Florian Reichardt

Florian Reichardt
Seebrucker Str. 46
81825 München

Telefon 0172/945 08 57
Telefax 089/436 17 17

SEMINARARBEIT

im Fach Wirtschaftsinformatik

E-Mail-Verschlüsselung mit Pretty Good Privacy

Leiter des Seminars: Herr Hieber
Schuljahr: 2000/2001

Inhaltsverzeichnis

1. Einleitung

Wer hat nicht einige Dinge, die niemanden etwas angehen. Denken wir nur an das traditionelle Tagebuch. Manch einer hat es zwar abgeschlossen, aber es war dennoch vor neugierigen Blicken nicht hundertprozentig sicher.

Deshalb wird schon seit jeher an sicheren Methoden gebastelt um geheime Dinge zu verstecken oder zu verschlüsseln. Einmal wäre da die Geheimschrift. Dabei gibt es ja viele verschiedene Methoden, wie z. B. das Schreiben mit Zitronensäure oder das Umwandeln des Alphabets in Zahlen bzw. andere Kombinationen. Doch auch hier kann es sein, dass die Geheimschrift irgendjemand „knackt“. Eine andere, vielleicht wohl die sicherste Methode Dinge aufzubewahren, ist der Safe. Hier hat nur der die Chance an die geheimen Daten zu gelangen, der das Passwort weiß oder den passenden Schlüssel hat.

Genau das ist das Prinzip der Kryptologie. Hier geht es auch darum Daten vor Unbefugten zu verschließen.

2. Allgemeines zur Kryptologie

2.1 Was ist Kryptologie?[1]

Unter Kryptologie versteht man die Lehre der Verschlüsselung. Dies bedeutet, dass geheime Daten so umgewandelt werden, dass sie niemand, außer dem Empfänger, lesen kann.

Das Wort Kryptologie stammt aus dem Griechischen. Kryptos bedeutet soviel wie „versteckt, verborgen" oder „unleserlich". Im Fremdwörterduden findet man den Eintrag „Geheimschrift".

In der folgenden Seminararbeit möchte ich mich mit der Verschlüsselung von E-Mails befassen, insbesondere mit dem Verschlüsselungsprogramm Pretty Good Privacy (kurz PGP).

2.2 Geschichte der Kryptologie[2]

Wann die ersten Geheimschriften auftauchten weiß niemand so genau. Allerdings haben schon die alten Spartaner ein Verfahren namens Sky-Tale erfunden. Bei diesem Verfahren wurde ein Zylinder mit einem bestimmten Radius eingesetzt. Um jemanden eine geheime Nachricht übermitteln zu wollen, schrieb man sie auf ein Papier und wickelte es um den Zylinder. Der Empfänger konnte die Mitteilung nur dann entziffern, wenn er einen Zylinder des selben Radius hatte.

Ein weiteres ähnliches wichtiges Verfahren erfand Julius Caesar. Bei seinem Verfahren wurde das Alphabet z. B. um 3 Stellen nach links verschoben. Hier ein Beispiel:

Ursprünglich: 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

Neu: 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

Vor allem viele Jahrhunderte später, im ersten und zweiten Weltkrieg, bekam das Thema Kryptologie immer mehr Bedeutung. Deutschland entwickelte im zweiten Weltkrieg das ENIGMA-Verfahren (Enigmas = griechisch, bedeutet Rätsel). Man verwendete eine Maschine mit mehreren Walzen, die speziell eingestellt werden mussten. Alan Turing, ein Kryptologe aus England erfand 1939 eine Methode dieses Verfahren zu knacken. Die USA nutzten hingegen

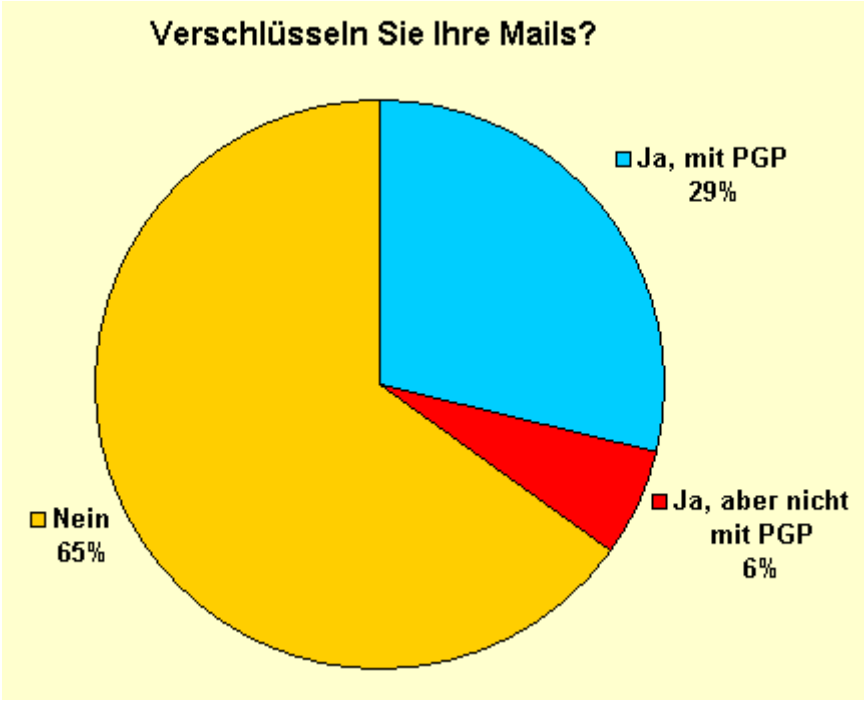
[1] Vgl. Internet: http://www.fu-berlin.de/jura/netlaw/publikationen/beitraege/ws96-buergin.html
[2] Vgl. Internet: http://home.t-online.de/home/poisoner/krypt.htm#Geschichte

die Sprache der Navaho-Indianer um geheime Botschaften auszutauschen, da diese Sprache fast niemand konnte und auch nur schwer zu erlernen war.

Seit dieser Zeit ist die Kryptologie zu einem wichtigen Punkt geworden, denn durch die Unmengen von Daten, die durch das World Wide Web täglich übertragen wurden und werden mussten Verfahren entwickelt werden, damit die geheimen Daten auch geheim bleiben.

2.3 Kryptologie heute[3]

Heutzutage hat die Verschlüsselung von Daten gerade im Internet höchste Priorität. Je mehr Daten durch das World Wide Web geleitet werden, desto mehr Leute können diese Daten abfangen und lesen, im schlimmsten Falle sogar verändern. Gerüchten zur Folge soll die amerikanische Regierung den gesamten E-Mail-Verkehr überwachen und Schlüsselwörter herausfiltern. Allerdings verschlüsseln immer noch viel zu wenige ihre E-Mails. Vor allem haben hier Firmen noch großen Handlungsbedarf, denn hier gilt es ja auch, Firmengeheimnisse oder neuer Strategien vor der Konkurrenz geheim zu halten. Doch eine Umfrage des Computermagazins PC-Welt 06/2000 bei der 250 Leser befragt wurden zeigt, dass es einen steigenden Trend zur E-Mail-Verschlüsselung gibt. Das am häufigsten angewendete Programm ist dabei eindeutig PGP.



[Quelle: PC-Welt 06/2000]

[3] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 233

3. Allgemeines zur E-Mail-Verschlüsselung

3.1 Was ist E-Mail-Verschlüsselung?

Bei der E-Mail-Verschlüsselung geht es darum, die geschriebene Nachricht so zu verschlüsseln, dass sie auf dem Weg zum Empfänger unlesbar ist. Nur der Empfänger kann dann die Nachricht wieder entschlüsseln und somit lesen.

3.2 Warum soll man E-Mails verschlüsseln?[4]

Wenn man einen normalen Brief verschickt, dann geschieht dies meistens in einem Kuvert, damit andere den Brief auf dem Weg zum Empfänger nicht lesen können. Unverschlüsselte Nachrichten kann man mit einer normalen Postkarte vergleichen, die jeder lesen kann. Warum man E-Mails verschlüsseln soll möchte ich im folgenden Abschnitt aufzeigen.

Wenn man eine E-Mail schreibt und dann auf den Button „Senden“ klickt, wird es gefährlich. Denn jede Nachricht wird über unzählige Zwischencomputer, die sogenannten Router, zum Empfänger geleitet. Das Problem ist jedoch, dass niemand genau weiß, welchen Weg die Mail einschlägt und durch welche der unzähligen Computer im WWW sie geleitet wird. Rein theoretisch ist es nun möglich, an jedem dieser Router die Message abzufangen, zu lesen und im schlimmsten Falle sogar zu verändern. Der Empfänger sieht diesen Eingriff allerdings nicht und meint, die Nachricht sei echt.

Bei rein privaten Mails, wo es um den Austausch von Urlaubserlebnissen oder um den abendlichen Kinobesuch geht, ist dies nicht so tragisch. Gefährlich wird es, wenn Firmen ihre Mails unverschlüsselt versenden und wenn es im Inhalt dieser Nachricht um interne Firmengeheimnisse geht oder Firmendaten versendet werden. Hier ist die Firma sogar verpflichtet, die E-Mails zu verschlüsseln, außer der Empfänger hat zugestimmt, die Daten unverschlüsselt zu senden.

Auf der privaten Ebene sollte jeder selbst entscheiden, ob er seine Nachrichten verschlüsselt oder nicht. Schlecht ist es in keinem Fall, denn somit bleibt die Mail wirklich geheim und auch keine amerikanische Regierung (siehe Punkt 2.3) kann die Nachricht lesen. Dank der heutigen Technik ist die E-Mail-Verschlüsselung gar kein Problem mehr, aber dazu später.

[4] Vgl. Internet: http://members.interdesk.ch/pgpkeys/faq/ger_pgpdoc1.html#3.2

3.3 Welche Arten der E-Mail-Verschlüsselung gibt es?[5]

Hier gibt es unzählige Methoden und Programme. In dieser Seminararbeit möchte ich die Verschlüsselung mit dem Programm Pretty Good Privacy aufzeigen. Aber es gibt noch ein paar andere Möglichkeiten, denn die Verschlüsselung mit PGP ist in manchen Situationen zu umständlich.

So kann man die E-Mails nur an dem heimischen Computer, an dem das Programm installiert ist, verschlüsseln. Ist man häufig unterwegs oder schreibt man oft Messages von einem anderen PC aus ist Pretty Good Privacy nicht geeignet. Das zweite Problem das sich stellt, ist, dass man verschlüsselte E-Mails nur an Empfänger versenden kann, die das Programm ebenfalls einsetzten. Deshalb gibt es auch einige Alternativen zu PGP, wobei Anzumerken ist, dass Pretty Good Privacy am weitesten Verbreitet und in Gebrauch ist.

Wenn man viel unterwegs ist, empfiehlt sich z. B. ein E-Mail-Account bei Web.de (zu finden im Internet unter http://freemail.web.de). Hier kann man sich kostenlos registrieren lassen und bekommt eine sogenannte Freemail-Adresse. Bei diesem Account gibt es kostenlos eine Verschlüsselungsfunktion, bei der man Mails ebenfalls verschlüsseln kann. Hier gibt es allerdings auch wieder Einschränkungen, denn man kann die E-Mails nur an Empfänger senden, die ebenfalls einen Free-Mail-Account bei Web.de haben oder ein anderes Mailprogramm einsetzten, das die sogenannte S/Mime-Funktion (näheres siehe übernächsten Abschnitt) unterstützt, wie z. B. Outlook Express oder der Netscape Navigator. Mittlerweile gibt es noch weitere E-Mail-Anbieter im Internet, die ebenfalls eine Verschlüsselungsfunktion anbieten.

Eine andere Alternative wäre WinZip. Das ist ein Komprimierungsprogramm, bei dem man Dateien in ein Archiv speichern und mit einem Kennwort hinterlegen kann. Die sogenannte .zip-Datei hängt man dann an das Mail an und der Empfänger kann es mittels dem richtigen Kennwort öffnen. Allerdings ist das hier mit der Sicherheit des Kennwortes so eine Sache, denn es gibt Programme, die die Kennwortfunktionen bei so einem Archiv umgehen bzw. hacken können.

[5] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 238

Letzte Alternative wäre das schon angesprochene S/Mime. Dies Funktion ist in den beiden bekanntesten Browsern, also Microsoft Internet Explorer und Netscape Navigator, integriert. S/Mime wurde ursprünglich von der Firma RSA Data Security Inc. entwickelt. Der Vorteil bei dieser Verschlüsselungsart ist, dass kein extra Programm installiert werden muss. Allerdings muss für den Einsatz von S/Mime ein Zertifikat bei einer Zertifikatsstelle beantragt werden, welcher je nach Klasse kostenpflichtig sein kann.

4. E-Mail-Verschlüsselung mit Pretty Good Privacy

4.1 Was ist Pretty Good Privacy?[6]

Pretty Good Privacy ist ein Programm, mit dem man E-Mails sicher verschlüsseln kann. Das Programm ist für den privaten Gebrauch Freeware, d. h. man kann es sich kostenlos aus dem Netz laden und kostenlos verwenden. Es gilt als das sicherste Verschlüsselungsprogramm, da es weltweit noch nie geknackt wurde. Es ist einfach zu bedienen und man kann es z. B. schnell in das E-Mail-Programm Outlook Express von Microsoft integrieren.

Pretty Good Privacy lässt sich mit den Worten „sehr gute Privatsphäre“ ins Deutsche übersetzten.[7] Es wurde 1990 von Philip Zimmermann[8] entwickelt. Seit dieser Zeit wurde es immer wieder verbessert und den aktuellen Betriebssystemen, wie Windows95, 98 und NT/2000 angepasst. PGP lässt sich auf folgender Seite downloaden:

www.pgpi.org

Die Version, auf der die vorliegende Seminararbeit aufbaut , ist die Version PGP 6.5.1i. Bei anderen Versionen kann es zu einigen Abweichungen z. B. bei der Installation kommen. Es gibt auch eine kommerzielle Version der Software, die derzeit allerdings DM 79,-- kostet.[9]

Ein zusätzliches Highlight in dem Programm PGP ist die sogenannte digitale Signatur. Das bedeutet, man kann Mails so kennzeichnen, dass der Empfänger die Sicherheit hat, die Nachricht stammt wirklich vom Autor und wurde auf dem Weg nicht verändert. Das wäre aber ein eigenes Thema. Deshalb möchte ich mich im Folgenden nur mit der Verschlüsselung von E-Mails mittels des Programms PGP befassen.

4.2 Wie installiere ich Pretty Good Privacy?[10]

Die Installation von PGP ist etwas aufwendiger, weil bei der Installation das Schlüsselpaar mit öffentlichen und privaten Schlüssel generiert werden. Deshalb hier eine kleine Anleitung.

Nachdem man den Lizenzvertrag akzeptiert hat, kann man die Komponenten auswählen, die man installieren möchte. Die Option „PGPnet“ kann man

[6] Vgl. Internet: http://members.interdesk.ch/pgpkeys/faq/ger_pgpdoc1.html#3.1
[7] Vgl. Internet: http://bi-node.teuto.de/pgp/html/node6.html#SECTION02230000000000000000
[8] Informationen zu P. Zimmermann: siehe Glossar
[9] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 232
[10] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 233ff

normalerweise deaktivieren, da sie für Außendienstmitarbeiter geeignet ist, die eine verschlüsselte Verbindung zu ihrem Intranet aufbauen wollen. Des weiteren bietet PGP sogenannte PlugIns. Es stehen PlugIns für die E-Mail-Programme Eudora und Microsoft Exchange/Outlook zur Verfügung. Wenn man mit einem der genannten Mailprogramme arbeitet, sollte man das jeweilige PlugIn mitinstallieren, da es die Arbeit beim ver- bzw. entschlüsseln erheblich erleichtert.

Nachdem alle Dateien auf die Festplatte kopiert wurden, wird man vom Programm gefragt, ob man schon bestehende Schlüssel hat oder neue anlegen möchte. Beim ersten Gebrauch von PGP wählt man „Nein“, um einen neuen Schlüssel zu erstellen. Danach muss der Rechner neu gestartet werden. Ab sofort wird automatisch bei jedem Start das Tool PGP-Tray neben der Uhr in der Task-Leiste geladen.

Um einen neuen Schlüssel anzulegen klickt man auf dieses neue Symbol und wählt PGP-Keys aus. Es wird ein Schlüsselerzeugungsassistent geladen. Mit Hilfe dieses Assistenten erzeugt man die neuen Schlüssel. Wenn man auf „Weiter“ klickt wird man aufgefordert Namen und E-Mail-Adresse einzugeben. In der nächsten Dialogbox kann man zwischen dem „RSA“- und dem „Diffie-Hellman/DSS“-Typ wählen. Da das erstgenannte Verfahren veraltet ist, belässt man die Einstellung so wie sie ist. Anschließend muss man die Länge der Schlüssel festlegen. Auch hier kann man die Voreinstellung von 2048Bit lassen, da diese Länge als sehr sicher gilt. Mit den heutigen technischen Möglichkeiten würde es Jahrzehnte dauern, bis ein Schlüssel dieser Länge geknackt wäre. Längere Schlüssel erhöhen zwar die Sicherheit, verlängern aber auch die Arbeitszeit von PGP, um eine Mail zu verschlüsseln. Die nächste Einstellung belässt man ebenfalls wie sie ist, da es nicht nötig ist, das neue Schlüsselpaar zeitlich zu begrenzen.

Jetzt wird es ernst, denn nun muss man ein Passwort eingeben. Mit Hilfe dieses Passwortes ist der privater Schlüssel vor Unbefugten sicher. Hier gilt die eiserne Regel. Je länger das Passwort und je unterschiedlicher die Zeichen, desto besser. Deshalb erlaubt PGP auch einen ganzen Satz als Kennwort festzulegen. Darum wird das Feld nicht Passwort, sonder Passphrase genannt. Das absolute Minimum eines Kennwortes sollten acht Zeichen sein. Es ist auch, wie eben angesprochen, ratsam Sonderzeichen und Zahlen einzubauen und das Passwort nicht nur in Klein- oder Großbuchstaben einzugeben sondern gemischt, da das die Sicherheit nochmals erhöht. Allerdings sollte es ein Passwort sein, das man sich auch gut merken kann, denn wenn man eine Nachricht entschlüsseln will, hilft einem nur der private Schlüssel mit passendem

Kennwort. Die Passphrasequalität zeigt an, wie sicher das gewählte Passwort ist. Ja länger also, desto besser. Durch die Bestätigung des Kennwortes werden eventuelle Tippfehler ausgeschlossen. Danach wird mittels eines komplizierten mathematischem Verfahrens das Schlüsselpaar erzeugt.

Vom Programm wird man dann gefragt, ob man den öffentlichen Schlüssel auf einem sogenannten Key-Server hinterlegen will. Dies hat den Vorteil, dass man mit Kommunikationspartnern nicht direkt Kontakt aufnehmen muss, um an den öffentlichen Schlüssel zu gelangen, sondern man holt ihn sich von diesem Server. Ein Nachteil ist allerdings, dass man nun nicht mehr bestimmen kann von wem man verschlüsselte Nachrichten bekommt, da der öffentlicher Key ja frei verfügbar ist. Wenn man das Hinterlegen des öffentlichen Schlüssels nicht will, so muss man dem Kommunikationspartner eine Mail mit dem Schlüssel als Anhang senden, doch hat man hier die Kontrolle, wer den Schlüssel bekommen soll und wer nicht. Ein weiterer Klick auf „Fertigstellen“ und das neue Schlüsselpaar ist angelegt.

Der Assistent wird automatisch beendet und man sieht am Bildschirm das Programm „PGPKeys“. Hier ist unter anderem auch der eben angelegte Schlüssel dabei. Die anderen Schlüssel kann man normalerweise löschen, um die Übersicht zu behalten. Sie dienen nur als Beispiele.

Es wäre ratsam, wenn man eine Sicherungskopie des Schlüsselpaars anlegen würde, denn durch einen unerwarteten Plattencrash kann es sein, dass die Schlüssel weg sind und man keine einzige Nachricht mehr entschlüsseln kann.

Die Software wäre nun eigentlich fertig und einsatzbereit, doch eine kleine Einstellung ist noch vorzunehmen. Ausgehende Mails, d. h. wenn man eine Mail versenden will, werden von PGP automatisch mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, was zur Folge hat, dass man die Mails im Ausgangsordner nicht mehr lesen kann. Um aber auch nach dem Verschlüsseln der Mail die Nachricht lesen zu können, ruft man über das Symbol in der Taskleiste die „Optionen“ auf. In der Registerkarte „Allgemein“ aktiviert man den Punkt „Immer mit Standardschlüssel verschlüsseln“. Somit kann man die Kopien in dem Ausgangsordner des Mailprogramms jederzeit lesen.

4.3 Wie funktioniert Pretty Good Privacy im Detail?[11]

Pretty Good Privacy arbeitet nach dem sogenannten „Public-Key-Verfahren“. Dieses Verfahren ist im Grunde recht einfach. Bei der Installation wird ein

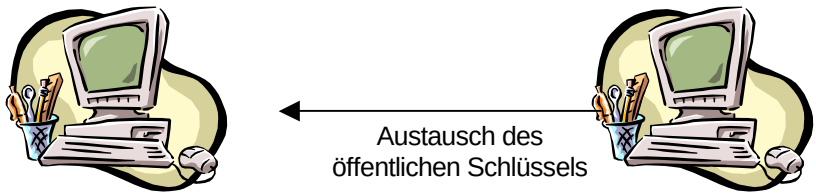
[11] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 234ff, Kasten

Schlüsselpaar angelegt. Dieses Paar besteht aus dem „öffentlichen Schlüssel“ und dem „privaten Schlüssel“.

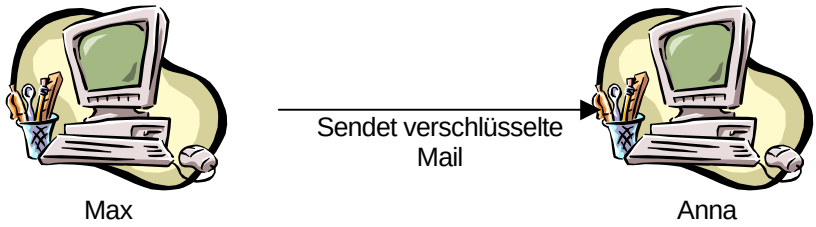
Mit Hilfe des öffentlichen Schlüssels kann man nur E-Mails verschlüsseln. Diesen Schlüssel muss man also allen Personen geben, von denen man Mails bekommen möchte.

Den privaten Schlüssel sollte man geheim und sorgfältig aufbewahren. Denn mittels diesem Schlüssel kann man die verschlüsselte Nachricht wieder entschlüsseln und somit lesbar machen.

Dieses Verfahren gilt als relativ sicher, da man nur Mails entschlüsseln kann, wenn beide Schlüssel zusammen passen. Des weiteren kann man nicht vom öffentlichen Schlüssel, der ja per Mailanhang verschickt wird, auf den privaten Schlüssel schließen. Ich möchte die Funktionsweise von PGP anhand eines Beispiels verdeutlichen:



Bevor Max an Anna eine E-Mail schicken kann, benötigt er den öffentlichen Schlüssel von Anna. Den bekommt er entweder von Anna direkt als E-Mailanhang oder Max holt sich den öffentlichen Schlüssel vom Key-Server ab. Voraussatzung ist hierbei allerdings, dass Anna ihren öffentlichen Schlüssel auch auf dem Key-Server hinterlegt hat.



Mittels des öffentlichen Schlüssels von Anna kann Max seine Nachricht verschlüsseln und an Anna senden. Anna kann dann die Mail mit ihrem privaten Schlüssel entschlüsseln und lesen.

Der Vorteil von PGP ist, dass das Programm nach dem sogenannten asymmetrischen Verschlüsselungsverfahren arbeitet. Dies hat einen entscheidenden Vorteil im Gegensatz zu dem symmetrischen Verschlüsselungsverfahren, was ich im folgenden Abschnitt verdeutlichen möchte.

Ich möchte erst die Funktionsweise des symmetrischen Verfahrens erklären. Hierbei benutzen Sender und Empfänger den gleichen Schlüssel. D. h. also: zum Verschlüsseln einer E-Mail wird derselbe Schlüssel benutzt wie zum entschlüsseln. Der Sender einer Mail muss also dafür sorgen, dass die Mail und der Schlüssel zum entschlüsseln zum Empfänger gelangen. Doch wie soll nun der Schlüssel zum Empfänger gelangen, denn es muss ja ein sicherer Weg sein, damit Unbefugte nicht an den Schlüssel kommen können. Eine Möglichkeit wäre per Telefon, aber auch hier gibt es ja bekanntlich keine hundertprozentige Sicherheit. Abgesehen davon: Warum sollte man eine Nachricht verschlüsseln wenn es eine hundertprozentig sichere Verbindung zum Empfänger gibt? Aber wie soll dann der Schlüssel zum Empfänger gelangen?

Genau hier setzt das asymmetrische Verschlüsselungsverfahren, auch Public-Key-Verfahren genannt an. Hierbei gibt es zwei Schlüssel, die ganz unabhängig voneinander sind. Mit dem öffentlichen Schlüssel kann man nur E-Mails verschlüsseln. Ist eine Message verschlüsselt, kann sie nicht einmal der Versender wieder entschlüsseln. Dies geht nur mittels des privaten Schlüssels, den der Empfänger hat. Somit bleibt das gegenseitige tauschen der Schlüssel überflüssig und ist somit am sichersten. Philip Zimmermann, der Erfinder von PGP ging damals davon aus, dass es keine sichere Methode gibt, Schlüssel auszutauschen. Deshalb entwickelte er das Public-Key-Verfahren, wo der Austausch wegfällt.

Das bekannteste Verfahren im Bereich der asymmetrischen Verschlüsselung ist das RSA-Verfahren. Es wurde 1977 von den Kryptologen Rivest, Shamir und Adleman entwickelt. Ich möchte kurz auf dieses Verfahren eingehen, denn eine detaillierte Erklärung wäre zu kompliziert.

Grundsätzlich basiert das Verfahren darauf, zwei große Primzahlen miteinander zu multiplizieren. Danach werden durch ein kompliziertes mathematisches Verfahren Zahlen errechnet, die mit dem Produkt der beiden Primzahlen verwandt sind. Aus einer dieser beiden verwandten Zahlen und aus dem

Produkt der Primzahlen wird dann der öffentliche Schlüssel erstellt. Die andere verwandte Zahl ergibt den Geheimschlüssel.[12]

Um eine Nachricht zu entschlüsseln ohne den privaten Schlüssel zu kennen, müsste man das Produkt der beiden Primzahlen kennen und dieses in die beiden einzelnen Faktoren zerlegen. Die klingt zwar recht einfach, ist aber mit den heutigen mathematischen Prozessen sehr schwierig. Aus diesem Grund ist die Sicherheit bei diesem Verfahren extrem hoch.

4.4 Wie ver- bzw. entschlüsselt man Nachrichten?[13]

Falls man bei der Erzeugung der Schlüssel das Ablegen über den Key-Server gewählt hat, muss der jeweilige Kommunikationspartner nur das Programm „PGPKeys“ starten und den Befehl „Server, Suchen“ wählen. Dann tippt er den Namen ein und erhält den dazugehörigen Schlüssel angezeigt, den er mit einem Klick auf die rechte Maustaste und der Option „In lokalen Schlüsselbund importieren“ hinterlegen kann.

Wenn man den Schlüssel nicht auf dem Server hinterlegt hat, muss man dem E-Mail-Partner diesen zukommen lassen. Dazu wählt man ebenfalls im Programm „PGPKeys“ den Punkt „Exportieren“ und legt dann ein Verzeichnis fest, wo der Schlüssel gespeichert werden soll. Zu beachten ist, dass der Befehlt „Privaten Schlüssel einbeziehen“ nicht aktiviert ist, da sonst auch der private Schlüssel mit verschickt wird. Dann sendet man den Schlüssel, der übrigens die Endung .ASC trägt, als Anhang an den Kommunikationspartner. Der Empfänger muss dann den Schlüssel wieder importieren, indem er die Schlüsseldatei doppelt anklickt.

Wenn man eine E-Mail mit dem Microsoftprogramm Outlook verschlüsseln möchte ist dies ganz einfach, da es von PGP das besagte PlugIn gibt. Wurde dies bei der Installation mitinstalliert, so ist die Verschlüsselung von Nachrichten kein Problem mehr. Vorraussetzung für Funktion des PlugIns ist allerdings, dass das Tool „PGP Tray“ im Hintergrund läuft, also das Schloss-Symbol neben der Uhr angezeigt wird. Man öffnet das Programm Outlook und schreibt ganz normal eine Nachricht. Dann trägt man die E-Mail-Adresse des Empfängers ein und klickt das Symbol „Verschlüsseln (PGP)“ an. Das war’s schon. PGP verschlüsselt automatisch die Nachricht mit dem öffentlichen Schlüssel des Empfängers und sendet sie ab. Wichtig zu bemerken ist allerdings, dass PGP die Betreffzeile nicht mit verschlüsselt. Somit ist es wichtig, dass in der sogenannten „Subject-Zeile“ kein selbst erklärender Text steht, wie z. B. „Kündigung“.

[12] Vgl. Internet: http://home.t-online.de/home/poisoner/krypt.htm#Asymmetrisch
[13] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 240ff

Die Kopie des Mails liegt wie gewöhnlich im Ordner „Gesendete Objekte“. Allerdings ist diese Nachricht dort verschlüsselt. Man kann sie nur lesen, wenn man bei der Schlüsselerstellung den Punkt „Alle Nachrichten auch mit eigenem öffentlichen Schlüssel verschlüsseln“ gewählt hat (Vgl. Punkt 3.2).

Das entschlüsseln einer Nachricht funktioniert ähnlich. Klickt man die gewünschte Mail doppelt an, und wählt man dann das Symbol „PGP-Nachricht entschlüsseln“ so erscheint ein Fenster, wo man die Passphrase, also Passwort/Satz, eingeben muss. Ein weiterer Klick und die E-Mail erscheint im Klartext.

Aber auch, wenn man das Programm Outlook nicht hat, ist das ver- bzw. entschlüsseln von Nachrichten mittels PGP sehr einfach. Es funktioniert mit jedem beliebigem E-Mail-Programm.

Zuerst wird die Nachricht wie gewohnt in einem neuen Mailfenster geschrieben. Wenn alles OK ist, klickt man auf das sich in der Taskleiste befindende PGP-Tray-Symbol. Dort wählt man den Punkt „Aktuelles Fenster verschlüsseln“ aus. Ein Nachteil ist, dass das Programm ohne Outlook die E-Mail-Adresse nicht erkennt. Statt dessen öffnet sich ein weiteres Fenster, wo alle verfügbaren öffentlichen Schlüssel zu finden sind. Nun muss man nur noch den jeweiligen öffentlichen Schlüssel doppelt anklicken und PGP verschlüsselt die Nachricht. Beim nächsten Klick auf „Senden“ wird die verschlüsselte Nachricht an den Empfänger versendet.

Beim Entschlüsseln von Nachrichten verfährt man genauso. Man öffnet die jeweilige Mail, klickt dann auf das PGP-Tary-Symbol und wählt den Punkt „Aktuelles Fenster entschlüsseln/verfizieren“. Im nächsten Fenster muss nur noch die Passphrase/das Passwort eingegeben werden um die Nachricht lesen zu können.

4.5 Wie sicher ist das Programm?

Wie schon erwähnt, gilt das Programm bisher als das sicherste, E-Mails zu verschlüsseln. Dies wird, wie im vorherigen Punkt ausführlich beschrieben, durch den Einsatz des asymmetrischen Verfahrens und der beiden Schlüssel Public-Key und Personal-Key möglich.

Fälschungen der Schlüssel sind so gut wie ausgeschlossen, allerdings kann man auch bei PGP von keiner hundertprozentigen Sicherheit reden, denn das typische Restrisiko wird wohl immer bleiben. So kann es durchaus sein, dass durch Viren und Trojaner der private Schlüssel in die Hände Unbefugter gelangt.

[14] Ein weiterer wichtiger Punkt, den man allerdings leicht vermeiden kann, ist, dass man die Daten auf jedem alten Computer vollständig löschen sollte. Denn gerade wenn der Computer auf dem Sperrmüll liegt, können sensible Daten in die Hände von Anderen kommen.[15] Dennoch sollte man das Programm auf jeden Fall einsetzten, denn auch eine nicht mit zig Schlössern verschlossene Tür ist zu.

Um noch mehr Sicherheit zu bekommen wäre es ratsam den öffentlichen Schlüssel nicht auf dem Key-Server zu hinterlegen, sondern jedem Kommunikationspartner extra per Mail-Anhang zu senden. Somit kann man wenigstens etwas überwachen, wer den Schlüssel bekommt und wer nicht.[16]

4.6 Wie sicher ist die E-Mail-Verschlüsselung allgemein?[17]

Die alternativen zu PGP sind zwar nicht schlecht und für den privaten Gebrauch durchaus empfehlenswert, vor allem bevor man gar nicht verschlüsselt, aber an die Sicherheit und die Fähigkeiten von PGP reicht keine der alternativen Programme hin.

Die absolute Sicherheit wird es wohl im World Wide Web nie geben, denn es gibt immer Leute, die alles daran setzten um an geheime Informationen zu gelangen, was im alltäglichen Leben auch nicht anders ist. Doch sollte man diesen Leuten auf jeden Fall so viele Steine wie nur möglich in den Weg legen.

[14] Vgl. Internet: http://bi-node.teuto.de/pgp/html/node9.html#Viren
[15] Vgl. Internet: http://bi-node.teuto.de/pgp/html/node9.html#Dateispuren
[16] Vgl. Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 237
[17] Vgl. Internet: http://bi-node.teuto.de/pgp/html/node9.html

5. Abschließende Bemerkung

Grundsätzlich sollte man den Gedanken Sicherheit im World Wide Web nicht irgendwo vergraben. Vor allem dann, wenn man viele E-Mails versendet. Denn die zahlreichen Hackerangriffe in den letzten Monaten zeigen, dass es immer wieder Leute gibt, die an geheime Daten hinkommen wollen und sei es auch nur zu deren Spaß um die Gegenseite schädigen zu können.

Durch das Programm von Philip Zimmermann ist es so einfach geworden, Mails zu verschlüsseln und somit vor neugierigen Blicken verschont zu bleiben. Deshalb sollte man auch im privaten Bereich die Nachrichten verschlüsseln, denn auch ein Liebesbrief an die Geliebte könnte von anderen gelesen und eben auch verändert werden, was fatale Folgen nach sich ziehen könnte.

Glossar

E-Mail

deutsch: elektronische Post = eine Nachricht, die elektronisch z. B. über einen Computer zu einem anderen Computer gelangt.

World Wide Web (WWW)

Das World Wide Web, auch Internet genannt, ist das weltweit größte Datennetz. Es verbindet Computer aus aller Welt miteinander.

Kryptologie

deutsch: versteckt, verborgen, unleserlich = Lehre der Verschlüsselung

Router

Zwischencomputer im Internet, durch die z. B. die Anfrage einer Internetseite geleitet wird.

Browser

Programm, mit dem man Internetseiten abfragen und darstellen lassen kann.

E-Mail-Account

Darunter versteht man einen elektronischen Briefkasten, wo man eine sog. E-Mail-Adresse zugeteilt bekommt. Der Briefkasten enthält die Ordner „Nachrichteneingang“ und „Nachrichtenausgang“.

E-Mail-Adresse

Eine E-Mail-Adresse ist eine weltweit einmalige Adresse, an die man elektronische Nachrichten (E-Mails) senden kann, vergleichbar mit einer normalen Hausadresse.

WinZip

WinZip ist ein weitverbreitetes Programm um Daten zu komprimieren, also aus einer oder mehreren großen Datei eine kleinere zu machen.

Zip-Datei

Eine mit *WinZip* erstellte komprimierte Datei.

Microsoft Internet Explorer

Bekannter *Browser*

Microsoft Outlook /Outlook Express

Eines der bekanntesten und verbreitetsten Programme um *E-Mails* versenden zu können.

Netscape Navigator/Messager

Bekannter *Browser* mit integriertem Programm zum Versenden von *E-Mails*.

Download

Darunter versteht man das herunterladen einer Datei oder eines Programms aus dem *Internet*.

Tool

Ein kleines Programm, das meist ein Zusatz zu anderen Programmen ist.

PlugIn

Ein kleines Programm, das sich in den *Internet Browser* integriert um z. B. Klang und Video-Dateien anhören und ansehen zu können oder um bestimmte Funktionen in den *Browser* zu integrieren (*PlugIn* für *Outlook* um *E-Mails* schneller und einfacher verschlüsseln zu können).

Philip Zimmermann

Philip Zimmermann ist der Erfinder von Pretty Good Privacy. Er arbeitet als Sicherheitsexperte in Boulder, Colorado.

Literaturverzeichnis

- Internetseite zur Kryptologie,
  Vgl. Internet: http://home.t online.de/home/poisoner/krypt.htm

- Magazin PC-Welt, Ausgabe 06/2000, Titel „Geheime Mails“, Seite 232ff

- Kryptographie, Projektgruppenarbeit von Markus Bürgin, Wintersemester 1996/97
  Vgl. Internet: http://www.fu-berlin.de/jura/netlaw/publikationen/beitraege/ws96-buergin.html

- PGP Dokumentation
  Vgl. Internet: http://members.interdesk.ch/pgpkeys/faq/ger_pgpdoc1.html

- Pretty Good Privacy - Das Verschlüsselungsprogramm für Ihre private elektronische Post von Christopher Creutzig, Andreas Buhl und Philip Zimmermann, 4. Auflage, Verlag ART D'AMEUBLEMENT, Bielefeld, ISBN 3-9802182-9-5
  Buch auch im Internet verfügbar:
  Vgl. Internet: http://bi-node.teuto.de/pgp/html/pgp.html

Erklärung

Hiermit erkläre ich, dass ich die Arbeit selbstständig verfasst habe und noch nicht anderweitig für Prüfungszwecke vorgelegt habe. Des weiteren habe ich keine anderen, als die angegeben Quellen oder Hilfsmittel verwendet.

_____ _____

Ort, Datum Unterschrift