

Verschlüsseln von elektronischen Daten mit PGP nach RSA

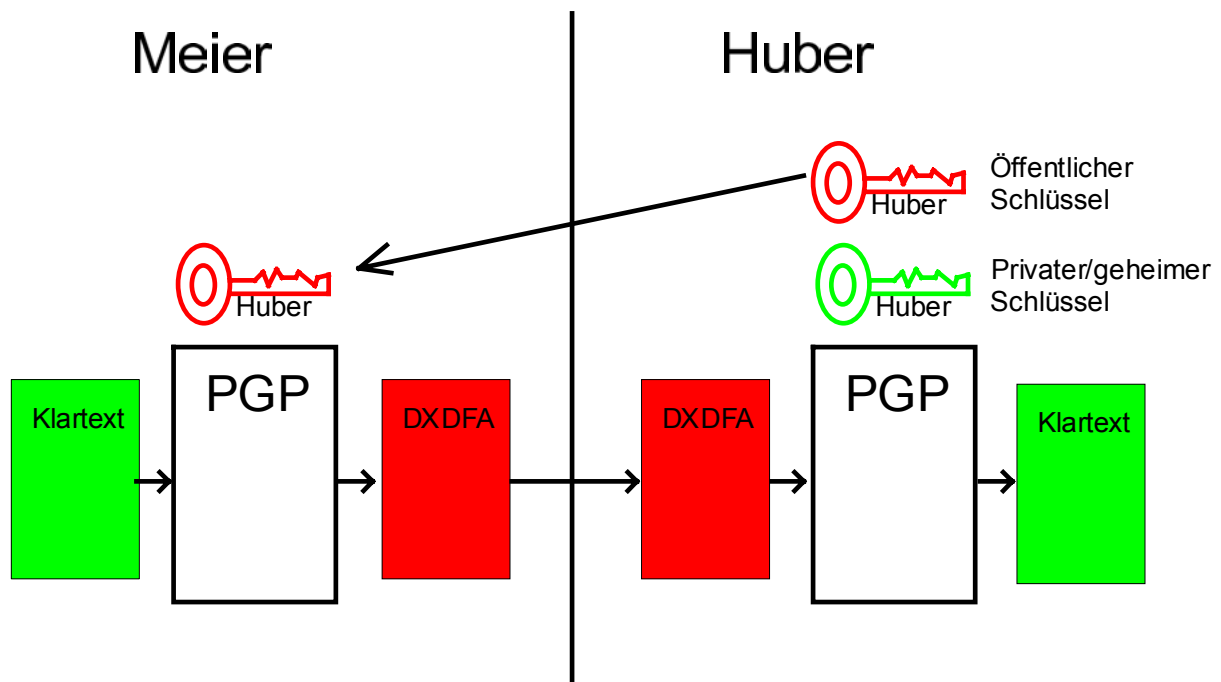
Verschlüsseln heißt, jedes Zeichen eines Klartextes durch ein anderes Zeichen zu ersetzen, so dass die Botschaft für fremde unleserlich wird. Der Empfänger verfügt über die Möglichkeit, diesen Vorgang rückgängig zu machen, so dass er (und nur er) die Botschaft lesen kann.

Bis in die 60-er Jahre benutzte man **symmetrische** Verfahren. Das Ver- und Entschlüsseln erfolgte mit dem selben Schlüssel. Der Schlüssel selbst musste deshalb auf einem sicheren Weg vom Sender zum Empfänger kommen. Durch rasche die Zunahme der Computerisierung in Behörden, Banken usw. wurde die Schlüsselverteilung immer schwieriger und aufwändiger.

Das Verfahren nach **RSA** löste dieses Problem durch eine **asymmetrische** Verschlüsselung. Der Empfänger der Nachricht generiert dazu ein **Schlüsselpaar**. Ein Schlüssel (**rot**) dient zum Verschlüsseln (quasi Zusperrern) der Nachricht. Dieser Schlüssel kann freizügig an alle verteilt werden, z. B. per unverschlüsselter eMail, auf der Homepage oder in Zertifizierungszentren. Der zweite Schlüssel (**grün**) dient zum Entschlüsseln. Diesen privaten/geheimen Schlüssel behält der Empfänger auf seinem PC und schützt ihn dort gegen unbefugte Benutzung durch ein Passwort.

Der Absender einer Nachricht (hier Meier) beschafft sich den öffentlichen (**roten**) Schlüssel des Empfängers (hier Huber) und benutzt ihn dazu, die Nachricht zu verschlüsseln. Diese Nachricht kann nun auf unsicheren Wegen zum Empfänger geschickt werden. Niemand kann diese Nachricht entschlüsseln, auch wenn man den roten Schlüssel und die Nachricht hat. Selbst wenn man den Klartext hat, kann man selbst die Nachricht nicht mehr entschlüsseln.

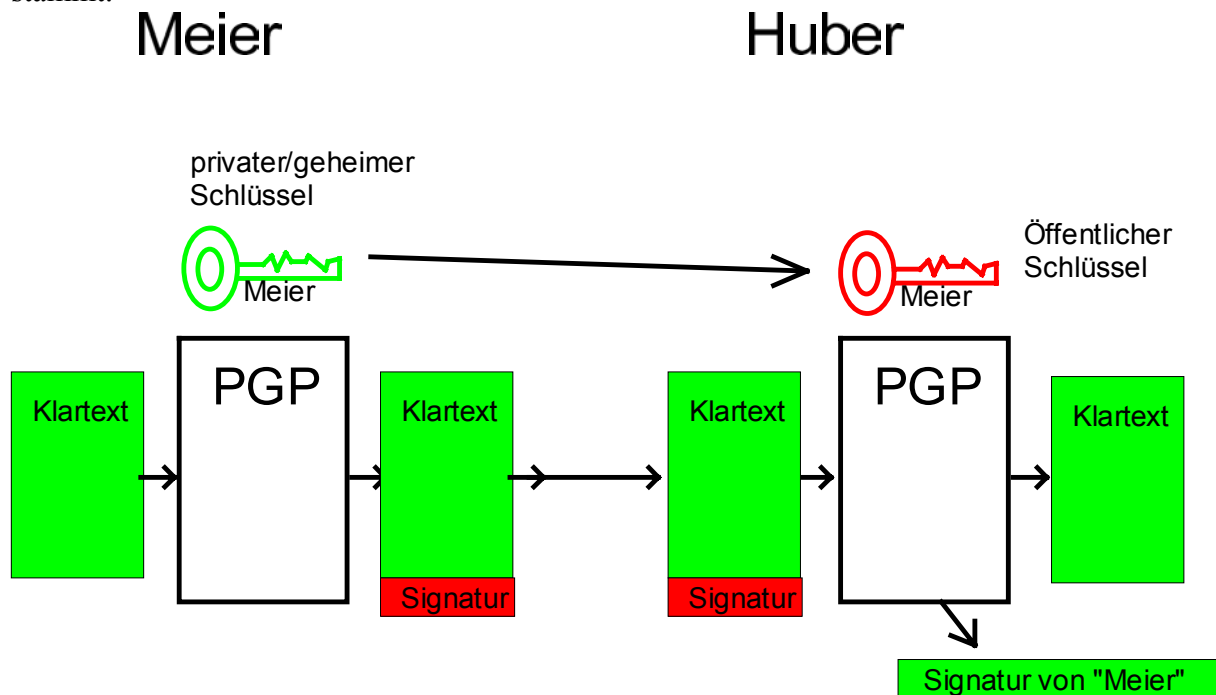
Nur der Empfänger, der seinen geheimen/privaten (**grünen**) Schlüssel hat, kann die Nachricht wieder in Klartext zurückverwandeln.



Das Programm PGP kann nach obigem Muster verwendet werden. Es kann aber auch in ein eMail-Programm integriert werden z. B. Outlook von Microsoft usw. Dann muss man nur einen neuen Knopf in Outlook drücken und schon läuft alles automatisch ab.

Beim **digitalen Signieren** wird folgender Mechanismus verwendet:

Der Unterzeichner (hier Meier) fügt mit PGP an den Klartext ein Stück Code an, welches er mit seinem geheimen (**grünen**) Schlüssel aus dem Text generiert hat. Jeder kann sich den öffentlichen (**roten**) Schlüssel von Meier beschaffen und mit PGP feststellen, dass der Text unverfälscht und eindeutig von Meier stammt.



Beide Verfahren (Verschlüsseln und Signieren) können auch gleichzeitig auf dieselbe Nachricht angewendet werden. Man kann auch eine Nachricht an mehrere Empfänger gleichzeitig senden. Dann muss die Botschaft für jeden Empfänger einzeln mit dessen öffentlichem Schlüssel verschlüsselt werden. (In Outlook ist das trotzdem nur ein Klick.)

Nun besteht nur noch die Gefahr, dass der öffentliche Schlüssel nicht wirklich vom vermuteten Empfänger stammt, sondern gefälscht ist. Aus diesem Grund hat man **Zertifizierungs-Center** geschaffen. Vertrauenswürdige Institutionen verwahren Ihren öffentlichen Schlüssel in einem öffentlich zugänglichen Speicher. Der Schlüssel kann dann von dieser vertrauenswürdigen Stelle abgeholt werden. Damit keine Verfälschung auf dem Weg vorgenommen werden kann, wird der Schlüssel vom **Trust-Center** digital signiert.

Bezugsquelle im Internet: <http://www.pgp.com/products/de/freeware.html>

Bei der Registrierung nur „später“ anklicken. Ansonsten Name und eMail-Adresse möglichst tippfehlerfrei eingeben.

*Diese kurze Übersicht überreicht Ihnen der Computer-Club **Netlife e.V.** von Postbauer-Heng mit seinem Vereinsraum im Bahnhof Postbauer-Heng.*

<http://www.netlife-ph.de>