

Inhaltsverzeichnis

Vorwort der Herausgeber	viii
-------------------------	------

Vorwort	xi
---------	----

I. Allgemeines 1

1. Über diesen Text	2
1.1. Leseanleitung	2
1.2. Übersetzung und Fachbegriffe	3
1.3. Konventionen	4
1.4. Danksagungen	5
2. Überblick	6
2.1. Zusammenfassung	6
2.2. Schnellanleitung	6
2.3. Allgemeines	7
2.4. Einsatzgebiete PGPs	8
2.5. Die Funktionsweise PGPs	9
3. Schwachstellen PGPs	14
4. Ein Blick auf's Detail	19
4.1. Schlüsselzertifikate	19
4.2. Schlüsselkennungen	20
4.3. Zufallszahlen	21
4.4. Verschlüsselungsalgorithmen	23
4.4.1. Die symmetrischen Verfahren	23
4.4.2. Die asymmetrischen Verfahren	26
4.4.3. Warum ein hybrides Verfahren?	28
4.5. Datenkomprimierung	29
4.6. Textprüfsummen und digitale Unterschriften	30

5.	Angriffsmöglichkeiten	34
5.1.	Schlechte Geheimhaltung	34
5.2.	Fälschung öffentlicher Schlüssel	35
5.3.	Schutz gegen gefälschte Zeitangaben	36
5.4.	Nicht richtig gelöschte Dateien	37
5.5.	Viren und Trojanische Pferde	39
5.6.	Lücken in der physischen Sicherheit	41
5.7.	„Sturmangriffe“ (tempest attacks)	42
5.8.	Probleme bei Mehrbenutzer-Computern	43
5.9.	Statistik von Nachrichtenverbindungen	44
5.10.	Kryptanalyse	47
6.	Politik	49
6.1.	Warum eigentlich PGP benutzen?	49
6.2.	Verschlüsselung in Deutschland	54
6.3.	Exportkontrolle in den USA	55
6.4.	Das deutsche Signaturgesetz	56
7.	Zum Umgang mit Schlüsseln	58
7.1.	Öffentliche Schlüssel vor Manipulation schützen	58
7.1.1.	Eine dumme Situation	58
7.1.2.	PGPs Ausweg	59
7.2.	Die Schlüssel und andere Leute	62
7.3.	Wie untersucht PGP, welche Schlüssel gültig sind?	63
7.4.	Private Schlüssel vor Diebstahl schützen	65
7.5.	Privaten Schlüssel verloren, was jetzt?	66
II.	Kommandozeilenversionen (2.6, 5.x, gpg)	67
8.	Überblick	68
9.	Allgemeines	70
10.	Die Installation von PGP 2.6.x	72
10.1.	Allgemein	72
10.2.	MS-DOS/Windows	72
10.3.	Linux	73
10.4.	Unix/Andere	73

11. Die Installation von PGP 5.0	74
11.1. MS-DOS/Windows	74
11.2. Linux	74
11.3. Unix	74
12. Die Installation von GnuPG	76
12.1. Allgemein	76
12.2. Linux	76
12.3. Unix	76
12.4. Windows 95/98/NT	76
13. PGP bedienen	78
13.1. Kurzanleitung am Bildschirm	78
13.2. Die Schlüsselverwaltung	79
13.2.1. Schlüssel generieren	80
13.2.2. Schlüssel aufnehmen	83
13.2.3. Schlüssel oder ID löschen	84
13.2.4. Inhaltsangabe des Schlüsselbunds	84
13.2.5. Schlüssel extrahieren	85
13.2.6. Fingerabdruck anzeigen	86
13.2.7. Schlüssel unterschreiben	86
13.2.8. Schlüssel zurückziehen	87
13.2.9. Schlüssel „abschalten“	88
13.3. Verschlüsseln einer Nachricht	88
13.4. Verschlüsseln an mehrere Empfänger	89
13.5. Unterschreiben einer Nachricht	90
13.6. Unterschreiben und Verschlüsseln	91
13.7. Konventionelle Verschlüsselung	91
13.8. Entschlüsselung und Prüfung der Unterschrift	92
13.9. Erzeugen einer Datei mit Zufallszahlen	93
13.10. Nachrichten im Radix-64-Format	93
13.11. Klartext-Unterschrift	96
13.12. Das PGP-Verzeichnis: PGPPATH	97
13.13. Kurzübersicht über die PGP-Befehle	99
13.13.1. Kommandos zum Umgang mit Nachrichten	99
13.13.2. Kommandos zur Schlüsselverwaltung	100
13.13.3. Selten verwendete Kommandos	103
13.13.4. Zusatzoptionen	103

14. Konfigurierbare Parameter	106
15. Spezielle Befehle	124
15.1. Auswahl eines Schlüssels über seine Schlüssel-ID	124
15.2. Trennung der Unterschrift von der Nachricht	125
15.3. Entschlüsseln ohne Unterschriftsprüfung	126
15.4. Textkonvertierungen	127
15.5. Vermeidung von Spuren	128
15.6. Import direkt vom Keyserver	129
15.7. Export zum Keyserver	130
15.8. Anzeige des entschlüsselten Klartextes am Bildschirm .	130
15.9. „Bitte nicht speichern“	130
15.10. „Anonym“ verschlüsseln	131
15.11. Original-Dateinamen verwenden	131
15.12. Ändern der Benutzer-ID und des Mantras	132
15.13. Vertrauensparameter ändern	133
15.14. Schlüsselbund prüfen	134
15.15. Telephonische Kontrolle eines öffentlichen Schlüssels .	135
15.16. Ein Wort zu großen öffentlichen Schlüsselbünden	135
15.17. PGP als Filterprogramm im Unix-Stil	136
15.18. Fragen unterdrücken: BATCHMODE	137
15.19. Standardantwort ja/nein	137
15.20. Der Beendigungscode von PGP	138
15.21. Umgebungsvariable für das Mantra: PGPPASS	140
III. Windowsversionen	143
16. Allgemeines	144
16.1. Vorbemerkungen	144
16.2. Systemvoraussetzungen	145
17. Installation	146
17.1. Vorsicht, Falle	146
17.2. Installation von PGP Freeware 5.0i für Windows	148
17.3. Installation von PGP Freeware 5.5.3i für Windows	153
17.4. Installation von PGP Freeware 6.0i für Windows	160

18. Schlüsselverwaltung – PGPkeys	166
18.1. Schlüsselerzeugung	166
18.2. Importieren von Schlüsseln	173
18.2.1. Allgemeines zum Schlüsselimport	174
18.2.2. Schlüsselimport aus der Zwischenablage	176
18.2.3. Schlüsselimport aus E-Mails	178
18.3. Exportieren von Schlüsseln	178
18.4. Unterschreiben eines Schlüssels	179
18.5. Anzeigen und Ändern von Schlüssel-Eigenschaften	183
18.5.1. Allgemein	184
18.5.2. Unterschlüssel (nur 6.0i)	186
18.5.3. Rückrufer (nur 6.0i)	186
18.6. Übersicht über PGPkeys	187
18.6.1. Die Schlüsselliste	187
18.6.2. Gruppen (nicht bei PGP 5.0i)	191
18.6.3. Die Menübefehle von PGPkeys	194
19. PGP benutzen – Aufrufmöglichkeiten	206
19.1. Die Explorer-Erweiterungen von PGP	206
19.2. PGPTools – Schnellstartleiste	208
19.2.1. PGPkeys starten	208
19.2.2. Verschlüsseln	208
19.2.3. Signieren	209
19.2.4. Verschlüsseln und Signieren	209
19.2.5. Entschlüsseln/Überprüfen	209
19.2.6. Überschreiben und Löschen	209
19.2.7. Überschreiben und Löschen freier Bereiche	210
19.3. PGPTray – PGP für die Windows-Zwischenablage	211
19.3.1. Zwischenablage verschlüsseln	211
19.3.2. Zwischenablage signieren	211
19.3.3. Zwischenablage verschlüsseln und signieren	212
19.3.4. Zwischenablage entschlüsseln/überprüfen	212
19.3.5. Schlüssel importieren	212
19.3.6. Zwischenablage bearbeiten	213
19.3.7. Anzeigeprogramm starten (nur 5.0i)	213
19.3.8. Zwischenablage leeren	213
19.3.9. aktuelles Fenster benutzen (nur 6.0i)	214
19.3.10. PGPTools starten	214
19.3.11. PGPkeys starten	215

19.3.12.	PGPdisk starten	215
19.3.13.	Grundeinstellungen	215
19.3.14.	Hilfe	215
19.3.15.	PGPtray beenden	215
19.4.	Plugins für E-Mailprogramme	215
19.4.1.	PGP-Plugin für Qualcomm Eudora (Light) . . .	216
19.4.2.	PGP-Plugin für Microsoft Outlook/Exchange . .	219
19.4.3.	PGP-Plugin für Pegasus Mail	223
20.	PGP benutzen – Aktionen durchführen	231
20.1.	Daten verschlüsseln	231
20.2.	Daten signieren	234
20.3.	Daten verschlüsseln und signieren	237
20.4.	Verschlüsselte Daten wieder entschlüsseln	237
20.5.	Signaturen prüfen	238
20.6.	Entschlüsseln und Signatur prüfen	240
21.	PGP-Grundeinstellungen	241
21.1.	Allgemeines	241
21.1.1.	Verschlüsselung und Signatur	241
21.1.2.	Schlüsselerzeugung	244
21.1.3.	Dateien löschen	244
21.2.	Dateien	246
21.2.1.	Öffentlicher Schlüsselbund	246
21.2.2.	Privater Schlüsselbund	247
21.2.3.	Startwerte für Zufallszahlen	247
21.3.	E-Mail	248
21.3.1.	PGP/MIME versenden	248
21.3.2.	Zeilenumbruch	248
21.3.3.	Immer verschlüsseln	249
21.3.4.	Immer signieren	250
21.3.5.	Automatisch entschlüsseln	250
21.4.	Keyserver	251
21.4.1.	PGP 5.0i	252
21.4.2.	PGP 5.5.3i	253
21.4.3.	PGP 6.0i	255
21.5.	Fortgeschrittene Einstellungen	258
21.5.1.	Verschlüsselung	258
21.5.2.	Vertrauenseinstellungen	259

IV. Anhang	263
A. Die vielen PGP-Versionen	264
A.1. Die Versionen 2.x	264
A.2. Die Versionen 5.x und 6.x	266
A.3. GnuPG	269
B. Kompatibilität der Versionen von PGP	271
C. Die beiliegende CD	273
D. Kurz vorgestellt: Die Verschlüsselungsalgorithmen	275
D.1. IDEA	275
D.2. RSA	277
D.3. ElGamal	279
E. Rechtsfragen	282
E.1. Warenzeichen, Copyright, Garantie	282
E.2. Patentrechte auf die Algorithmen	282
E.3. Lizenzierung und Vertrieb	285
F. Computerorientierte politische Vereinigungen in Deutschland	288
G. Glossar	292
H. Index	296