit Algorithmen zu analysieren und zu interpretieren.

Allerdings birgt dieses Verfahren auch Nachteile, die auf jeden Fall zu nennen sind. Zum einen sind die Schlüssel im Vergleich zu konventionellen Methoden enorm lang und aufwendig zu produzieren. Hiermit einher gehen der Zeitaufwand und die Rechenkapazität, die zum Ent- und Verschlüsseln von Texten benötigt werden. Auch wenn diese Methode der *Public Key* Verschlüsselung als sehr sicher und fast unüberwindbar beschrieben ist, ist nicht bewiesen, dass sie tatsächlich so unüberwindbar ist. Es wird diskutiert, ob zukünftige Rechenleistung oder Algorithmen in der Lage sein werden beliebig lange Schlüssel zu „knacken“. Außerdem besteht auf fast allen gängigen Verfahren Patentschutz, das heißt, dass diese kostenpflichtig sind.

3. Begriffserläuterungen und Anhänge

3.1 Symmetrische und Asymmetrische Verschlüsselung

1. Asymmetrisch

   Man spricht von asymmetrischer Verschlüsselung, wenn zum Ver- und Entschlüsseln einer Nachricht jeweils verschiedene Schlüssel verwendet werden. Jeder Benutzer verfügt über zwei Schlüssel, der eine (privater Schlüssel oder *Private Key*) muss geheim gehalten und der andere (öffentlicher Schlüssel oder *Public Key*) den Kommunikationspartnern öffentlich zugänglich gemacht werden.

2. Symmetrisch

   Wenn für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird, spricht man von symmetrischer Verschlüsselung.
   Daten werden mit dem geheimen Schlüssel verschlüsselt, diese verschlüsselten Daten werden übertragen, und der Empfänger entschlüsselt die Daten mit demselben geheimen Schlüssel.
   Jeder, der den Schlüssel kennt, kann sowohl verschlüsseln als auch entschlüsseln. Jemand, der ihn nicht kennt, kann weder das eine noch das andere.

3.2 Quellennachweis

Der Großteil dieser Arbeit stammt von ***http://www.pgpi.org/doc***, die Ich zuletzt am 13.6.2002 besuchte.
Informationen über digitale Signaturen erhielt ich auf
http://www-rz.fh-reutlingen.de/deutsch/mail/pgp/funktion/digitale_signatur.html.
(Zuletzt besucht am 13.6.2002)