

# Contents

<b>Preface</b>	<b>v</b>
Conventions used in this document	v
For more information	vi
From the Web	vi
Technical Support	vi
Your feedback is welcome	vi
Recommended Introductory Readings	vi
Other Readings	vii
What's in this book	vii
<b>Contents</b>	<b>ix</b>
<b>Chapter 1: Introducing PGP for Personal Privacy</b>	<b>15</b>
What's new in PGP Version 5.5	15
What's new in PGP Version 5.5 documentation	16
Using PGP	16
A quick overview	16
Create a private and public key pair	17
Exchange public keys with others	18
Validate your keys	18
Encrypt and sign your email and files	18

Decrypt and verify your email and files . . . . .	19
Wipe files . . . . .	19
<b>Chapter 2: Getting Started . . . . .</b>	<b>21</b>
System requirements . . . . .	21
Compatibility with other versions . . . . .	21
About PGP for Personal Privacy . . . . .	22
PGP for email and files . . . . .	22
Using PGP/MIME . . . . .	23
Upgrading from a previous version . . . . .	23
Upgrading from PGP Version 2.6.2 or 2.7.1 . . . . .	24
Upgrading from PGPmail 4.0 . . . . .	25
Upgrading from PGPmail 4.5 . . . . .	25
Upgrading from PGP Version 5.0 . . . . .	26
Installing PGP Version 5.5 . . . . .	27
From a CD ROM . . . . .	27
From the Network Associates Web site . . . . .	27
Running PGP . . . . .	28
Using PGP from the System tray . . . . .	28
Using PGP from supported email applications . . . . .	30
Using PGP from the Windows Explorer . . . . .	31
Selecting recipients . . . . .	31
Taking shortcuts . . . . .	32
PGPkeys icon definitions . . . . .	32
<b>Chapter 3: Making and Exchanging Keys . . . . .</b>	<b>35</b>
Key concepts . . . . .	35
Making a key pair . . . . .	36

How to remember your passphrase . . . . .	40
Protecting your keys . . . . .	41
Distributing your public key . . . . .	42
Making your public key available through a key server . . .	42
Including your public key in an email message . . . . .	44
Exporting your public key to a file . . . . .	44
Obtaining the public keys of others . . . . .	45
Getting public keys from a key server . . . . .	45
Adding public keys from email messages . . . . .	47
Importing a public key from a file . . . . .	47
Verifying the authenticity of a key . . . . .	47
Getting keys via trusted introducers . . . . .	49
<b>Chapter 4: Sending and Receiving Private Email . 51</b>	
Encrypting and signing email . . . . .	51
Encrypting and signing with supported email applications	52
Decrypting and verifying email . . . . .	53
Decrypting and verifying from supported email applications	54
About PGPllog . . . . .	55
About recipient groups . . . . .	55
<b>Chapter 5: Using PGP for Secure File Storage . . . 59</b>	
Using PGP to encrypt and decrypt files . . . . .	59
Encrypting and signing via the clipboard . . . . .	59
Decrypting and verifying via the clipboard . . . . .	61
Encrypting and signing from the Windows Explorer . . . . .	62
Decrypting and verifying from the Windows Explorer . . . . .	64

Using PGP functions from the Windows Explorer . . . . .	65
To permanently overwrite a file . . . . .	65

## **Chapter 6: Managing Keys and Setting Preferences 67**

Managing your keys . . . . .	67
The PGPkeys window . . . . .	68
PGPkeys attribute definitions . . . . .	69
Examining a key's properties . . . . .	71
Specifying a default key pair . . . . .	73
Adding a new user name or address . . . . .	73
Checking a key's fingerprint . . . . .	74
Signing someone's public key . . . . .	75
Granting trust for key validations . . . . .	76
Disabling and enabling keys . . . . .	76
Deleting a key or signature . . . . .	77
Changing your passphrase . . . . .	77
Importing and exporting keys . . . . .	78
Revoking a key . . . . .	79
Setting your preferences . . . . .	80
General preferences . . . . .	80
Files preferences . . . . .	83
Email preferences . . . . .	84
Key Server preferences . . . . .	85
Advanced preferences . . . . .	87
About key searches . . . . .	88
To search for a user's key . . . . .	88

## **Chapter 7: Troubleshooting PGP . . . . . 91**

## **Chapter 8: Security Features and Vulnerabilities . 95**

Why I wrote PGP . . . . .	95
Encryption basics . . . . .	100
How public key cryptography works . . . . .	101
How your files and messages are encrypted . . . . .	102
The PGP symmetric algorithms . . . . .	103
Data compression . . . . .	105
About the random numbers used as session keys . . . . .	106
How decryption works . . . . .	107
How digital signatures work . . . . .	107
How to protect public keys from tampering . . . . .	110
How does PGP keep track of which keys are valid? . . . . .	114
How to protect private keys from disclosure . . . . .	116
Beware of snake oil . . . . .	118
Vulnerabilities . . . . .	124
Compromised passphrase and private key . . . . .	124
Public key tampering . . . . .	125
Not Quite Deleted Files . . . . .	125
Physical security breach . . . . .	128
Tempest attacks . . . . .	128
Protecting against bogus timestamps . . . . .	129
Exposure on multi-user systems . . . . .	130
Traffic analysis . . . . .	130
Cryptanalysis . . . . .	131

## **Chapter 9: Transferring Files Between the MacOS and Windows using PGP . . . . . 133**

Sending from the MacOS to Windows . . . . .	134
MacBinary: Yes . . . . .	135
MacBinary: No . . . . .	135
MacBinary: Smart . . . . .	135
Receiving Windows files on the MacOS . . . . .	137
Supported Applications . . . . .	137
<b>Glossary . . . . .</b>	<b>139</b>
<b>Index . . . . .</b>	<b>143</b>