Der Herr der Schlüsselringe

Wenn man etwas sehr Wertvolles sichern will, schließt man es am besten ein - mit einem Schlüssel. Noch besser mit einem Schlüssel, den es nur einmal gibt und den man ganz sicher aufbewahrt.

Denn wenn dieser Schlüssel in die falschen Hände fällt, ist es um die Sicherheit des wertvollen Gutes geschehen. Dessen Sicherheit steht und fällt mit der Sicherheit und Einmaligkeit des Schlüssels. Also muss man den Schlüssel mindestens genauso gut absichern, wie das zu sichernde Gut selbst. Damit er nicht kopiert werden kann, muss auch die genaue Beschaffenheit des Schlüssels völlig geheim gehalten werden.

Geheime Schlüssel sind in der Kryptografie ein alter Hut: Schon immer hat man Botschaften geheim zu halten versucht, indem man den Schlüssel verbarg. Dies wirklich sicher zu machen, ist sehr umständlich und dazu auch sehr fehleranfällig.

Das Grundproblem bei der „gewöhnlichen“ geheimen Nachrichtenübermittlung ist, dass für Ver- und Entschlüsselung derselbe Schlüssel benutzt wird und dass sowohl der Absender als auch der Empfänger diesen geheimen Schlüssel kennen müssen. Aus diesem Grund nennt man solche Verschlüsselungssysteme auch **„symmetrische Verschlüsselung“**.

Dies führt zu einer ziemlich paradoxen Situation: Bevor man mit einer solchen Methode ein Geheimnis (eine verschlüsselte Nachricht) mitteilen kann, muss man schon vorher ein anderes Geheimnis mitgeteilt haben: den Schlüssel. Und da liegt der Hase im Pfeffer: Man muss sich ständig mit dem Problem herumärgern, dass der Schlüssel unbedingt ausgetauscht werden muss, aber auf keinen Fall von einem Dritten abgefangen werden darf.

Gpg4win dagegen arbeitet - außer mit dem geheimen Schlüssel - mit einem weiteren Schlüssel (engl. „key“), der vollkommen frei und öffentlich (engl. „public“) zugänglich ist. Man spricht daher auch von einem „Public-Key“-Verschlüsselungssystem.

Das klingt widersinnig, ist es aber nicht. Der Witz an der Sache: Es muss kein geheimer Schlüssel mehr ausgetauscht werden. Im Gegenteil: Der geheime Schlüssel darf auf keinen Fall ausgetauscht werden! Weitergegeben wird nur der öffentliche Schlüssel (im öffentlichen Zertifikat) - und den darf sowieso jeder kennen.

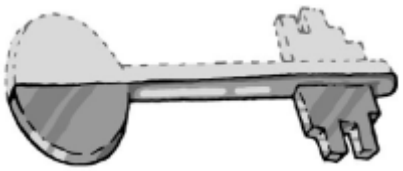
Mit Gpg4win benutzen Sie also ein Schlüsselpaar - einen geheimen und einen zweiten öffentlichen Schlüssel. Beide Schlüsselteile sind durch eine komplexe mathematische Formel untrennbar miteinander verbunden. Nach heutiger wissenschaftlicher und technischer Kenntnis ist es unmöglich, einen Schlüsselteil aus dem anderen zu berechnen und damit das Verfahren zu knacken.

Das Prinzip der Public-Key-Verschlüsselung ist recht einfach:

Der **geheime** oder **private Schlüssel** (engl. ,,secret key„ oder ,,private key“) muss geheim gehalten werden.

Der **öffentliche Schlüssel** (engl. „public key“) soll so öffentlich wie möglich gemacht werden.

Beide Schlüsselteile haben ganz und gar unterschiedliche Aufgaben: Der geheime Schlüsselteil **entschlüsselt** Nachrichten.



Der öffentliche Schlüsselteil **verschlüsselt** Nachrichten. **Der öffentliche Brieftresor**

In einem kleinen Gedankenspiel wird die Methode des „Public-Key“-Verschlüsselungssystems und ihr Unterschied zur symmetrischen Verschlüsselung („Geheimschlüssel-Methode“ oder engl. „Non-Public-Key“-Methode) deutlicher …

Die „Geheimschlüssel-Methode“ geht so:

Stellen Sie sich vor, Sie stellen einen Brieftresor vor Ihrem Haus auf, über den Sie geheime Nachrichten übermitteln wollen.

Der Brieftresor ist mit einem Schloss verschlossen, zu dem es nur einen einzigen Schlüssel gibt. Niemand kann ohne diesen Schlüssel etwas hineinlegen oder herausnehmen. Damit sind Ihre geheimen Nachrichten zunächst einmal gut gesichert - so sicher wie in einem Tresor.

Da es nur einen Schlüssel gibt, muss Ihr Korrespondenzpartner denselben Schlüssel wie Sie haben,

um den Brieftresor damit auf- und zuschließen und eine geheime Nachricht deponieren zu können.

Diesen Schlüssel müssen Sie Ihrem Korrespondenzpartner auf geheimem Wege übergeben.

Erst wenn der andere den geheimen Schlüssel hat, kann er den Brieftresor öffnen und die geheime Nachricht lesen.

Alles dreht sich also um diesen Schlüssel: Wenn ein Dritter ihn kennt, ist es sofort aus mit den geheimen Botschaften. Sie und Ihr Korrespondenzpartner müssen ihn also **genauso** geheim austauschen wie die Botschaft selbst.

Aber - eigentlich könnten Sie ihm bei dieser Gelegenheit ja auch gleich die geheime Mitteilung übergeben …

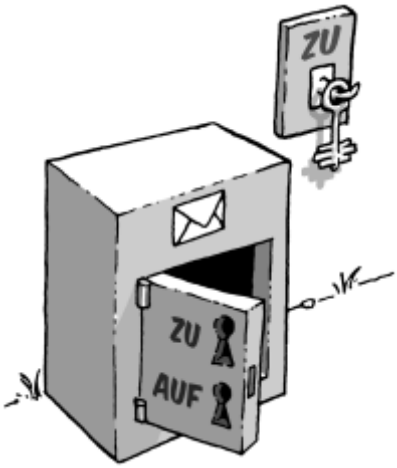
Übertragen auf die E-Mail-Verschlüsselung: Weltweit müssten alle E-Mail-Teilnehmer geheime Schlüssel besitzen und auf geheimem Wege austauschen, bevor sie geheime Nachrichten per E-Mail versenden könnten.

Vergessen Sie diese Möglichkeit am besten sofort wieder …

Nun zur „Public-Key“-Methode:

Sie installieren wieder einen Brieftresor vor Ihrem Haus. Aber: Dieser Brieftresor ist - ganz im Gegensatz zu dem ersten Beispiel - stets offen. Direkt daneben hängt - weithin öffentlich sichtbar - ein Schlüssel, mit dem jedermann den Brieftresor zuschließen kann (asymmetrisches Verschlüsselungsverfahren).

Zuschließen, aber nicht aufschließen: das ist der Trick!



Dieser Schlüssel gehört Ihnen und - Sie ahnen es: Es ist Ihr öffentlicher Schlüssel.

Wenn jemand Ihnen eine geheime Nachricht hinterlassen will, legt er sie in den Brieftresor und schließt mit Ihrem öffentlichen Schlüssel ab. Jedermann kann das tun, denn der Schlüssel dazu ist ja völlig frei zugänglich.

Kein anderer kann den Brieftresor nun öffnen und die Nachricht lesen. Selbst derjenige, der die Nachricht in dem Brieftresor eingeschlossen hat, kann ihn nicht wieder aufschließen, z.B. um die Botschaft nachträglich zu verändern.

Denn die öffentliche Schlüsselhälfte taugt ja nur zum Abschließen.

Aufschließen kann man den Brieftresor nur mit einem einzigen Schlüssel: Ihrem eigenen geheimen, privaten Schlüsselteil.

Wieder übertragen auf die E-Mail-Verschlüsselung: Jedermann kann eine E-Mail an Sie verschlüsseln.

Er benötigt dazu keineswegs einen geheimen, sondern ganz im Gegenteil einen vollkommen öffentlichen, „ungeheimen“ Schlüssel. Nur ein einziger Schlüssel entschlüsselt die E-Mail wieder: Ihr privater, geheimer Schlüssel.

Spielen Sie das Gedankenspiel noch einmal anders herum durch:

Wenn Sie einem anderen eine geheime Nachricht zukommen lassen wollen, benutzen Sie dessen Brieftresor mit seinem öffentlichen, frei verfügbaren Schlüssel.

Sie müssen Ihren Briefpartner dazu nicht persönlich kennen, ihn getroffen oder je mit ihm gesprochen haben, denn sein öffentlicher Schlüssel ist überall und jederzeit zugänglich. Wenn Sie Ihre Nachricht hinterlegt und den Brieftresor des Empfängers mit seinem öffentlichen Schlüssel wieder verschlossen haben, ist sie völlig unzugänglich für jeden anderen, auch für Sie selbst. Nur der Empfänger kann den Brieftresor mit seinem privaten Schlüssel öffnen und die Nachricht lesen.

Aber was ist nun eigentlich gewonnen: Es gibt doch immer noch einen geheimen Schlüssel!?

Der Unterschied gegenüber der „Non-Public-Key“-Methode ist allerdings ein gewaltiger:

Ihren privater Schlüssel kennen und benutzen nur Sie selbst. Er wird niemals einem Dritten mitgeteilt -- die Notwendigkeit einer geheimen Übergabe entfällt, sie verbietet sich sogar.

Es muss überhaupt nichts Geheimes mehr zwischen Absender und Empfänger ausgetauscht werden - weder eine geheime Vereinbarung noch ein geheimes Codewort.

Das ist - im wahrsten Sinne des Wortes - der Knackpunkt: Alle symmetrischen Verschlüsselungsverfahren können geknackt werden, weil ein Dritter sich beim Schlüsselaustausch in den Besitz des Schlüssels bringen kann.

Dieses Risiko entfällt, weil ein geheimer Schlüssel nicht ausgetauscht wird und sich nur an einem einzigen, sehr sicheren Ort befindet: dem eigenen Schlüsselbund - letztendlich Ihrem eigenen Gedächtnis.

Diese moderne Methode der Verschlüsselung mit einem nicht geheimen und öffentlichen, sowie einem geheimen und privaten Schlüsselteil nennt man auch „asymmetrische Verschlüsselung“.