1 Worum geht es?

In diesem Dokument geht um ein **Verfahren** zum **Schutz** von **binären Daten** vor

- **unerlaubtem Lesen** (Spionage) -> *data security*
- **unerlaubtem Modifizieren** (Sabotage) -> *data integrity*

während der

- **Speicherung** (z.B. auf Festplatten, CDROMs, ...) und
- **Übertragung**. (z.B. via E-Mail, ftp, ...)

durch Einsatz eines

- durch Verzicht auf eine graphische Oberfläche sehr kleinen (ehemals unter 200 kB, mittlerweile ca. 600 kB Größe des gesamten Programms)
- relativ einfach zu benutzenden
- leistungsfähigen
- für sehr viele Betriebssysteme (UNIX-Flavours, MacOS, OS/2, OS390, DEC VMS, MS Windows, DOS, AmigaOS, Atari TOS, ...) verfügbaren, prinzipiell plattform-unabhängigen
- kostenlosen (gilt uneingeschränkt nur für GnuPG)

Software-Tools:

PGP = *Pretty Good™ Privacy* (bzw. GnuPG)

2 Einige Grundbegriffe der Kryptologie

Klartext (*plain text*):
unverschlüsselte Nachricht (braucht nicht unbedingt lesbarer Text zu sein)
Geheimtext (*cypher text*):
verschlüsselte Nachricht
Ver-/Entschlüsselungs-Algorithmus:
Vorschrift zum Umwandeln von Klartext in Geheimtext und umgekehrt.
Grundlage aller kryptographischen Algorithmen sind mathematische Operationen, deren Umkehrung extrem aufwendig ist.
Beispiel: Multiplikation von 2 je ca. 500-stelligen Primzahlen einerseits und Primfaktor-zerlegung der entstandenen ca. 1000-stelligen natürlichen Zahl andererseits.
Kryptographiesysteme, deren Sicherheit auf der Geheimhaltung des zugrunde liegenden Algorithmus beruhen, sind als unsicher einzustufen.
Schlüssel (*key*):
Parameter, der die Ver-/Entschlüsselung steuert
Vertraulichkeit (*privacy*):
Schutz vertraulicher Nachrichten vor unbefugter Kenntnisnahme
Authentizität (*authenticity*):
Sicherstellung, dass eine Nachricht in der vorliegendem Form tatsächlich von dem angegebenen Absender stammt
Symmetrische Verfahren:
Für Ver- und Entschlüsselung wird der selbe Schlüssel eingesetzt.
Vorteile: einfach zu implementieren, schnell, sehr sicher schon bei kurzen Schlüsseln.
Nachteil: Sichere Übertragung des Schlüssels notwendig.
Beispiele: ROT13 („Caesar Chiffre“, 2000 Jahre alt), XOR (bitweises XOR des Klartextes mit dem Schlüssel), DES (Data Encryption Standard, verwendet eine Schlüssellänge von 53 bit und gilt daher inzwischen als unsicher), TripleDES (wie DES, jedoch mit drei-

facher Schlüssellänge), Blowfish (entwickelt von Bruce Schneier), AES, IDEA (International Data Encryption Algorithm, entwickelt 1990 von X. Lai und J. Massey), CAST (entwickelt von C. Adams und S. Tavares)

Asymmetrische Verfahren (*Public Key*-Verfahren):
Für Ver- und Entschlüsselung werden unterschiedliche Schlüssel eingesetzt (einer zum Verschlüsseln, einer zum Entschlüsseln). Dieses Konzept wurde 1976 von W. Diffie und M. Hellman vorgeschlagen.
Nachteile: aufwendig zu implementieren, langsam, Schlüsselverwaltung erforderlich.
Vorteil: keine sichere Übertragung des Schlüssels erforderlich.
Beispiele: RSA (entwickelt 1977 von R. Rivest, A. Shamir und L. Adelman), DSA (Digital Signature Algorithm, vom US-amerikanischen National Institute of Standards and Technology NIST entwickelt), ElGamal (entwickelt von T. ElGamal)

Digitale Signatur:
Besteht aus einer Prüfsumme („*hash*“) der zu signierenden Nachricht, einer Identifikation des Signierenden sowie dem Datum der Signatur. Dieser Datensatz wird so verschlüsselt, dass er nur vom rechtmäßigen Empfänger der signierten Nachricht entschlüsselt werden kann. Stimmt die beim Empfänger berechnete Prüfsumme der übermittelten Nachricht mit der in der Signatur übermittelten Prüfsumme überein, so ist die Nachricht authentisch.

3 Wie funktioniert *public key* Kryptographie prinzipiell?

Bei *public key*-Verfahren besitzt jeder Teilnehmer an der verschlüsselten Kommunikation ein **Schlüsselpaar**: einen unbedingt geheim zu haltenden **privaten Schlüssel** (*private key*) und einen zur Weitergabe bestimmten **öffentlichen Schlüssel** (*public key*).

Kommunikationspartner tauschen (einmalig) vor dem ersten verschlüsselten Austausch von Nachrichten ihre **öffentlichen** Schlüssel aus. Dieser Austausch darf von potentiellen Angreifern abgehört werden. Es muss aber unbedingt sicher gestellt werden, dass die Schlüssel **unverfälscht** ankommen, also **authentisch** sind! Hierzu werden die von Absender und Empfänger erzeugten kurzen, lesbaren „**Fingerabdrücke**“ (Signaturen, *finger prints*) der öffentlichen Schlüssel verglichen. Der Vergleich muss über einen vertrauenswürdigen – aber nicht notwendigerweise abhörsicheren – Kanal erfolgen.

Dann verschlüsselt der Absender die Nachricht mit dem öffentlichen Schlüssel des Empfängers und signiert sie mit seinem geheimen Schlüssel (digitale Unterschrift). Der Empfänger der Nachricht entschlüsselt sie mit seinem privaten Schlüssel und prüft ihre Authentizität mit dem öffentlichen Schlüssel des Absenders.

4 Was ist PGP?

PGP ist ein *public key*-Kryptographieprogramm zum **Ver- und Entschlüsseln** sowie **digitalen Signieren** von beliebigen **Dateien** einschliesslich der damit zusammenhängenden **Schlüsselverwaltung** (*key management*). Dabei werden verschiedene **anerkannt starke Verschlüsselungsalgorithmen** (*strong encryption*) geschickt kombiniert, um hohe Sicherheit bei einfacher Benutzung und kurzen Ausführungszeiten zu erreichen. Dadurch, dass der C **Quellcode** der meisten Versionen von PGP **veröffentlicht** wurde, konnte er von den besten Kryptologen der Welt auf Schwachstellen untersucht werden (*peer review*). Daten, die mit einer derjenigen Freeware-Versionen von PGP verschlüsselt werden, **deren Quellcode öffentlich zugänglich ist**, gelten – richtige Anwendung von PGP vorausgesetzt – als mit den heutigen technischen Mitteln durch Unbefugte nicht les- oder manipulierbar.

Aufbauend auf der Kernfunktionalität von PGP wurde eine Vielzahl von – meist kommerziellen – Produkten entwickelt, die eine komfortable Verschlüsselung von E-Mails, kompletten Festplatteninhalten oder der gesamten Datenkommunikation in firmeninternen Netzen (*Virtual Private Networks*) ermöglichen.

5 Woher kommt PGP?

PGP Version 1.0 wurde am 5. Juni 1991 in den USA von dem Bürgerrechtler **Philip („Phil") R. Zimmermann** („PRZ") /14/ als ***public domain*-Software** veröffentlicht. Zimmermann implementierte in PGP den RSA-Algorithmus, der von Firma RSA Security, Inc. durch ein US-Patent geschützt war. Dieses Problemen wurde später dadurch gelöst, dass der entsprechende Code durch die von RSA Security, Inc. frei verfügbare RSAREF-Bibliothek ersetzt wurde. Zimmermann wollte mit PGP ein Zeichen gegen die seitens der Politik drohende Einschränkung der freien, unbelauschten Kommunikation zwischen den Bürgern setzen. Zu dieser Zeit waren die Veröffentlichung und der Export von Kryptographie-Verfahren und -Software in den USA gesetzlich sehr stark eingeschränkt. Zimmermann musste sich ab 1993 wegen der Veröffentlichung von PGP in einem Gerichtsverfahren wegen Verstoßes gegen das Kriegswaffenkontroll-Gesetz verantworten, das erst 1996 eingestellt wurde. Noch heute werden PGP, seine Entwickler, Befürworter und Anwender – insbesondere in den USA – teilweise als subversiv bis potentiell kriminell eingestuft.

1994 erhielt die US-amerikanische Firma **Viacrypt** das Recht, die PGP-Software kommerziell zu vermarkten. Hiermit wurde dem Wunsch professioneller Anwender entsprochen, die nur kostenpflichtige Software mit garantierten Support akzeptieren.

Mitte 1995 wurde vom Norweger **Stale Schumacher** /1/ Version 2.6.2i von PGP außerhalb der USA veröffentlicht, die als **ausgereifte „Standard"-Version des ursprünglichen PGP** außerhalb der USA gilt. PGP 2.6.x verwendet RSA und IDEA.

Seit Ende 1999 darf das Programm PGP legal aus den USA exportiert werden.

Im Mai 1996 gründete Phil Zimmermann mit Partnern die Firma **PGP Inc.**, in der Viacrypt aufging und vermarktete das auf angeblich völlig neu geschriebenem Code basierende PGP™ Version 5.x kommerziell. Seit Version 5 verwendet PGP standardmäßig ein anderes Schlüsselformat (DSS) als die Vorgängerversionen (RSA). Im Dezember 1997 wurde die Firma PGP Inc. und damit das Recht an Warenzeichen und Quellcode von Firma **McAfee Associates** gekauft, die wenig später in Firma **Network Associates Incorporated** (NAI) /12/ aufging.

Im Jahr 1997 gründete Phil Zimmermann die **OpenPGP Alliance** /15/ mit dem Ziel, einen nicht lizenzpflichtigen Standard zur Verschlüsselung von E-Mails unter Verwendung von PGP zu erarbeiten und dessen Umsetzung in der Praxis durchzusetzen. Dieser Standard existiert inzwischen unter dem Namen **OpenPGP**. Er ist dokumentiert als RFC 2440 /17/.

Von NAI wurden im Jahr 1998 das OpenPGP-konforme PGP 6.x und im September 2000 PGP 7.x in kommerziellen und Freeware-Varianten freigegeben sowie eine Reihe darauf aufbauender, rein kommerzieller Produkte mit erheblich erweiterter Funktionalität.

Zimmermann verließ NAI Anfang 2001 im Streit darüber, ob man den Quellcode von PGP weiter offen legen solle, um dessen Vertrauenswürdigkeit nachzuweisen. Im Oktober 2001 löste Network Associates den Unternehmensbereich „**PGP Security**" auf, wo-

bei 250 Beschäftigte ihren Arbeitsplatz verloren. PGP als Produkt und Warenzeichen wurden im August 2002 im Rahmen eines *management buy out* von Firma **PGP Corporation** /13/ zurückgekauft, die von „Veteranen" der ehemaligen PGP Inc. mit *Venture Capital* gegründet wurde. Phil Zimmermann ist bis heute im *Technical Advisory Board* als Berater für die PGP Corporation tätig. Noch im Jahr 2002 wurde Version 8.0 von PGP freigegeben. Momentan (Juni 2004) liegt PGP in der stabilen Version 8.0 sowie der Version 8.5 *public beta* vor. Die von PGP Corporation entwickelte PGP-Basisversion darf für private Zwecke kostenlos eingesetzt werden. Für kommerzielle Nutzung ist eine Lizenz, die ca. 50 US$ kostet, zu erwerben.

Im Rahmen des internationalen Projektes **GNU Privacy Guard**[1] ***(*GnuPG, GPG*)*** /2/ wurde um 1997 von dem Deutschen Werner Koch als Hauptautor der Quellcode für ein **weitgehend zu PGP Version 5 kompatibles** Programm völlig neu geschrieben. Da es nicht das von PGP verwendete, patentierte IDEA-Verfahren zur Verschlüsselung benutzt, darf es lizenzfrei eingesetzt werden. Die unter UNIX ablauffähige Version 1.0.0 von GnuPG wurde im September 1999 freigegeben. GnuPG ist inzwischen für viele UNIX-Flavours und MS Windows verfügbar. GnuPG ist Bestandteil aller GNU/Linux-Distributionen und erfüllt den OpenPGP-Standard. Der Einsatz von GnuPG wird in Deutschland offiziell vom Bundesamt für Sicherheit in der Informationsverarbeitung (BSI) /3/ empfohlen. Momentan (Juni 2004) liegt GnuPG in der stabilen Version 1.2.4 und der Entwicklerversion 1.3.6 vor.

Das deutsche **GNU Privacy Projekt** (**GNUPP**) /6/ der **Free Software Foundation** (FSF) hat die Aufgabe, deutschen Privatpersonen und Firmen den privaten wie auch kommerziellen Einsatz von **GnuPG** unter **MS Windows** zu erleichtern durch Bereitstellung graphischer Benutzeroberflächen, Erstellung deutscher Dokumentation, Softwaretests und weitere Dienstleistungen. Momentan erhältlich sind der **GNU Privacy Assistent** GPA in Version 0.7.0 sowie der **Windows Privacy Tools Tray** WinPT Tray /9/ in der Version 1.0rc2. In Entwicklung befindet sich das eigenständige E-Mail-Programm **Sylpheed** mit integriertem GnuPG. Inwieweit das Projekt GNUPP momentan noch aktiv ist, ist unklar.

Die Projekte GnuPG und GNUPP wurden vom Bundesministerium für Wirtschaft finanziell unterstützt.

Die **kommerziellen Versionen** von PGP enthalten teilweise als offizielles Merkmal(!) „**Hintertüren**" (*back doors*) (bezeichnet z.B. als „Option zur Einrichtung von Drittschlüsseln" bzw. „*Additional Decryption Key*", ADK) für autorisierte Personen („Chefs", Sicherheitsabteilungen von Firmen) sowie – hartnäckigen Gerüchten zufolge – eine Hintertür für die **NSA** (National Security Agency /4/, der größte Geheimdienst der USA). Phil Zimmermann betont, dass in denjenigen Versionen von PGP, die von/mit ihm entwickelt wurden, keine Hintertüren für staatliche US-amerikanische Organisationen enthalten sind. Es gibt aber kommerziell vertriebene Kryptographie-Software, die die in PGP enthaltenen Algorithmen verwendet, für die diese Voraussetzung nicht zutrifft.

[1] Da „Pretty Good Privacy" ist ein eingetragenes Warenzeichen ist, musste für die Neuentwicklung im Rahmen des GNU-Projektes /7/ ein neuer Name für das Programm gefunden werden.

6 Wie arbeitet man als Anfänger mit PGP?

Diese Kurzanleitung für PGP bezieht sich auf die Bedienung von GnuPG Version 1.2.4.

1. Software aus einer vertrauenswürdigen Quelle /2/ **beschaffen**.
2. Software auf einem lokalen Rechner **installieren** und vor unbefugter Manipulation schützen. Das Arbeiten mit PGP an einem Rechner, mit dem man über eine Datenleitung verbunden ist, sollte man unbedingt vermeiden, da dann streng geheime Informationen nicht oder vergleichsweise schlecht geschützt über diese Leitung übertragen werden.
3. Zu verwendenden **Verschlüsselungsalgorithmus**, **Schlüssellänge** (mindestens 1024 bit) und **Gültigkeitsdauer** (z.B. 1..2 Jahre) des Schlüsselpaares auswählen und **einmalig** das eigene **Schlüsselpaar erzeugen**. Hierzu muss man den **eigenen Namen** und die **eigene E-Mail-Adresse** eingeben sowie einen selbst auswählbaren **Schlüssel-Satz** (Mantra, ***passphrase***), **der strengstens geheim zu halten ist**. Der Schlüssel-Satz muss einerseits gut zu merken, andererseits aber möglichst lang sein (10..20 Zeichen) und sollte eine Mischung aus großen und kleinen Buchstaben sowie Zahlen und internationalen Sonderzeichen (keine deutschen Sonderzeichen) enthalten. Die Bestandteile des Schlüssel-Satzes dürfen in keinem Wörterbuch der Welt enthalten sein! Tipp: Anfangsbuchstaben der Worte und die Satzzeichen eines langen, einfach zu merkenden Satzes als Schlüssel-Satz verwenden.
   Jedes mal, wenn man den eigenen privaten Schlüssel benötigt, muss man beim Arbeiten mit PGP auch den Schlüssel-Satz eingeben.
4. Das eigene Schlüsselpaar auf Papier ausdrucken und auf einem haltbaren Datenträger speichern. Ausdruck und Datenspeicher an einem sicheren Ort aufbewahren. **Niemals den Schlüssel-Satz in irgendeiner Form auf irgendeinem Rechner speichern!**
5. **Öffentliche Schlüssel** mit dem Kommunikationspartner **austauschen**, in der Regel per E-Mail. Dazu wird der eigentlich binäre Schlüssel von PGP in 6-bit-Blöcke zerlegt, die als druckbare ASCII-Zeichen dargestellt werden (Base 64 Codierung). Alle Schlüssel werden von PGP in elektronischen **Schlüsselringen** (*key rings*) verwaltet: einem *public keyring* und einem *secret keyring*. Jedem Schlüssel wird eine Vertrauenswürdigkeit zugeordnet.
6. Fingerprint des privaten Schlüssels des Kommunikationspartners erzeugen. Er besteht aus 10 Gruppen von je 4 alphanumerischen Zeichen (nur großen Buchstaben und Ziffern).
7. ***Fingerprints*** der beiden ausgetauschten öffentlichen Schlüssel **verifizieren**, um die unverfälschte Übermittlung der öffentlichen Schlüssel zu bestätigen. Dies sollte persönlich, per Telefon oder eine vertrauenswürdige Zertifizierungsagentur (*certification authority*, CA) erfolgen. In der Praxis wird hierfür leider oft auch E-Mail verwendet, was das gesamte Verfahren gegenüber ambitionierten Angreifern wertlos macht!
8. Zu übermittelnde Dateien mit dem öffentlichen Schlüssel des Kommunikationspartner verschlüsseln und dem eigenen privaten Schlüssel „unterschreiben“.
9. Erhält man verschlüsselte Daten, so werden sie mittels des eigenen privaten Schlüssels entschlüsselt und ihre Authentizität mit dem öffentlichen Schlüssel des Absenders verifiziert.

7 Wie funktioniert PGP?

In PGP wird ein **hybrides Verschlüsselungsverfahren** eingesetzt, das sowohl einen symmetrischen als auch einen asymmetrische Algorithmus verwendet /10/.

Soll eine zu versendende Nachricht **verschlüsselt** werden, so erzeugt PGP aus einer **Zufallszahl** einen geheimen „**Einmal-Schlüssel**“ (*session key*), mit dem die Nachricht unter Verwendung eines **symmetrischen** Verfahrens schnell und effizient verschlüsselt wird. Anschließend wird von PGP nur der „Einmal-Schlüssel“ mit dem öffentlichen Schlüssel des Empfängers mittels eines **asymmetrischen** Verfahrens verschlüsselt. Dann werden beide verschlüsselten Teile von PGP zusammengefasst (*digital envelope*) und vom Absender an den Empfänger übermittelt.

Soll eine erhaltene Nachricht **entschlüsselt** werden, so entschlüsselt PGP mittels des **Schlüssel-Satzes** den geheimen Schlüssel des Empfängers und mittels dieses Schlüssels zunächst unter Verwendung eines **asymmetrischen** Verfahrens den vom Absender erzeugten „Einmal-Schlüssel“. Schließlich wird mittels des „Einmal-Schlüssels“ unter Verwendung eines **symmetrischen** Verfahrens die Nachricht entschlüsselt.

8 Wie sicher ist PGP?

Die Sicherheit von PGP hängt primär davon ab, ob es sachgemäß angewandt wird. Erhält ein Angreifer Zugriff auf Schlüssel-Satz und privaten Schlüssel, so ist der Einsatz von PGP schlimmer als gar keine Verschlüsselung, da der Empfänger einer verschlüsselten Nachricht sich in falscher Sicherheit wiegt. Ein Ausspionieren der kritischen Informationen innerhalb eines Rechners kann z.B. durch Viren, Würmer, *keylogger* etc. sowie auf fahrlässig verwendeten Netzwerkverbindungen durch *sniffer* o.ä. erfolgen. Schliesslich können sicherheitsrelevante Informationen auch durch Analyse der elektromagnetischen Abstrahlung eines Rechners oder durch „*social engineering*“ gewonnen werden.

Das Entschlüsseln mit PGP fachgerecht verschlüsselter Nachrichten ist nach dem aktuell veröffentlichten Kenntnisstand der Kryptologie selbst mit der schnellsten Spezial-Hardware nicht in akzeptabler Zeit möglich. Diese Situation könnte sich dramatisch ändern, sobald Quantencomputer einsatzbereit werden. Nota bene: Da die NSA über Heerscharen von Kryptanalytikern und ein gigantisches Budget verfügt, ist davon auszugehen, dass sie dem veröffentlichten Stand der Technik um ca. 10 Jahre voraus ist.

9 Welche Version von PGP für Windows ist empfehlenswert?

Es gibt aktuell im wesentlichen drei von Privatpersonen kostenlos einsetzbare Varianten von PGP für Windows-Systeme, die weit verbreitet, aber leider nur eingeschränkt zueinander kompatibel sind:

- PGP 2.6.2i /1/ von Stale Schumacher: englisch, ausgereift, vertrauenswürdig, veraltet, für MS-DOS, ohne graphische Benutzeroberfläche
- PGP 8.0.1 DE /13/ von PGP Corporation: deutsch, aktuell, angeblich vertrauenswürdig, für Win 98 über Win 2k(SP 3) bis Win XP (SP 1), mit graphischer Benutzeroberfläche
- GnuPG 1.2.4 /2/ der FSF: englisch, aktuell, vertrauenswürdig, empfehlenswert, für MS Windows Versionen xxx, yyy, zzz

10 Weiter führende Themen

- Verschlüsseln für mehrere Empfänger
- Datenkompression der verschlüsselten Nachricht
- Schlüssel-Verwaltung
- PGP Public-Key-Server, Web of Trust, Certification Authorities, *key revocation*,

11 Gibt es prinzipielle Alternativen zu PGP/GnuPG?

Zur Verschlüsselung der Daten bei **festen Punkt-zu-Punkt-Verbindungen** (ein bestimmter Sender, ein bestimmter Empfänger) können alternativ eingesetzt werden

- **Verschlüsselungs-Hardware** (Crypto-Boxen), die aber sehr teuer und deren Sicherheit nicht einfach nachweisbar ist
- eine durch **Verschlüsselungs-Software** wie **ssh** (*secure shell*) implementierte zusätzliche Protokollschicht, die die übertragenen Daten für Sender und Empfänger unmerklich („transparent“) ver- und entschlüsselt, die jedoch deutlich weniger sicher ist.

12 Wo finde ich mehr Informationen zu PGP/GnuPG?

Internetquellen:

/1/ **The International PGP Home Page**
http://www.pgpi.org
Diese Site wird von dem norwegischen PGP-Aktivisten Stale Schumacher betrieben. Hier wurden früher die komplett neu eingegebenen und kompilierten internationalen Freeware-Versionen von PGP zur Verwendung außerhalb der USA (erkennbar am „i“ am Ende der Versionsbezeichnung) zum kostenlosen Download zur Verfügung gestellt. Hier gibt es auch heute noch die jeweils aktuelle **internationale PGP-Software** mit Dokumentation. Es handelt sich inzwischen um eine nur für die private Nutzung kostenlose Version („Freeware“) der lizenzpflichtigen kommerziellen Software der PGP Corporation.

/2/ **The GNU Privacy Guard**
http://www.gnupg.org
Hier gibt es die jeweils aktuelle **GNU-PGP-Software** mit Dokumentation. Es handelt sich um ein auch für kommerzielle Zwecke kostenlose PGP-Neuentwicklung **ohne bekannte Hintertüren**. Der Quelltext ist verfügbar. Privatleute und Firmen sollten diese Version einsetzen.

/3/ **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
http://www.bsi.de
Diese Site enthält eine Fülle von Informationen sowie eine Sammlung wichtiger kostenloser Software rund um das Thema Informationssicherheit, insbesondere für kleine und mittlere Unternehmen ohne eigene IT-Abteilung.

/4/ **National Security Agency (NSA)**
http://www.nsa.gov
Größter US-amerikanischer Geheimdienst mit ca. 100.000 Mitarbeitern und einem geschätzten Jahresbudget von ca. 15 Milliarden Dollar. Zentrale in Fort Meade, Maryland, USA. Unterliegt keinerlei demokratischer Kontrolle. Betreibt u.a. das Abhörnetz ECHELON /18/, dessen Hauptquartier in Deutschland (noch) in Bad Aibling in Sudostbayern liegt.

/5/ **Ins Internet – mit Sicherheit**
http://www.bsi-fuer-buerger.de
Spezielle Site des BSI mit Informationen über Datensicherheit für Privatpersonen.

/6/ **Das GNU Privacy Projekt**
http://www.gnupp.de
Entwickelt graphische Benutzeroberflächen für die GPG Software, portiert sie auf weitere Betriebssysteme und testet die GnuPG-Software. Die Site enthält u.a. ein gutes Glossar.

/7/ **GNU Operation System – Free Software Foundation**
http://www.gnu.org
Ziel des 1984 gegründeten GNU-Projektes ist die Entwicklung eines kostenlosen UNIX-artigen Betriebssystems einschließlich wesentlicher Anwendungsprogramme. Die Entwicklungsarbeit wird von Tausenden von freiwilligen Helfern geleistet.

/8/ **CrypTool – eLearning-Programm für Kryptographie**
http://www.cryptool.de
Das Open-Source-Projekt CrypTool entwickelt seit 1988 das unter MS Windows ablauffähige Freeware-Programm CrypTool, mit dem kryptographische Verfahren von Nutzern mit soliden kryptographischen Vorkenntnissen angewendet und analysiert werden können. CrypTool ist nicht zur produktiven Datenverschlüsselung geeignet.

/9/ **SourceForge.net: Project WinPT – Windows Privacy Tools**
http://www.sourceforge.net/project/showfiles.php?group_id=71360
Homepage des Projektes WinPT, das insbesondere das auf GnuPG basierende, ursprünglich vom Projekt GNUPP entwickelte Tool WinPT Tray weiter entwickelt.

/10/ Creutzig, C.; Buhl, A.; Zimmermann, P.: **PGP - Pretty Good Privacy - Der Briefumschlag für Ihre elektronische Post**
Bielefeld: Verlag Art d'Ameublement, 4. Auflage 1999, ISBN 3-9802182-9-5, ca. 25 €, nicht mehr lieferbar
Online-Version unter http://www.foebud.org/pgp/html/pgp.html

/11/ **Heise Krypto-Kampagne**
http://www.heise.de/security/dienste/pgp/
Umfangreiche Sammlung von Informationen, Software und Links rund um PGP.

/12/ **Network Associates Inc.**
http://www.nai.com
Homepage der Firma, die die Rechte an PGP von Firma PGP Inc. gekauft hatte.

/13/ **PGP Corporation**
http://www.pgp.com
Homepage der in Palo Alto, Kalifornien, ansässigen Firma, die die Rechte an PGP von Network Associates gekauft hat und bis heute besitzt. PGP Corp. vertreibt aktuell vier auf PGP basierende Produktlinien: PGP Universal, PGP Desktop, PGP Command Line und PGP Mobile.

/14/ **Philip Zimmermanns persönliche Website**
http://www.philzimmermann.com
Enthält viel interessante Informationen und Links rund um Phil Zimmermann und PGP.

/15/ **OpenPGP Alliance Home Page**
http://www.openpgp.org
Homepage der kleinen, aus aktuell 13 Mitgliedsfirmen bestehenden Organisation, die die Verbreitung eines auf PGP basierenden Standards zur E-Mail-Verschlüsselung fördern will.

/16/ **PGP fuer alle**
http://www.pgpfueralle.de
Website von Dirk Kuepper. Enthält Lern-Videos zur Installation diverser Versionen von PGP.

/17/ **RFC 2440**
http://www.ietf.org/html.charters/openpgp-charter.html
Technische Dokumentation des Standards, der OpenPGP zugrunde liegt.

/18/ **Informationen über das ECHELON-Projekt**
http://www.heise.de/tp/deutsch/special/ech/default.html
Das Abhörnetz ECHELON wurde nach dem zweiten Weltkrieg eingerichtet. Es wird gemeinsam von den USA, Großbritannien, Australien, Neuseeland und Kanada betrieben. Während es zunächst auf die Gewinnung militärischer Informationen ausgerichtet war, dient es inzwischen angeblich auch zur Weiterleitung wirtschaftlich relevanter Informationen an die Großindustrie der Betreiberländer. Experten gehen davon aus, dass mittels ECHELON **alle** Telefongespräche, Faxe, E-Mails und der gesamte sonstige Datenverkehr über Funk und das Internet in Deutschland automatisiert abgehört und ausgewertet wird. Inwieweit und wie lange diese Daten von der NSA auch gespeichert werden, ist nicht bekannt.

Bücher und Zeitschriften:

/19/ **Schneier, Bruce: Angewandte Kryptographie - Protokolle, Algorithmen und Sourcecode in C**
AddisonWesley, 1996, ISBN 3-89319854-7, ca. 60 €

/20/ **Buchmann, Johannes: Introduction to Cryptography**
Springer-Verlag, 2001, englisch, ISBN 0-38795034-6, ca. 40 €

/21/ **Elsner, Carsten: Der Dialog der Schwestern**
in c't: Magazin für Computer und Technik, 1999 Heft 25, Seite 288 ff
Erklärung des RSA-Algorithmus