

Historie der Verschlüsselung

© MyPGP (P17001.02 vom 13.10.2017)

Symmetrische und Asymmetrische Schlüssel

Bis Mitte der 1970er Jahre gab es nur symmetrische Schlüssel. Dabei verwenden der Absender und der Empfänger den selben Schlüssel zum Verschlüsseln und zum Entschlüsseln einer Nachricht. Dieser Schlüssel musste also einmal zwischen Absender und Empfänger ausgetauscht worden sein und zwar so, dass kein Dritter Kenntnis über diesen Schlüssel erlangen konnte. Ein Schlüsselaustausch über das Internet wäre **nicht** sicher, da Dritte den Schlüssel mitlesen könnten.

Asymmetrisches Verschlüsselungsverfahren arbeiten mit zwei unterschiedlichen Schlüsseln, die zusammen ein Schlüsselpaar bilden. Der öffentliche Schlüssel (engl. public key) kann für jeden lesbar (u.a. im Internet) veröffentlicht werden, der private Schlüssel (engl. private key) ist nur dem Schlüsselpaarerzeuger bekannt.

Der Absender verschlüsselt seine Nachricht mit dem öffentlichen Schlüssel des Empfängers und der Empfänger kann diese verschlüsselte Nachricht mit seinem privaten Schlüssel entschlüsseln.

Das heute sehr gebräuchliche RSA-Verfahren zur Erzeugung asymmetrischer Schlüssel wurde von Ronald Rivest, Adi Shamir und Leonard Adleman bereits 1977 erfunden. Die Anfangsbuchstaben der Nachnamen der drei Erfinder gaben dem Verfahren seinen Namen.

Internet, eMails und PGP

Mit der kommerziellen Nutzung des Internets ab 1991/1992 wurde auch die Kommunikation über elektronische Nachrichten (eMails) populär. Die Nachrichten wurden im Klartext im Internet vom Absender zum Empfänger weitergeleitet - jeder Internet-Knotenpunkt konnte die Nachrichten mitlesen.

Um das Mitlesen von Nachrichten zu verhindern, erfand Philip R. (Phil) Zimmermann 1991 das Programm PGP (engl. Pretty Good Privacy). Dabei wird ein (langsamer) asymmetrischer Schlüssel in Kombination mit einem (schnellen) symmetrischen Schlüssel verwendet. PGP-Programme ver- und entschlüsseln nicht nur die Nachrichten, sondern verwalten auch die öffentlichen und privaten Schlüssel.



Philip R. (Phil) Zimmermann

Quelle: Homepage von Philip Zimmermann

<http://www.philzimmermann.com/DE/photos/index.html>
Download vom 5.2.2017

Philip Zimmermann hat dieses Foto für Publikationen freigegeben.

PGP durfte bis Ende der 1990er Jahre ähnlich wie Waffen nicht aus den USA exportiert werden. Um diese Exportbeschränkung zu umgehen, veröffentlichte Phil Zimmermann

1995 den Quellcode in einem Buch. Als Buch konnte PGP legal exportiert werden. Der Quellcode wurde abgetippt und als internationale Version außerhalb der USA verfügbar gemacht.

OpenPGP

1997 wurde die PGP-Spezifikation durch die IETF (International Engineering Task Force) unter dem Namen OpenPGP standardisiert. Die OpenPGP-Spezifikation (aktuelle Version RFC4880, zu finden unter <https://tools.ietf.org/html/rfc4880>) ist kostenfrei für alle nutzbar.

Die [OpenPGP Allianz](#) ist ein Zusammenschluss mehrerer Hersteller, die sich dem OpenPGP-Standard verbunden fühlen. Die Allianz wird aktuell von einem Mitarbeiter der TU Braunschweig betreut.

GnuPG

Eine sehr gebräuchliche Implementierung der OpenPGP-Spezifikation ist die in Deutschland erstellte und gepflegte Software GnuPG (Gnu Privacy Guard, auch abgekürzt mit GPG). GnuPG ist eine Software-Bibliothek, die durch Zeilenkommandos angesprochen wird. Auch Edward Snowden soll dieser Software-Bibliothek vertraut haben.

Viele bekannte eMail-Programme (mit graphischen Oberflächen) benutzen die GnuPG-Software, so z.B. die eMail-Software Thunderbird mit dem Verschlüsselungszusatz Enigmail oder auch die vom Bundesamt für Sicherheit in der Informationstechnik 2006 beauftragte Windows-Version Gpg4win (GNU Privacy Guard for Windows). Informationen zur Wortschöpfung 'GNU' siehe unten.

Was sollten Einsteiger beachten ?

Die Verschlüsselung als solche ist ausgereift und sehr sicher. Geheimdienste werden in der Regel nicht versuchen, die Verschlüsselung zu "knacken", sondern den privaten Schlüssel zu stehlen oder bei der Erzeugung mitzulesen.

Der Schlüsseleigentümer sollte daher **immer selbst** das Schlüsselpaar, bestehend aus dem öffentlichen und privaten Schlüssel, erzeugen. Es sollten Programme verwendet werden, die sich hauptsächlich mit der Schlüsselerzeugung beschäftigen - eine Schlüsselerzeugung über einen Browser ist kritisch zu sehen, da der Browser die gesamte Kontrolle über den Datentransfer besitzt.

Leider ist damit auch die Umsetzung des DE-Mail-Gesetzes des Bundes zu kritisieren, da die Schlüsselerzeugung über den Browser erlaubt ist. Sicherer ist die Schlüsselerzeugung über das eMail-Programm Thunderbird mit dem Zusatz Enigmail oder für Windows Gpg4win.

Der zweite Angriffspunkt ist die Wahl des richtigen öffentlichen Schlüssels des Empfängers. Öffentliche Schlüssel können mit PGP auch problemlos unter fremden Namen im Internet zur Verfügung gestellt werden. Die erstmalige Auswahl des **richtigen** öffentlichen Schlüssels ist von zentraler Bedeutung für die Sicherheit der eMail-Kommunikation. Hier hilft MyPGP, den richtigen öffentlichen Schlüssel zu finden.

Stand der Technik

Die Schlüsselerzeugung und das Ver- und Entschlüsseln von eMails wird heutzutage von komfortablen eMail-Programmen übernommen. Die Verfahren zum Ver- und Entschlüsseln sind schon seit Ende der 1990-er Jahre etabliert. Sie werden immer wieder weiterentwickelt, um neue Erkenntnisse und Erfahrungen zu berücksichtigen.

Zurzeit gibt es keine Hinweise, dass Geheimdienste in der Lage sind, die Verschlüsselung zu knacken. Die Verschlüsselung mit OpenPGP und den darauf aufsetzenden Programmen ist sicher und komfortabel.

GNU ist die Abkürzung für 'GNU is Not Unix' und ist ein rekursives Akronym. Rekursive Akronyme zeichnen sich dadurch aus, dass die Erklärung der Abkürzung die Abkürzung selbst enthält. GNU ist eine Sammlung von Anwendungen und Bibliotheken, die später zu einem freien Unix-ähnlichen Betriebssystem weiterentwickelt werden sollen.

© **paperwork.mypgp.de** // Mit dieser Quellenangabe Freigabe für die nicht-kommerzielle Nutzung.