

PGP Windows 95, 98, e NT

Guia do Usuário

versão 6.0

Copyright © 1990-1998 Network Associates, Inc. e suas Companhias Afiliadas. Todos os direitos reservados.

Tradução para o português do Brasil, diagramação e versões HTML e PDF feitas por
Christian Haagensen Gontijo - chrishg@geocities.com
novembro de 1999.

PGP*, Versão 6.0.2

11-98. Original impresso nos Estados Unidos da América.

PGP, Pretty Good, e Pretty Good Privacy são marcas registradas da Network Associates, Inc. e/ou suas Companhias Afiliadas nos EUA e outros países. Todas as outras marcas registradas e não registradas neste documento são de única propriedade de seus respectivos proprietários.

Porções deste software podem usar algoritmos de chave pública descritos nas patentes americanas sob os números 4,200,770, 4,218,582, 4,405,829, e 4,424,414, licenciados exclusivamente por Public Key Partners; a cifra de criptografia IDEA(tm) descrita no número de patente nos EUA 5,214,703, licenciados da Ascom Tech AG; e da Northern Telecom Ltd., Algoritmo de Codificação CAST, licenciado da Northern Telecom, Ltd. IDEA é marca da Ascom Tech AG. Network Associates Inc. pode ter aplicativos com patentes e/ou patentes pendentes cobrindo o assunto neste software ou sua documentação; o fornecimento deste software ou documentação não lhe dá nenhuma licença à estas patentes. O código de compressão em PGP é por Mark Adler e Jean-Loup Gailly, usados com permissão da implementação gratuita Info-ZIP. Software LDAP provido cortesia da University of Michigan em Ann Arbor, Copyright © 1992-1996 Regentes da University of Michigan. Todos os direitos reservados. Este produto inclui software desenvolvido pelo Apache Group para uso no projeto do servidor HTTP Apache (<http://www.apache.org/>). Copyright © 1995-1997 The Apache Group. Todos os direitos reservados. Veja arquivos texto incluídos com o software ou o site web de PGP para maiores informações. Este software é baseado em parte no trabalho do Independent JPEG Group. Fonte TEMPEST cortesia de Ross Anderson e Marcus Kuhn.

O software provido com esta documentação é autorizado a você para seu uso individual sob a condição do Acordo de Licença ao Usuário Final e Garantia Limitada provida com o software. As informações neste documento estão sujeitas à mudanças sem advertência. Network Associates Inc. não garante que a informação adeque-se à seus requerimentos ou que a informação está livre de erros. A informação pode incluir inexatidões técnicas ou erros tipográficos. Alterações podem ser feitas às informações e podem ser incorporadas em novas edições deste documento, se e quando disponibilizado pela Network Associates Inc.

Exportação deste software e documentação podem estar sujeitas ao acordo com as regras e regulamentações promulgadas de tempos em tempos pelo Bureau of Export Administration, United States Department of Commerce, que restringe a exportação e reexportação de certos produtos e dados técnicos.

Network Associates, Inc.	(408) 988-3832 principal
3965 Freedom Circle	(408) 970-9727 fax
Santa Clara, CA 95054	http://www.nai.com info@nai.com

* é às vezes utilizado ao invés do ® para marcas registradas para proteger marcas registradas fora dos EUA.

GARANTIA LIMITADA

Garantia Limitada. Network Associates, Inc. garante que o Produto de Software executará substancialmente conforme os materiais escritos que o acompanham para um período de sessenta (60) dias da data de compra original. Para a extensão permitida por lei aplicável, garantias implícitas no Produto de Software, se existirem, são limitadas a um período de sessenta (60) dias. Alguns jurisdições não permitem limitações em duração de uma garantia implícita, assim a limitação anterior pode não se aplicar a você.

Remediação ao Consumidor. A total obrigação da Network Associates, Inc e seus provedores e seu remédio exclusivo será, sob opção da Network Associates, Inc, ou (a) retorno do valor de compra pago pela licença, se houve ou (b) conserto ou substituição do Produto de Software que não satisfaça a garantia limitada da Network Associates, Inc e que será devolvido a seu custo para a Network Associates, Inc com uma cópia de seu recibo. Esta garantia limitada é nula se a falha do Produto de Software foi resultado de acidente, abuso, ou má aplicação. Qualquer Produto de Software consertado ou substituído será garantido para o resto do período da garantia original ou trinta (30) dias, o que for mais longo. Fora dos Estados Unidos, nenhum estes remédios nem qualquer serviço de suporte ao produto oferecidos por Network Associates, Inc está disponível sem prova de compra de uma fonte autorizada internacional e pode não estar disponível pela Network Associates, Inc para a extensão à que eles estão sujeitos às restrições sob as leis de controle de exportação dos EUA e regulamentos.

NENHUMA OUTRA GARANTIA. PARA A MÁXIMA EXTENSÃO PERMITIDA POR LEI APLICÁVEL, E COM EXCEÇÃO DAS GARANTIAS LIMITADAS ADIANTE, O SOFTWARE E DOCUMENTAÇÃO É PROVIDO “COMO É” E A NETWORK ASSOCIATES, INC. E SEUS PROVEDORES NEGAM TODAS AS OUTRAS GARANTIAS E CONDIÇÕES, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO LIMITADAS A, GARANTIAS IMPLÍCITAS DE MERCABILIDADE, APTIDÃO PARA UM PROPÓSITO PARTICULAR, CONFORMÂNCIA COM A DESCRIÇÃO, TÍTULO E NÃO-INFRAÇÃO DE DIREITOS DE TERCEIROS, E A PROVISÃO OU FALHA DE PROVER SERVIÇOS DE SUPORTE. ESTA GARANTIA LIMITADA LHE DÁ DIREITOS LEGAIS ESPECÍFICOS. VOCÊ PODE TER OUTROS, QUE VARIAM DE JURISDIÇÃO A JURISDIÇÃO.

LIMITAÇÃO DE OBRIGAÇÃO. PARA A EXTENSÃO MÁXIMA PERMITIDA POR LEI APLICÁVEL, EM NENHUM EVENTO DEVE NETWORK ASSOCIATES, INC. OU SEUS PROVEDORES ESTAREM SUJEITOS A QUALQUER DANO INDIRETO, INCIDENTAL, CONSEQÜENTE, ESPECIAL OU EXEMPLAR OU PERDA DE LUCROS SEJA QUAIS FOREM (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS EMPRESARIAIS, INTERRUÇÃO EMPRESARIAL, PERDA DE INFORMAÇÃO EMPRESARIAL, OU QUALQUER OUTRA PERDA PECUNIÁRIA) SURGINDO DO USO OU INABILIDADE DE USO DO PRODUTO DE SOFTWARE OU A FALHA EM PROVER SERVIÇOS DE SUPORTE, ATÉ MESMO SE NETWORK ASSOCIATES, INC. FOI ACONSELHADA DA POSSIBILIDADE DE TAIS DANOS. EM QUALQUER CASO, AS INTEIRAS OBRIGAÇÕES CUMULATIVAS DA NETWORK ASSOCIATES, INC. PARA VOCÊ OU QUALQUER OUTRA PARTE POR QUALQUER PERDA OU DANO RESULTANDO DE QUALQUER REIVINDICAÇÃO, DEMANDAS OU AÇÕES QUE SURGIREM DE, OU RELATIVO A ESTE ACORDO NÃO EXCEDERÃO O PREÇO DE COMPRA PAGO POR ESTA LICENÇA. COMO ALGUMAS JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO OU LIMITAÇÃO DE OBRIGAÇÃO, AS LIMITAÇÕES MENCIONADAS ACIMA PODEM NÃO SE APLICAR A VOCÊ.

Prefácio	12
Como contactar a Network Associates	13
Serviço ao Consumidor	13
Suporte Técnico	13
Treinamento na Network Associates	14
Comentários e <i>feedback</i>	14
Leituras Recomendadas	15
Livros não-técnicos e iniciantes	15
Livros Intermediários	15
Livros Avançados	16
Introduzindo PGP	17
O que há de novo em PGP versão 6.0.....	17
Novos recursos de PGPdisk	19
Usando PGP	20
Uma rápida visão geral	20
Passos Básicos para usar PGP	20
Iniciando	24
Executando PGP	24
Usando PGP pela bandeja de sistema	24
Executando funções de PGP pela Área de Transferência	24
Abrindo a janela de PGPkeys	25
Configurando preferências de PGP	25
Obtendo Ajuda	25
Finalizando PGP	26
Usando PGP através dos aplicativos de email suportados	26
Usando PGP/MIME	26

Usando PGP através de PGPtools	27
Usando PGP através do Windows Explorer	27
Selecionando Destinatários.....	28
Tomando Atalhos.....	28
Definições dos Ícones de PGPkeys	29
Criando e Trocando Chaves	33
Conceitos chave	33
Criando um Par de Chaves.....	34
Para Criar um Novo Par de Chaves	34
Criando uma Frase-Senha Que Você Vai Se Lembrar	39
Adicionando um ID fotográfico à sua chave	39
Para adicionar sua fotografia à sua chave:.....	40
Para substituir seu ID fotográfico	41
Criando novas subchaves.....	41
Para criar novas subchaves	42
Divisão de Chaves.....	43
Para criar uma chave dividida em múltiplas partes.....	43
Protegendo suas chaves.....	46
Distribuindo sua chave pública.....	47
Tornando sua chave pública disponível através de um Servidor de Chaves	47
Para enviar sua chave pública a um Servidor de Chaves	48
Atualizando sua chave em um Servidor de Chaves	48
Removendo assinaturas ou nomes de usuário associados com sua chave	48
Para apagar sua chave de um Servidor de Certificados	49
Incluindo sua Chave Pública em uma Mensagem de Email	50
Para Incluir sua Chave Pública em uma Mensagem de Email.....	50
Exportando sua chave pública para um arquivo	50

Para exportar sua chave pública para um arquivo	50
Obtendo as chaves públicas de outros	51
Para obter a chave pública de alguém.....	51
Obtendo uma Chave de um Servidor de Chaves Públicas	51
Para obter a chave pública de alguém através de um servidor de chaves	52
Adicionando chaves públicas a partir de mensagens de email	53
Para adicionar uma chave pública a partir de uma mensagem de email.....	53
Importando uma chave pública de um arquivo	53
Para importar uma chave pública de um arquivo	53
Verificando a autenticidade de uma chave	54
Por quê verificar a autenticidade de uma chave?.....	54
Verificando com uma impressão digital	54
Assinando a chave pública	55
Obtendo chaves públicas a partir de apresentadores de confiança	55
Enviando e Recebendo Email Seguro	56
Codificando e assinando email	56
Codificando e assinando com os aplicativos de email suportados	56
Para codificar e assinar com aplicativos de email suportados	57
Para codificar e assinar texto usando PGTools	59
Codificando email para grupos de destinatários	61
Trabalhando com listas de distribuições	61
Para criar um grupo (lista de distribuição).....	61
Para adicionar membros a uma lista de distribuição.....	61
Para remover membros de uma lista de distribuição	62
Para remover uma lista de distribuição	62
Para adicionar uma lista de distribuição a outra lista de distribuição	62
Enviando email codificado e assinado para listas de distribuição	62

Para enviar email codificado e assinado a uma lista de distribuição	62
Decifrando e verificando email.....	63
Para decifrar e verificar a partir de aplicativos de email suportados	63
Para decifrar e verificar a partir de aplicativos de email não suportados	65
Usando PGP para Armazenamento Seguro de Dados.....	66
Usando PGP para codificar e decifrar arquivos.....	66
Usando o menu de PGP do botão direito para codificar e assinar	66
Para codificar e assinar usando o menu do botão direito	66
Usando PGPtools para codificar e assinar	69
Para codificar e assinar usando PGPtools	69
Usando PGPtray para decifrar e verificar	71
Para decifrar e verificar arquivos usando PGPtray.....	71
Usando PGPtools para decifrar e verificar.....	72
Para decifrar e verificar usando PGPtools	72
Assinando e decifrando arquivos com uma chave dividida.....	72
Para assinar ou decifrar arquivos com uma chave dividida.....	73
Para enviar sua parte da chave através da rede	75
Usando PGP Wipe para apagar arquivos	77
Para apagar permanentemente um arquivo usando o menu do botão direito	77
Para apagar permanentemente um arquivo usando PGPtools.....	78
Usando PGP Free Space Wiper para limpar espaço livre em seus discos	78
Para eliminar espaço livre de seus discos	79
Gerenciando Chaves e Configurando Preferências	81
Gerenciando suas chaves	81
A janela de PGPkeys.....	81
Definição dos atributos de PGPkeys.....	83
Examinando as propriedades de uma chave	86

Janela de propriedades gerais da chave	87
Janela de propriedades de subchaves	89
Especificando um par de chaves padrão	89
Para especificar seu par de chaves padrão	90
Adicionando um novo nome de usuário ou endereço para um par de chaves	90
Para adicionar um novo nome de usuário ou endereço a uma chave existente	90
Verificando a chave pública de alguém.....	91
Para checar uma chave pública com a impressão digital da chave	91
Assinando a chave pública de alguém	92
Para assinar a chave pública de alguém.....	92
Concedendo confiança a validação de chaves	95
Para conceder confiança a uma chave	95
Desabilitando e habilitando chaves.....	96
Para desabilitar uma chave	96
Para habilitar uma chave	96
Apagando uma chave, assinatura, ou ID de usuário	96
Para apagar uma chave, uma assinatura, ou um ID de usuário	97
Alterando sua Frase-Senha	97
Para alterar sua frase-senha.....	97
Importando e Exportando Chaves.....	98
Para importar uma chave de um arquivo	98
Para adicionar uma chave de uma mensagem de email	99
Para exportar uma chave para um arquivo.....	99
Revogando uma chave	99
Para revogar uma chave	100
Para apontar um revogador designado	100
Configurando suas preferências.....	102

Para configurar preferências gerais.....	102
Para configurar preferências de arquivos.....	104
Para configurar preferências de email.....	105
Para configurar preferências de servidores	107
Para configurar preferências avançadas	111
Procurando por uma chave	113
Para procurar pela chave de um usuário	113
PGPdisk.....	115
O que é PGPdisk?	115
Recursos de PGPdisk	115
Por que usar PGPdisk?.....	116
Iniciando o programa PGPdisk	117
Para iniciar PGPdisk	117
Trabalhando com volumes PGPdisk.....	118
Criando um novo volume PGPdisk.....	118
Para criar um novo volume PGPdisk	118
Alterando uma frase-senha.....	120
Para alterar sua frase-senha.....	120
Adicionando frases-senhas alternativas	121
Para adicionar frases-senhas alternativas	121
Removendo uma frase-senha	123
Para remover uma frase-senha	123
Removendo todas as frases-senhas alternativas.....	123
Para remover todas as frases-senhas alternativas.....	123
Adicionar/Remover Chaves Públicas	124
Para adicionar uma chave pública em seu volume PGPdisk	124
Para remover uma chave pública de seu volume PGPdisk	124

Montando um volume PGPdisk	125
Para montar um volume usando o botão “Mount”	126
Usando um volume PGPdisk montado	126
Desmontando um volume PGPdisk	127
Para desmontar um volume PGPdisk.....	127
Especificando Preferências	127
Para especificar preferências.....	127
Mantendo Volumes PGPdisk.....	129
Montando arquivos PGPdisk em um servidor remoto	129
Montando automaticamente volumes PGPdisk	129
Para montar automaticamente volumes PGPdisk	129
Realizando <i>backups</i> de volumes PGPdisk	130
Para efetuar <i>backup</i> de volumes PGPdisk	130
Trocando volumes PGPdisk.....	130
Alterando o tamanho de um volume PGPdisk.....	131
Para alterar o tamanho de um volume PGPdisk.....	131
Detalhes Técnicos e Considerações de Segurança.....	132
Sobre volumes PGPdisk.....	132
O algoritmo de criptografia de PGPdisk.....	132
Qualidade da Frase-Senha.....	133
Precauções especiais de segurança tomadas por PGPdisk.....	134
Apagamento da frase-senha	134
Proteção de memória virtual	134
Proteção de memória contra migração de íons estáticos.....	134
Outras considerações de segurança.....	135
Solucionando Problemas com PGP	136
Transferindo Arquivos entre MacOS e Windows	143

Enviando do MacOS ao Windows	144
Recebendo arquivos Windows no MacOS	146
Aplicativos Suportados	146
Phil Zimmermann sobre PGP.....	148
Por que escrevi PGP	148
Os algoritmos simétricos de PGP	152
Sobre as rotinas de compressão de dados de PGP	153
Sobre os números aleatórios usados como chaves de sessão.....	154
Sobre o sumário da mensagem.....	154
Como proteger suas chaves públicas de falsificações.....	155
Como PGP mantém registro de quais chaves são válidas?	158
Como proteger suas chaves privadas de serem descobertas	160
E se você perder sua chave privada?.....	161
Cuidado com veneno de cobra	162
Vulnerabilidades	166
Comprometimento da frase-senha e chave privada	166
Falsificação da chave pública	167
Arquivos não apagados completamente do disco	167
Viroses e Cavalos de Tróia	168
Arquivos de troca ou memória virtual	168
Falha de segurança física	169
Ataques “Tempest”	170
Protegendo-se contra marcas de hora falsas	170
Exposição em sistemas multiusuário	171
Análise de tráfico	171
Criptoanálise	172
Glossário	173

Prefácio

PGP é parte da caixa de ferramentas de segurança de sua organização por proteger um de seus recursos mais importantes: *informação*. Corporações tradicionalmente colocam fechaduras em suas portas e gabinetes de arquivo, e exigem dos empregados que mostrem identificação para provar que eles possuem acesso a vários locais da empresa. PGP é uma valiosa ferramenta para lhe ajudar a proteger a segurança e integridade dos dados e mensagens da sua organização. Para muitas companhias, a perda de confidencialidade significa perda de negócios.

Livros inteiros foram escritos sobre o assunto de implementação de segurança em rede. O enfoque deste guia está em implementar PGP como uma ferramenta dentro de sua estrutura de segurança de rede. PGP é meramente uma parte de um sistema de segurança, mas é uma parte extremamente importante. PGP provê codificação, que protege os dados dos olhos de qualquer um a quem não se intencionam, mesmo para aqueles que podem ver os dados codificados. Isto protege a informação de estranhos internos e externos.

Este guia descreve como usar PGP[®] para Windows 95, 98, e NT. PGP tem muitas características novas, que são descritas no [Capítulo 1, “Introduzindo PGP”](#).

Se você é novo à criptografia e gostaria de uma introdução à terminologia e conceitos que você encontrará enquanto estiver usando PGP, veja “Uma Introdução à Criptografia”.

Como contactar a Network Associates

Serviço ao Consumidor

Para ordenar produtos ou obter informações sobre produtos, contate o departamento Customer Care da Network Associates em (408) 988-3832 (telefone dos EUA) ou escreva para o seguinte endereço:

Network Associates, Inc.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
U.S.A.

Suporte Técnico

Network Associates é famosa por sua dedicação à satisfação do consumidor. Nós continuamos esta tradição fazendo de nosso site na World Wide Web um recurso de valor para respostas às questões de suporte técnico. Encorajamos você a fazer desta a sua primeira parada por respostas a perguntas freqüentemente feitas, para atualizações de software da Network Associates, e para acesso às notícias e informações de codificação da Network Associates.

World Wide Web <http://www.nai.com>

Suporte Técnico para seu produto PGP também está disponível através destes canais:

Telefone (EUA): (408) 988-3832

Email PGPSupport@pgp.com

Se os serviços automatizados não tiverem as respostas que você precisa, contacte a Network Associates em um dos seguintes números entre segunda-feira e sexta-feira entre 6h00m e 18h00m (horário do Pacífico).

Telefone (EUA): (408) 988-3832

Para prover as respostas que você precisa rápida e eficientemente, a equipe de suporte técnico da Network Associates precisa de algumas informações sobre seu computador e todos seus softwares. Por favor, tenha esta informação pronta antes de sua chamada:

- Nome do produto e número de versão
- Marca e modelo do computador
- Quaisquer hardwares ou periféricos adicionais conectados a seu computador
- Tipo de sistema operacional e números de versão
- Tipo de rede e versão, se aplicável
- Conteúdo de quaisquer mensagens de status ou erro exibidos na tela ou que apareçam em um arquivo de log (registro). Nem todos os produtos produzem arquivos de log.
- Aplicativo de email e versão (se o problema envolve o uso de PGP com um produto de email, por exemplo, o plug-in para Eudora)
- Passos específicos para reproduzir o problema

Treinamento na Network Associates

Para informações sobre agendamento de treinamentos “on-site” para qualquer produto Network Associates, ligue (800) 338-8754 (telefone nos EUA).

Comentários e *feedback*

Network Associates aprecia seus comentários e *feedback*, mas não possui nenhuma obrigação a você pelas informações que você enviar. Por favor enderece seus comentários sobre a documentação de PGP para: Network Associates, Inc., 3965 Freedom Circle Santa Clara, CA 95054-1203 U.S.A.. Você também pode enviar comentários via e-mail para tns_documentation@nai.com.

Leituras Recomendadas

Livros não-técnicos e iniciantes

- Whitfield Diffie and Susan Eva Landau, “Privacy on the Line”, MIT Press; ISBN: 0262041677
Este livro é uma discussão da história e política envolvendo criptografia e segurança de comunicações. É uma excelente leitura, até mesmo para os iniciantes e pessoas não-técnicas, mas com informação que mesmo muitos peritos não conhecem.
- David Kahn, “The Codebreakers”, Scribner; ISBN: 0684831309
Este livro é uma história de códigos e quebradores de códigos desde os tempos dos egípcios até o fim da Segunda Guerra Mundial. Kahn começou a escrever este livro nos anos sessenta, e há uma edição revisada publicada em 1996. Este livro não lhe ensinará tudo sobre como é feita a criptografia, mas foi a inspiração de toda uma nova geração de criptógrafos.
- Charlie Kaufman, Radia Perlman, and Mike Spencer, “Network Security: Private Communication in a Public World”, Prentice Hall; ISBN: 0-13-061466-1
Esta é uma boa descrição de sistemas de segurança de rede e protocolos, incluindo descrições do que funciona, o que não funciona, e por quê. Publicado em 1995, portanto não possui muito dos mais recentes avanços, mas ainda é um livro bom. Também contém um das descrições mais claras de como funciona o DES de qualquer livro escrito.

Livros Intermediários

- Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, John Wiley & Sons; ISBN: 0-471-12845-7
Este é um bom livro técnico introdutório sobre como funcionam muitos trabalhos de criptografia. Se você quer se tornar um perito, este é o lugar para começar.
- Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone, “Handbook of Applied Cryptography”, CRC Press; ISBN: 0-8493-8523-7
Este é o livro técnico que você deveria adquirir depois do livro de Schneier. Há muita matemática pesada neste livro, entretanto é utilizável para quem não entende a matemática.
- Richard E. Smith, “Internet Cryptography”, Addison-Wesley Pub Co; ISBN: 020192480
Este livro descreve vários protocolos de segurança da Internet. Mais importante, descreve como sistemas que são bem projetados acabam com falhas por causa de

operações descuidadas. Este livro é leve na matemática, e pesado em informação prática.

- William R. Cheswick and Steven M. Bellovin, “Firewalls and Internet Security: Repelling the Wily Hacker” Addison-Wesley Pub Co; ISBN: 0201633574
Este livro é escrito por dois pesquisadores sênior na AT&T Bell Labs, sobre suas experiências mantendo e reprojetoando a conexão Internet da AT&T. Muito legível.

Livros Avançados

- Neal Koblitz, “A Course in Number Theory and Cryptography” Springer-Verlag; ISBN: 0-387-94293-9
Um excelente livro de ensino de matemática em nível de graduação, em teoria dos números e criptografia.
- Eli Biham and Adi Shamir, “Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag; ISBN: 0-387-97930-1
Este livro descreve a técnica da criptoanálise diferencial como aplicado ao DES. É um excelente livro para se aprender sobre esta técnica.

Bem vindo a PGP. Com PGP, você pode fácil e seguramente proteger a privacidade de seus dados codificando-os, de forma que apenas os indivíduos a quem eles se intencionam possam lê-los. Você também pode digitalmente assinar informações, o que certifica sua autenticidade.

O que há de novo em PGP versão 6.0

Esta versão de PGP inclui estes novos recursos:

- **Secure Viewer (Visualizador Seguro):** o “Secure Viewer” é a solução por software de PGP para proteger as informações privadas na sua tela do computador de serem interceptadas através de radiação eletromagnética - também conhecido como “ataques TEMPEST”. É amplamente conhecido que espiões, com equipamentos especiais, podem capturar e reconstruir conteúdo de telas de vídeo através da radiação de frequências de rádio. Quando texto é codificado com a opção Visualizador Seguro habilitada, o texto decifrado é exibido em uma fonte e janela especiais que previne ataques TEMPEST, ilegíveis à equipamentos de captura de radiações. O recurso “Secure Viewer” permite que você veja com segurança seu texto decifrado.
- **Funcionalidade PGPdisk.** A funcionalidade PGPdisk está embutida em PGP versão 6.0. PGPdisk é uma aplicação de codificação fácil de usar que permite que você disponibilize uma área de espaço de disco para armazenar seus dados sensíveis.
- **Revogados Designados.** Você agora pode especificar que outra chave pública em seu chaveiro pode revogar sua chave. Isto pode ser útil em situações onde você tem medo de perder sua chave privada, esquecer sua frase-senha, ou em casos extremos como incapacidade física de usar a chave. Em tais casos, a pessoa que você designar poderá revogar sua chave, enviá-la ao servidor, e será como se você tivesse revogado você mesmo.
- **“Plug-ins” Adicionais.** Plug-ins de email para Outlook Express e Outlook 98 estão incluídos. Um plugin para Groupwise está disponível separadamente.
- **Photographic User ID (Identificação Fotográfica de Usuário).** Você pode adicionar sua fotografia em sua chave pública. IDs fotográficos podem ser assinados como qualquer ID de usuário, para prover informações extras quando verificando a chave.

- **Comunicações Seguras com o PGP Certificate Server 2.0.** PGP provê uma conexão segura quando qualquer pedido é enviado ao servidor. Esta conexão segura previne qualquer análise de tráfego que possa determinar as chaves que você está obtendo de ou enviando para o servidor.
- **Apagamento Seguro usando PGP Certificate Server.** Você pode apagar ou incapacitar sua própria chave no servidor, bastando se autenticar via Transport Layer Security (TLS).
- **Barra de Ferramentas PGPkeys.** Uma barra de ferramentas de ícones foi adicionada a PGPkeys para facilitar o acesso às funções de administração de chaves mais frequentemente usadas.
- **Destinatário Desconhecido ou Procura no Servidor pelo Assinante.** Quando decifrando ou verificando uma mensagem, você pode automaticamente executar uma procura no servidor por todas as chaves para a qual a mensagem foi codificada ou assinada, para determinar a identidade das mesmas.
- **Administração de Subchaves** (apenas Diffie-Hellman/DSS). Com a característica de administração de subchaves, você pode administrar suas chaves para codificação (DH) e assinatura (DSS) separadamente.
- **Assinatura de Reverificação.** As assinaturas colecionadas em chaves são automaticamente verificadas quando adicionadas a seu chaveiro. É possível, entretanto, seja por corrupção de dados ou alterações maliciosas, que assinaturas inválidas possam existir. Esta nova característica permite que você re-verifique as assinaturas, para assegurar-se de que elas são válidas.
- **Assinatura com Expiração.** Você pode criar assinaturas em outras chaves que vão expirar depois de uma determinada data.
- **Interface Aperfeiçoada.** Uma barra de ferramentas intuitiva foi acrescentada a PGPkeys, para facilitar o acesso às funções de administração de chaves mais frequentemente usadas.
- **Melhor Integração do Aplicativo.** PGPTray permite codificar, decifrar, assinar e verificar no próprio local e com a maioria dos aplicativos, sem necessidade explícita do usuário copiar e colar.
- **Eliminação (“Wiping”) de Espaço Livre.** PGPtools agora pode eliminar todo o espaço livre em seus discos.
- **Eliminação Aperfeiçoada.** Tanto a eliminação de arquivos quanto volumes agora usam um conjunto significativamente melhorado de padrões para múltiplas eliminações, especialmente afinado para os tipos de mídias usados pelos computadores de hoje.

- **Key Splitting (Divisão de Chave).** Qualquer chave privada de alta segurança pode ser dividida em múltiplas partes entre vários “proprietários” usando um processo criptográfico conhecido como “Blakely-Shamir splitting”.
- **PGPdisk ADK.** Uma chave adicional de decifragem (“Additional Decryption Key”, ADK) pode ser especificada para acesso a todos os novos PGPdisks, criados com uma configuração “instalação cliente” de PGP. Isto utiliza um novo suporte a chaves públicas em PGPdisk.

Novos recursos de PGPdisk

- **Suporte a Chaves Públicas.** Uma chave pública ou múltiplas chaves públicas agora podem ser configuradas para abrir um PGPdisk. Este suporte está integrado a PGP 6.0 e seus chaveiros. Por exemplo, se Bob quer dar à sua esposa Mary acesso a seu PGPdisk, ele pode dar acesso a Mary adicionando a chave pública dela ao PGPdisk. A chave para o disco será codificada para a chave de Mary.
- **Novo Assistente de Disco (“Disk Wizard”).** O processo de se criar um PGPdisk foi simplificado graças ao novo Assistente de Disco, que irá guiá-lo através do processo passo a passo.
- **Suporte a Windows NT.** PGPdisk agora executa em Windows NT 4.0 além de Windows 95, 98, e MacOS.

Usando PGP

PGP é um aplicativo de segurança que permite que você e seus colegas de trabalho troquem ou armazenem informações com segurança, de forma que ninguém mais possa lê-las.

Um dos modos mais convenientes de usar PGP é através de um dos aplicativos populares de email suportados pelos plug-ins de PGP. Com estes plug-ins, você pode codificar e assinar e também decifrar e verificar suas mensagens, enquanto você está escrevendo e lendo seu email, com o simples apertar de um botão.

Se você está usando um aplicativo de email que não é suportado pelos plug-ins, você pode facilmente codificar o texto da mensagem usando PGPTray. Além disso, se você precisar codificar ou decifrar arquivos anexados, você pode fazê-lo diretamente através da Área de Transferência (“Clipboard”) de Windows, escolhendo a opção de menu apropriada. Você também pode usar PGP para codificar e assinar arquivos no disco rígido de seu computador para armazenamento seguro, eliminar arquivos com segurança de seu disco rígido, e eliminar o espaço livre em disco, de forma que dados sensíveis não possam ser recuperados com softwares de recuperação de disco.

Uma rápida visão geral

PGP está baseado em uma tecnologia de criptografia amplamente conhecida, conhecida como *criptografia por chave pública*, onde duas chaves complementares, chamadas de *par de chaves*, são usadas para manter comunicações seguras. Uma das chaves é designada como uma *chave privada*, a qual só você tem acesso, e a outra é uma *chave pública* que você pode trocar livremente com outros usuários de PGP. Tanto a chave privada quanto a pública são armazenadas em arquivos de “chaveiro”, que são acessível pela janela de PGPkeys. É desta janela que você executa todas as funções de administração das chaves.

Para uma visão mas aprofundada da tecnologia de criptografia de PGP, veja “*Uma Introdução à Criptografia*”, que está incluída com o produto.

Passos Básicos para usar PGP

Esta seção dá uma rápida olhada nos procedimentos que você normalmente segue no uso de PGP. Para detalhes sobre quaisquer destes procedimentos, veja os capítulos apropriados neste livro.

1. Instale PGP em seu computador. Veja o *Guia de Instalação de PGP* incluído com o produto para instruções completas de instalação.

2. Crie um par de chaves, privada e pública.

Antes de você possa começar a usar PGP, você precisa gerar um par de chaves. Um par de chaves PGP é composto de uma chave privada, a qual só você tem acesso, e uma chave pública, que você pode copiar e disponibilizar livremente a todos com quem você troca informações.

Você tem a opção de criar um novo par de chaves imediatamente após terminar a instalação de PGP, ou você pode fazê-lo a qualquer hora abrindo o programa GPGkeys.

Para mais informações sobre como criar um par de chaves privado e público, veja [“Criando um par de chaves”](#).

3. Troque chaves públicas com outros.

Depois que você criou um par de chaves, você pode começar a corresponder-se com outros usuários de PGP. Você precisará de uma cópia da chave pública deles e eles precisarão da sua. Sua chave pública é apenas um bloco de texto, portanto é bastante fácil trocar chaves com alguém. Você pode incluir sua chave pública em uma mensagem de email, copiá-la para um arquivo, ou postá-la em um servidor público ou privado de chaves, onde qualquer um pode adquirir uma cópia quando eles precisarem.

Para mais informações sobre como trocar chaves públicas, veja [“Distribuindo sua chave pública”](#) e [“Obtendo as chaves públicas de outros”](#).

4. Valide as chaves públicas.

Uma vez que você obteve uma cópia da chave pública de alguém, você pode adicioná-la a seu chaveiro público. Você deve conferir para ter certeza de que a chave não foi falsificada e que realmente pertence ao dono pretendido. Você faz isto comparando a “impressão digital” única em sua cópia da chave pública de alguém com a “impressão digital” na chave original daquela pessoa. Quando você tiver certeza de que possui uma chave pública válida, você a assina para indicar que você sabe que esta chave é segura de se usar. Além disso, você pode conceder ao dono da chave um nível de confiança que indica o quanto você confia naquela pessoa para atestar a autenticidade da chave pública de outra pessoa.

Para mais informações sobre validação de suas chaves, veja [“Verificando o autenticidade de uma chave”](#).

5. Codifique e assine seu email e arquivos.

Depois que você gera seu par de chaves e trocou chaves públicas, você pode começar

a codificar e assinar mensagens de email e arquivos.

- Se você está usando um aplicativo de email suportada pelos plug-ins, você pode codificar e assinar suas mensagens selecionando as opções apropriadas na barra de ferramentas de seu aplicativo.
- Se sua aplicativo de email não é suportada pelos plug-ins, você pode executar as funções apropriadas de PGPTray. Você também pode codificar e assinar arquivos usando PGPtools antes de anexá-los a seu email. Codificá-los assegura que só você e seus destinatários intencionais podem decifrar o conteúdo dos arquivos; assiná-los assegura que quaisquer alterações estarão visíveis.

Para mais informações sobre como codificar e assinar informações, veja [“Codificando e assinando email”](#).

6. Decifre e verifique seu email e arquivos.

Quando alguém envia a você dados codificados, você pode decodificar o conteúdo e verificar qualquer assinatura adicionada para ter certeza de que os dados foram originados pelo remetente alegado e que não foram alterados.

- Se você está usando um aplicativo de email que suporta os plug-ins, você pode decifrar e verificar suas mensagens selecionando as opções apropriadas na barra de ferramentas de seu aplicativo.
- Se sua aplicativo de email não é suportada pelos plug-ins, você pode copiar a mensagem para a Área de Transferência e executar as funções apropriadas de lá. Se você quer decifrar e verificar anexos, você pode fazer isso pela Área de Transferência de Windows. Você também pode decifrar arquivos codificados armazenados em seu computador, e verificar arquivos assinados para assegurar-se de que eles não foram falsificados.

Para mais informações sobre como decifrar e verificar dados, veja [“Decifrando e verificando email”](#).

7. Elimine arquivos.

Quando você precisa apagar um arquivo permanentemente, você pode usar o recurso de Eliminação (“Wipe”) para assegurar-se de que o arquivo fique irrecuperável. O arquivo é imediatamente sobrescrito, de forma que não possa ser recuperado usando

softwares de recuperação de disco.

Para mais informações sobre eliminação de arquivos, veja [“Usando PGP Wipe para apagar arquivos”](#).

Este capítulo explica como executar PGP e provê uma visão rápida dos procedimentos que você seguirá regularmente usando o produto. Também contém uma tabela com os ícones usados com PGPkeys.

Executando PGP

PGP trabalha sobre dados gerados por outros aplicativos. Portanto, as funções apropriadas de PGP foram projetadas de forma a estarem imediatamente disponíveis a você, baseadas na tarefa que você está executando em um determinado momento. Há quatro modos primários para usar PGP:

- Através da bandeja de sistema, ou “system tray” (PGPTray)
- Através dos aplicativos de email suportados (plug-ins PGP de email)
- Através do menu “Arquivo” do Windows Explorer
- Através da barra de ferramentas de PGPTools

Usando PGP pela bandeja de sistema

Você pode ter acesso a muitas das principais funções de PGP clicando o ícone da fechadura, que normalmente está localizado na bandeja de sistema (“system tray”), e escolhendo então o item de menu apropriado (se você não achar este ícone em sua bandeja de sistema, execute PGPTray através do menu Iniciar).

Executando funções de PGP pela Área de Transferência

Você notará que muitas das opções na bandeja de sistema se referem a funções PGP que você executa da Área de Transferência de Windows. Se você está usando um aplicativo de email que não é suportado pelos plug-ins PGP, ou se você está trabalhando com texto gerado por algum outro aplicativo, você executa sua codificação/decifração e assinatura/verificação pela Área de Transferência de Windows.

Por exemplo, para codificar ou assinar texto, você o copia de seu aplicativo para a Área de Transferência, codifica e assina usando a função PGP apropriada, então o cola em seu aplicativo antes de enviá-lo aos destinatários intencionados. Quando você recebe uma mensagem de email codificada ou assinada, você simplesmente faz o processo contrário e copia o texto codificado, conhecido como *texto cifrado*, de seu aplicativo para a Área de Transferência, decifra e verifica as informações, e então vê o conteúdo. Depois que você viu a mensagem decifrada, você pode decidir se guarda a informação ou a mantém em sua forma codificada.

Abrindo a janela de PGPkeys

Quando você escolhe “Launch PGPkeys” do menu pop-up de PGP, abre-se a janela de PGPkeys, mostrando os pares de chave privados e públicos que você criou para você mesmo, e também quaisquer chaves pública de outros usuários que você adicionou a seu chaveiro público (se você não criou um novo par de chaves ainda, o “PGP Key Generation Wizard” o conduzirá pelos passos necessários. Porém, antes de passar pelo processo de criar um novo par de chaves, você deveria ver o [Capítulo 3](#) para detalhes completos sobre as várias opções).

Da janela de PGPkeys você pode criar novos pares de chaves e pode administrar todas as outras chaves. Por exemplo, é dali que você examina os atributos associados a uma chave em particular, especifica o grau de confiança que você tem que a chave de fato pertence ao dono alegado, e indica o quanto você confia no dono da chave para atestar a autenticidade das chaves de outros usuários. Para um explicação completa das funções de administração de chaves que você executa da janela de PGPkeys, veja o [Capítulo 6](#).

Configurando preferências de PGP

Quando você escolhe “PGP Preferences” do menu pop-up de PGP, você tem acesso à caixa de diálogo “PGP Preferences”, na qual você especifica configurações que afetam como o PGP programa funções baseadas em seu ambiente de computação. Clicando a aba apropriada, você pode avançar às configurações de preferência que você quer modificar. Para uma explicação completa destas configurações, veja o [Capítulo 6](#).

Obtendo Ajuda

Quando você escolhe “Help” do menu ou janela de PGP, você tem acesso ao sistema de ajuda de PGP, o qual provê uma visão geral e instruções para todos os procedimentos que você possivelmente executará. Muitas das caixas de diálogo também têm ajuda sensível ao contexto, que você acessa clicando o ponto de interrogação no canto direito da janela e apontando então à área de interesse na tela. Uma pequena explicação aparece.





Finalizando PGP


Por padrão, o programa PGPTray é executado sempre que você inicializa seu computador, como indicado pelo ícone da fechadura exibido na bandeja do sistema. Se por alguma razão você precisa finalizar PGPTray, você pode fazê-lo escolhendo “Exit PGPTray” no menu pop-up de PGP.

Usando PGP através dos aplicativos de email suportados

Se você tem um destes populares aplicativos de email suportados pelos plug-ins de PGP, você pode acessar as funções necessárias de PGP clicando os botões apropriados na barra de ferramentas de seu aplicativo:

- Qualcomm Eudora
- Microsoft Exchange
- Microsoft Outlook
- Microsoft Outlook Express
- Novell Groupwise (disponível separadamente)


Por exemplo, você clica o ícone de envelope e fechadura () para indicar que você quer codificar sua mensagem, e o ícone da caneta e papel () para indicar que você quer assinar sua mensagem. Algumas aplicações também têm um ícone de uma fechadura e broca () que o permite fazer ambos ao mesmo tempo. Quando você recebe um email de outro usuário de PGP, você decifra a mensagem e verifica a assinatura digital da pessoa clicando a fechadura aberta e envelope, ou selecionando “Decrypt/Verify” do PGPmenu ()

Você também pode acessar a qualquer hora a janela de PGPkeys enquanto escrevendo ou recebendo seus emails clicando o botão PGPkeys () em alguns plug-ins.

Usando PGP/MIME


Se você está usando um aplicativo de email com um dos plug-ins que suporta o padrão PGP/MIME, e você está se comunicando com outro usuário cujo aplicativo de email também suporta este padrão, vocês podem automaticamente codificar e decifrar suas

mensagens de email e qualquer arquivo anexado quando você enviar ou recuperar seu email. Tudo que você tem que fazer é ativar a criptografia PGP/MIME e funções de assinatura na caixa de diálogo “Preferences” (Preferências) de PGP. Quando você receber email de alguém que usa o recurso PGP/MIME, as mensagens chegam com um ícone anexado à janela de mensagem, o que indica que a mesma usa codificação PGP/MIME.

Para decifrar o texto e arquivos anexos em emails encapsulados por PGP/MIME e para verificar qualquer assinatura digital, basta você clicar duas vezes no ícone com a fechadura e broca (). Anexos ainda estarão codificados se PGP/MIME não for usado, mas o processo de decifração normalmente é envolvido mais para o destinatário.

Usando PGP através de PGTools

Se você está usando um aplicativo de email que não tem suporte de um plug-in, ou se você quer executar funções de PGP de dentro de outras aplicações, você pode codificar e assinar, decifrar e verificar, ou eliminar seguramente mensagens e arquivos diretamente da janela de PGTools. Você pode abrir a janela de PGTools da seguinte forma:

- Clique Iniciar → Programas → PGP → PGTools.
- Dê um clique duplo no ícone de PGTools () na bandeja do sistema.

Quando a janela de PGTools ([Figura 2-1](#)) se abre, você pode começar seu trabalho de codificação.



Figura 2-1. Janela de PGTools

Se você está trabalhando com texto ou arquivos, você pode codificar, decifrar, assinar, e verificar selecionando o texto ou arquivo e arrastando-o sobre o botão apropriado na janela de PGTools.

Se você está trabalhando com arquivos, clique no botão apropriado na janela de PGTools para escolher um arquivo ou selecionar a Área de Transferência.

Usando PGP através do Windows Explorer

Você pode codificar e assinar ou pode decifrar e verificar arquivos como documentos de processadores de texto, planilhas eletrônicas e clipes de vídeo diretamente do Windows Explorer. Se você não está usando um aplicativo de email como Qualcomm Eudora que

suporta o padrão de PGP/MIME, ou um aplicativo como Exchange ou Outlook que não requerem PGP para codificar ou assinar arquivos, você deve usar este método para anexar arquivos que você quer enviar junto com suas mensagens de email. Você também poderia querer codificar e decifrar arquivos que você armazena em seu próprio computador para impedir que outros tenham acesso a eles.

Para acessar funções de PGP de dentro do Windows Explorer, escolha a opção apropriada no submenu de PGP do menu Arquivo. As opções que aparecem dependem do estado atual do arquivo que você selecionou. Se o arquivo ainda não foi codificado ou assinado, então as opções para executar estas funções aparecem no menu. Se o arquivo já foi codificado ou assinado, então opções para decifrar e verificar o conteúdo do arquivo são exibidos.

Selecionando Destinatários

Quando você envia email a alguém que possui um aplicativo de email suportado pelos plug-ins de PGP, o endereço de email do destinatário determina quais chaves usar quando codificando o conteúdo. Porém, se você inserir um nome de usuário ou endereço de email que não correspondam a quaisquer das chaves em seu chaveiro público, ou se você está codificando via Área de Transferência ou Windows Explorer, você deverá selecionar manualmente a chave pública do destinatário usando a caixa de diálogo “Key Selection” (Seleção de Chave) de PGP. Para selecionar a chave pública de um destinatário, simplesmente arraste o ícone representando a chave dele na caixa de lista de destinatários e então clique OK.

Para instruções completas sobre como codificar e assinar, e decifrar e verificar email, veja o Capítulo 4. Se você quer codificar arquivos para armazenar em seu disco rígido, ou enviar como anexos de email, veja o Capítulo 5.

Tomando Atalhos









Embora você irá achar que PGP é fácil de usar, vários atalhos estão disponíveis para lhe ajudar a realizar suas tarefas de codificação ainda mais rapidamente. Por exemplo, enquanto você está administrando suas chaves na janela de PGPkeys, você pode apertar o botão direito do mouse para realizar todas as funções de PGP necessárias, ao invés de acessá-las da barra de menu. Você também pode arrastar um arquivo que contém uma chave na janela de PGPkeys para adicioná-la a seu chaveiro.

Atalhos de teclado também estão disponíveis para a maioria das operações de menu. Estes atalhos de teclado são mostrados em todos os menus de PGP, e outros atalhos são descritos em contexto ao longo deste manual.

Definições dos Ícones de PGPkeys

Ícones da Barra de Menu de PGPkeys

A seguinte tabela mostra todos os ícones usados na barra de menu de PGPkeys, juntamente com uma descrição das funções dos mesmos.

Ícone	Função
	Executa o assistente para geração de chave (“PGP Key Generation Wizard”). Clique este botão para criar um novo par de chaves.
	Revoga a assinatura ou chave atualmente selecionada. Clique este botão para desabilitar uma chave ou revogar uma assinatura. Revogar uma chave previne qualquer um de codificar dados para ela.
	Permite que você assine a chave atualmente selecionada. Assinando a chave, você está certificando que a chave e o ID de usuário pertencem ao usuário identificado.
	Apaga o item atualmente selecionado. Clique este botão para remover uma chave, assinatura, ou ID fotográfico.
	Abre a janela de procura por chave (“Key Search”) que lhe permite procurar chaves em chaveiros locais e servidores distantes.
	Envia a chave atualmente selecionada ao servidor. Clique este botão para enviar sua chave para o servidor de Certificados ou de domínio.
	Atualiza a chave atualmente selecionada através de um servidor de Certificados ou de domínio. Clique este botão para importar chaves de um servidor de Certificados ou de domínio para seu chaveiro.
	Exibe a caixa de diálogo “Properties” para a chave atualmente selecionada. Clique este botão para ver as propriedades gerais e de subchaves (“subkeys”) para uma

chave.



Permite que você importe chaves de um arquivo para seu chaveiro.



Permite que você exporte a chave selecionada para um arquivo.

Ícones de janelas de PGPkeys

A tabela a seguir mostra todos os mini-ícones usados na janela PGPkeys, juntamente com uma descrição do que eles representam.

Ícone	Descrição
	Uma chave dourada e um usuário representam seu par de chaves Diffie-Hellman/DSS, que consiste de sua chave privada e sua chave pública.
	Uma chave dourada simples representa uma chave pública Diffie-Hellman/DSS.
	Uma chave cinza e um usuário representam seu par de chaves RSA, que consiste de sua chave privada e sua chave pública.
	Uma chave cinza simples representa uma chave pública RSA.
	Quando um par de chaves ou chave está escurecido, as chaves estão temporariamente indisponíveis para codificar e assinar. Você pode desabilitar uma chave através da janela de PGPkeys, o que previne que chaves raramente usadas atrapalhem a caixa de diálogo de Seleção de Chave (“Key Selection”).



Este ícone indica que um ID fotográfico de usuário (“Photographic User ID”) está acompanhado da chave pública.



Uma chave com um X vermelho indica que a chave foi revogada. Usuários revogam suas chaves quando elas não são mais válidas ou foram comprometidas de alguma forma.



Uma chave com um relógio indica que a chave expirou. A data de expiração de uma chave é estabelecida quando a chave é criada.



Um envelope representa o possuidor da chave e lista os nomes do usuário e endereços de email associados à chave.



Um círculo cinza indica que a chave é inválida.



Um círculo verde indica que a chave é válida. Um círculo vermelho adicional na coluna ADK (“Additional Decryption Key”) indica que a chave possui uma Chave Adicional de Decodificação associada; um círculo cinza adicional na coluna ADK indica que a chave não possui uma ADK associada.



Um círculo verde e um usuário indica que você possui a chave, e que sua confiabilidade está implícita.



Um lápis ou caneta de pena indicam as assinaturas dos usuários de PGP que atestaram a autenticidade da chave. Uma assinatura com um X vermelho através dela indicam uma assinatura revogada. Uma assinatura com um ícone escurecido de um lápis indica uma assinatura ruim ou inválida. Uma assinatura com uma seta azul próxima a ela indica que é exportável.



Uma barra vazia indica uma chave inválida ou um usuário não confiado.



Uma barra meio-cheia indica uma chave marginalmente válida ou um usuário marginalmente confiado.



Uma barra listada indica uma chave válida que você possui e é implicitamente confiável, seja qual forem as assinaturas na chave.



Uma barra cheia indica uma chave completamente válida ou um usuário completamente confiado.

Este capítulo descreve como gerar o par de chaves pública e privada que você precisa para se corresponder com outros usuários de PGP. Também explica como distribuir sua chave pública e como obter as chaves públicas de outros, de forma que você possa começar a trocar email privado e autenticado.

Conceitos chave

PGP é baseado em um sistema de *criptografia por chave pública* amplamente aceito e altamente confiável, como mostrado na [figura 3-1](#), pela qual você e outros usuários de PGP geram um par de chaves que consiste em uma chave privada e uma chave pública. Como seu nome implica, só você tem acesso à sua chave privada, mas para corresponder com outros usuários de PGP você precisa de uma cópia da chave pública deles e eles precisam de uma cópia da sua. Você usa sua chave privada para assinar as mensagens de email e arquivos anexos que você envia para outros, e para decifrar as mensagens e arquivos que eles enviam a você. Reciprocamente, você usa as chaves públicas de outros para enviar a eles emails codificados e para verificar as assinaturas digitais deles.





Figura 3-1. Diagrama de Criptografia por Chave Pública

Criando um Par de Chaves

A menos que você já tenha feito isso antes usando outra versão de PGP, a primeira coisa que você precisa fazer antes de enviar ou receber um email codificado e assinado é criar um novo par de chaves. Um par de chaves consiste em duas chaves: uma chave privada que só você possui, e uma chave pública que você distribui livremente para as pessoas com quem você se corresponde. Você gera um novo par de chaves na janela PGPkeys usando o “PGP Key Generation Wizard”, que o guiará durante o processo.

NOTA: Se você está atualizando PGP de uma versão mais nova, você provavelmente já tem gerada uma chave privada e já distribuiu sua respectiva chave pública para aqueles com quem você se corresponde. Neste caso você não tem que fazer um novo par de chaves (como descrito na próxima seção). Ao invés, você especifica a localização de suas chaves quando você executar o programa PGPkeys. Você pode ir para o painel “Files” da caixa de diálogo “Preferences” e localizar seus arquivos de chaveiro a qualquer hora.

Para Criar um Novo Par de Chaves

1. Abra a janela PGPkeys. Você pode abri-la assim:
 - Clicando Iniciar --> Programas --> PGP --> PGPkeys
 - Clicando no ícone de PGPTray () na bandeja do sistema, e então “PGPkeys”.
2. Clicando () na barra de ferramentas da seu aplicativo de email.

A janela de PGPkeys se abre, como mostrado na [figura 3-2](#).

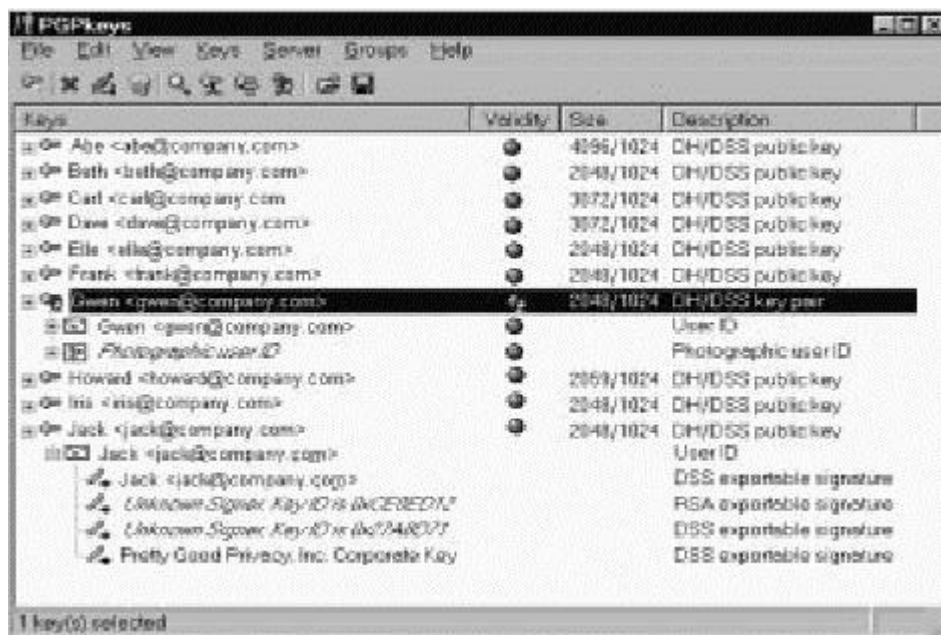



Figura 3-2. A janela PGPkeys

3. Clique () na barra de ferramentas de PGPkeys. O PGP Key Generation Wizard mostra algumas informações introdutória na primeira tela.
4. Quando você tiver terminado de ler estas informações, clique em “Next” para avançar à próxima caixa de diálogo.

O PGP Key Generation Wizard lhe pede para entrar seu nome e endereço de email.

5. Entre seu nome na primeira linha e seu endereço de email na segunda linha.

Não é absolutamente necessário entrar com seu nome real ou até mesmo seu endereço de email. Porém, usando seu nome real torna mais fácil para outros identificá-lo como dono de sua chave pública. Também, usando seu endereço de email correto, você e outros podem aproveitar a característica do plug-in que automaticamente procura a chave apropriada em seu chaveiro atual quando você envia correio a um destinatário em particular. Chaves de Assinaturas Corporativas e Chaves Adicionais de Decodificação não têm nenhum uso para um endereço de email porque eles não representam indivíduos.

6. Clique “Next” para avançar à próxima caixa de diálogo. O Assistente de Geração de Chave lhe pede que selecione um tipo chave.
7. Selecione um tipo de chave, Diffie-Hellman/DSS ou RSA e então clique Avançar.

Versões anteriores de PGP usam uma tecnologia mais antiga chamada RSA para

gerar chaves. Com PGP Versão 5.0 e superiores, você tem a opção de criar um novo tipo de chave, baseado na variante de Elgamal melhorada da tecnologia Diffie-Hellman.

- Se você planeja se corresponder com pessoas que ainda estão usando chaves RSA, você pode querer gerar um par de chaves RSA que é compatível com versões anteriores do programa.
- Se você planeja se corresponder com pessoas que têm PGP Versão 5.0 ou superior, você pode tirar proveito da nova tecnologia e gerar um par de chaves Diffie-Hellman/DSS.
- Se você quer trocar email com todos os usuários de PGP, faça um par de chaves RSA e um par de chaves Diffie-Hellman/DSS, então use o par apropriado, dependendo da versão de PGP usado pelo destinatário. Você deve criar um par de chaves separado para cada tipo de chave da que você precisar.

NOTA: Se sua versão de PGP não suporta RSA, este passo pode não estar disponível a você. Para mais informações sobre suporte RSA, veja o arquivo LeiaMe que acompanha o produto.

8. O PGP Key Generation Wizard lhe pede para especificar um tamanho para suas novas chaves.

Selecione um tamanho para as chaves entre 768 e 3072 bits, ou entre um tamanho personalizado entre 768 e 4096 bits.

NOTA: Um tamanho personalizado para as chaves pode levar muito tempo para serem gerados, dependendo da velocidade do computador que você está usando.

O tamanho das chaves corresponde ao número de bits usados para construir sua chave digital. Quanto maior a chave, menores chances alguém terá para quebrá-las, mas muito mais tempo levará para executar os processos de decifração e codificação. Você precisará encontrar um ponto de equilíbrio entre a conveniência de executar as funções de PGP mais depressa com uma chave menor e o maior nível de segurança provido por uma chave maior. A menos que você esteja trocando informações extremamente sensíveis, que seria de interesse suficiente para que alguém estivesse disposto a montar um ataque criptográfico caro e demorado para lê-las, você está seguro usando uma chave composta por 1024 bits.

NOTA: Quando criando um par de chaves Diffie-Hellman/DSS, o tamanho da porção DSS da chave é menor que ou igual ao tamanho da porção Diffie-Hellman da chave, e está limitado a um tamanho máximo de 1024 bits.

9. Clique “Next” para avançar ao próximo painel. O PGP Key Generation Wizard lhe pede que indique quando o par de chaves irá expirar.
10. Indique quando você quer que suas chaves expirem. Você pode usar tanto a opção padrão, que é “Nunca” (“Never”), ou pode entrar uma data específica depois da qual as chaves expirarão. Uma vez que você criar um par de chaves e distribuir sua chave pública para o mundo, você provavelmente continuará usando as mesmas chaves daquele ponto em diante. Porém, sobre certas condições você pode querer criar um par de chaves especial, que você planeja usar por apenas um período limitado de tempo. Neste caso, quando a chave pública expira, já não pode ser usada por alguém para codificar mensagens para você, mas poderá ainda ser usada para verificar sua assinatura digital. Semelhantemente, quando sua chave privada expira, ainda pode ser usada para decifrar mensagens que foram enviadas a você antes de sua chave pública expirar, mas já não podem ser usadas para assinar mensagens para outros.
11. Clique “Next” para seguir à próxima tela. O Assistente de Geração de Chaves lhe pede que entre uma “frase-senha” (passphrase).
12. Na caixa de diálogo “Passphrase”, entre a série de caracteres ou palavras que você quer usar para manter acesso exclusivo à sua chave privada. Para confirmar sua entrada, aperte a tecla “Tab” para avançar à próxima linha, então entre a mesma frase-senha novamente.

Normalmente, como um nível adicional de segurança, os caracteres que você entra para a frase-senha não aparecem na tela. Porém, se você está seguro que ninguém está vendo, e você gostaria de ver os caracteres de sua frase-senha enquanto você os digita, desmarque a caixa “Hide Typing”.

NOTA: Sua frase-senha deve conter várias palavras e podem incluir espaços, números, e caracteres de pontuação. Escolha algo que você possa se lembrar facilmente, mas que outros não sejam capazes de adivinhar. A frase-senha é “sensível a caso”, o que significa que faz distinção entre maiúsculas e minúsculas. Quanto mais longa sua frase-senha, e maior a variedade de caracteres que contenha, mais segura ela é. Frases-senhais fortes incluem letras maiúsculas e minúsculas, números, pontuação e espaços, mas são mais fáceis de serem esquecidas. Veja [“Criando um frase-senha que você vai se lembrar”](#), para mais informações sobre como escolher uma frase-senha.

ADVERTÊNCIA: Ninguém, inclusive a Network Associates, pode recuperar uma frase-senha esquecida.

13. Clique “Next” para iniciar o processo de geração da chave.

O Assistente de Geração de Chave indica que está ocupado gerando sua chave.

Se você entrou uma frase-senha inadequada, uma mensagem de advertência aparece antes das chaves serem geradas e você tem a escolha de aceitar a frase-

senha ruim ou entrar uma mais segura antes de continuar. Para mais informações sobre frases-senha, veja [“Criando um frase-senha que você vai se lembrar”](#).

Se não houver suficiente informação aleatória sobre a qual a chave será construída, a caixa de diálogo “Random Data” aparece. Como instruído na caixa de diálogo, mova seu mouse pela tela e pressione uma série de teclas aleatórias até que a barra de progresso esteja completamente preenchida. Seus movimentos do mouse e teclas pressionadas geram informações aleatórias que são necessárias para se criar um par de chaves único.

NOTA: PGPkeys junta dados aleatórios continuamente a partir de muitas fontes no sistema, inclusive posição do mouse, temporizadores, e pressionamento de teclas. Se a caixa de diálogo de Dados Aleatórios não aparecer, isto indica que PGP já coletou todos os dados aleatórios que precisava para criar o par de chaves.

Depois que o processo de geração da chave começa, pode demorar um tempo para gerar as chaves. De fato, se você especificar um tamanho diferente dos valores padrão para uma chave Diffie-Hellman/DSS, a opção de geração de chave rápida não é usada e pode levar horas para gerar sua chave com tamanhos maiores. Eventualmente o Assistente de Geração de Chave indicará que o processo de geração das chaves foi completado.

14. Clique “Next” para seguir à próxima tela.

O Assistente de Geração de Chaves indica que você gerou com sucesso um novo par de chaves e pergunta se você quer enviar sua chave pública para um Servidor de Chaves.

15. Especifique se você quer enviar sua nova chave pública para o servidor, e então clique “Next” (o servidor padrão é especificado em suas preferências).

Quando você envia sua chave pública ao Servidor de Chaves, qualquer um que tiver acesso àquele Servidor de Chaves pode obter uma cópia de sua chave quando precisar. Para detalhes completos, veja [“Distribuindo sua chave pública”](#). Quando o processo de geração da chave estiver completo, a tela final aparece.

16. Clique “Done”.

Um par de chaves que representam suas chaves recentemente criadas aparece na janela de PGPkeys. Neste momento você pode examinar suas chaves, conferindo as propriedades delas e os atributos associados às suas chaves; você também pode querer adicionar outros endereços de email que pertençam a você. Veja [“Adicionando um novo nome de usuário ou endereço para um par de chaves”](#), para detalhes sobre como adicionar um novo nome de usuário à sua chave.

Criando uma Frase-Senha Que Você Vai Se Lembrar

Codificar um arquivo e depois se achar impossibilitado de decifrá-lo é uma dolorosa lição para aprender a escolher uma frase-senha da qual você se lembrará. A maioria das aplicações requer uma senha entre três e oito letras. Uma senha de uma só palavra é vulnerável a um “ataque de dicionário”, que consiste em fazer um computador tentar todas as palavras de um dicionário até achar sua senha. Para proteger-se contra esta maneira de ataque, é amplamente recomendado que você crie uma frase que inclua uma combinação de letras maiúsculas e minúsculas, números, marcas de pontuação, e espaços. Isto resulta em uma senha mais forte, mas obscura, que é improvável que se lembre facilmente. Nós não recomendamos que você use uma frase-senha de uma só palavra.

Uma frase-senha é menos vulnerável a um ataque de dicionário. Isto é realizado facilmente usando várias palavras em sua frase-senha, ao invés de tentar contrariar um ataque de dicionário inserindo arbitrariamente montes de caracteres engraçados não-alfabéticos, que têm o efeito de fazer sua frase-senha muito fácil de se esquecer e poder conduzir a uma perda desastrosa de informações porque você não pode decifrar seus próprios arquivos. Porém, a menos que a frase-senha que você escolher seja algo que é facilmente gravável em sua memória de longo prazo, é pouco provável que você irá se lembrar dela literalmente. É provável que a escolha de uma frase no calor de um determinado momento resulte em seu esquecimento por completo. Escolha algo que já está gravado em sua memória de longo prazo. Talvez um provérbio tolo que você ouviu anos atrás e que de alguma maneira ficou em sua mente por todo esse tempo. Não deve ser algo que você repetiu recentemente a outros, nem uma frase famosa, porque você quer que ela seja dura para um atacante sofisticado adivinhar. Se já estiver profundamente enraizado em sua memória de longo prazo, você provavelmente não a esquecerá.

Claro que, se você está despreocupado o bastante para escrever sua frase-senha e grudá-la no seu monitor ou guardá-la dentro da gaveta de sua escrivaninha, não importa o quê você escolherá.

Adicionando um ID fotográfico à sua chave

Você pode incluir um ID fotográfico de usuário (“Photographic User ID”) em sua chave Diffie-Hellman/DSS.

ADVERTÊNCIA: Embora você possa ver o ID fotográfico que acompanha a chave de alguém para verificação, você sempre deve conferir e comparar as “impressões digitais”. Veja [“Verificando a chave pública de alguém”](#) para mais informações sobre autenticação.

Para adicionar sua fotografia à sua chave:

1. Abra o programa PGPkeys.
2. Selecione seu par de chaves e então clique “Add Photo” (Adicionar Fotografia) no menu “Keys”.

A caixa de diálogo “Add Photo” abre-se, como mostrado na [Figura 3-3](#).



Figura 3-3. A caixa de diálogo “Add Photo”.

3. Arraste ou cole sua fotografia sobre a caixa de diálogo “Add Photo” ou procure-a clicando o botão “Select File”.

NOTA: A fotografia deve ser um arquivo .JPG ou .BMP. Para qualidade máxima da fotografia, corte a figura para 120x144 antes de adicioná-la à caixa de diálogo “Add Photo”. Se você não fizer isto, PGP irá colocar a foto nesta escala para você.

4. Clique OK.

A caixa de diálogo “Passphrase” abre-se, como mostrado na [Figura 3-4](#).

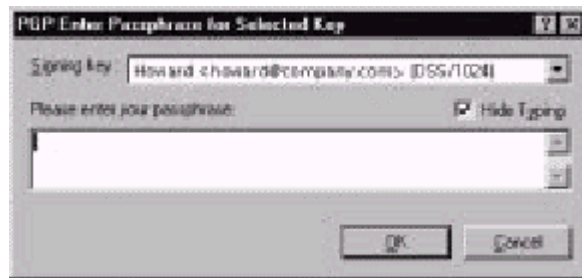


Figura 3-4. A caixa de diálogo “Passphrase”

5. Entre sua frase-senha no espaço provido, então clique OK.

Seu ID fotográfico de usuário é adicionado à sua chave pública e é listado na janela de PGPkeys. Você pode enviar sua chave agora para o servidor. Veja [“Para enviar sua chave pública a um servidor de chaves”](#), para instruções adicionais.

Para substituir seu ID fotográfico


1. Abra o programa PGPkeys.
2. Selecione seu par de chaves
3. Selecione a fotografia que você quer substituir.
4. Escolha “Delete” no menu “Edit”.
5. Adicione seu novo ID fotográfico usando as instruções mostradas em [“Para adicionar sua fotografia à sua chave”](#).

Criando novas subchaves

Cada chave Diffie-Hellman/DSS é na verdade composta de duas chaves: uma chave DSS, usada para assinar, e uma subchave Diffie-Hellman para codificar. PGP Versão 6.0 permite criar e revogar novas chaves de codificação sem sacrificar sua chave mestra de assinatura e as assinaturas adicionadas a ela. Um dos usos mais comuns para esta característica é para criar múltiplas chaves que são configuradas para serem usadas durante diferentes períodos da vida da chave. Por exemplo, se você cria uma chave que vai expirar em 3 anos, você também poderia criar três subchaves e poderia usar cada uma delas para um dos anos de vida da chave. Esta pode ser uma medida de segurança útil e provê um

modo automático para trocar periodicamente uma nova chave de codificação sem ter que recriar e distribuir uma nova chave pública.

Para criar novas subchaves

1. Abra o programa PGPkeys.
2. Selecione seu par de chaves e então clique “Properties” no menu “Keys”, ou clique ().

A janela de propriedades é aberta.

3. Clique a aba “Subkeys”.

A janela “subkeys” é aberta, como mostrado na [figura 3-5](#).



Figura 3-5. Página “PGP key property” (caixa de diálogo “Subkeys”)

4. Para criar uma nova subchave, clique “New”.

A janela “New Subkey” é aberta.

5. Especifique um tamanho de chave entre 768 e 3072 bits, ou insira um valor personalizado entre 768 e 4096 bits.
6. Indique a data inicial na qual você quer que sua subchave seja ativada.
7. Indique quando você deseja que sua subchave irá expirar. Você pode usar a seleção padrão, que é “Nunca” (“Never”), ou pode inserir uma data específica após a qual a subchave irá expirar.
8. Clique OK.

A janela “passphrase” aparecerá.

9. Insira sua frase-senha e então clique OK.

Sua nova subchave é listada na janela “Subkeys”.

Divisão de Chaves

Qualquer chave privada pode ser dividida em partes entre vários “proprietários”, usando um processo criptográfico conhecido como “divisão de chave de Blakely-Shamir”. Esta técnica é recomendada para chaves com segurança extremamente alta. Por exemplo, a Network Associates mantém uma chave corporativa dividida entre vários indivíduos. Sempre que eles precisam assinar com aquela chave, as partes da chave são temporariamente reunidas. Para dividir uma chave, selecione o par de chaves que será dividido e escolha “Share Split” no menu “Keys”. Então lhe será pedido que você especifique quantas pessoas diferentes serão necessárias para reunir a chave. As partes são armazenadas como arquivos ou codificados para a chave pública de um dos proprietários, ou codificados convencionalmente se o proprietário não possuir uma chave pública. Depois que a chave foi dividida, tentativas de usá-la para assinar ou decifrar irão automaticamente tentar reunir a chave. Para informações sobre como reunir uma chave dividida, veja [“Assinando e decifrando arquivos com uma chave dividida”](#).

Para criar uma chave dividida em múltiplas partes

1. Abra o programa PGPkeys.

2. Na janela de PGPkeys, crie um novo par de chaves ou selecione um par de chaves já existente que você quer dividir.
3. No menu “Keys”, clique “Share Split”.

A janela “Share Split” se abre ([Figura 3-6](#)) sobre a janela de PGPkeys.

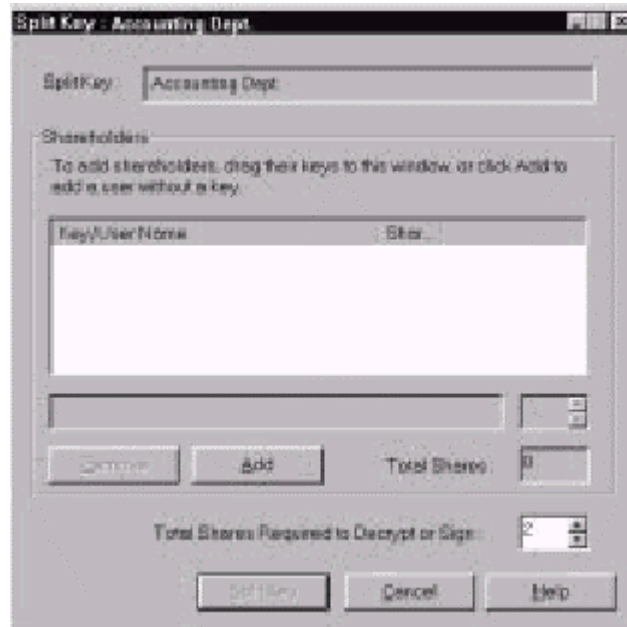


Figura 3-6. A janela “Share Split”

4. Adicione os proprietários para o par de chaves arrastando as chaves deles da janela de PGPkeys para a lista de Proprietários na caixa de diálogo “Share Split”.

Para adicionar um proprietário que possui uma chave pública, clique “Add” na caixa de diálogo “Share Split”, entre o nome da pessoa e então dê permissão à pessoa para digitar a frase-senha dela.

5. Quando todos os proprietários estiverem listados, você pode especificar o número de partes da chave que são necessários para se decifrar ou assinar com esta chave.

Na [figura 3-7](#), por exemplo, o número total de partes que compõe a chave de Administração é quatro, e o número total de partes requeridas para decifrar ou assinar é três. Isto provê um “plano de contingência” no evento de um dos proprietários estiver impossibilitado de prover a parte dele na chave, ou esquecer a frase-senha.

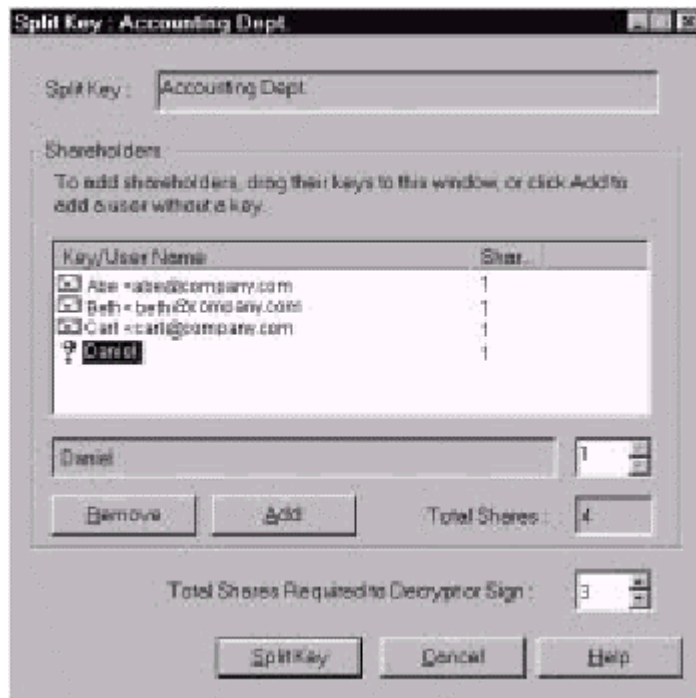


Figura 3-7. A caixa de diálogo “Share Split” (exemplo)

Por padrão, cada proprietário é responsável por uma parte. Para aumentar o número de partes que um proprietário possui, clique o nome do mesmo na lista de proprietários para exibi-lo no campo de texto logo abaixo. Digite o novo número de partes da chave ou use as setas para selecionar uma nova quantidade.

6. Clique “Split Key”.

Uma janela se abre e pede que você selecione um diretório aonde armazenar as partes.

7. Selecione o local para armazenar as partes da chave.

A janela “Passphrase” é aberta.

8. Entre a frase-senha para a chave que você quer dividir, e então clique OK.

Uma caixa de diálogo de confirmação se abre.

9. Clique “Sim” para dividir a chave.

A chave é dividida e as partes são armazenadas no local que você especificou. Cada parte da chave é armazenada com o nome do proprietário como nome de arquivo e uma extensão .SHF, como mostrado no exemplo abaixo:



10. Distribua as partes da chave para os donos, então apague as cópias locais. Uma vez que uma chave é dividida entre vários proprietários e tenta-se assinar ou decifrar com ela, isto fará PGP tentar reunir a chave automaticamente.

Para aprender a reunir uma chave dividida para assinar ou decifrar arquivos, veja [“Assinando e decifrando arquivos com uma chave dividida”](#).

Protegendo suas chaves

Uma vez você gerou um par de chaves, é sábio colocar uma cópia dela em um local seguro no caso de algo acontecer aos originais. PGP pede que você armazene uma cópia de *backup* quando você fecha o programa PGPkeys após criar um novo par de chaves.

Suas chaves privadas e suas chaves públicas são armazenadas em arquivos de chaveiro separados, os quais você pode copiar como qualquer outro arquivo para outro local em seu disco rígido ou para um disquete. Por padrão, o chaveiro privado (*secring.skr*) e o chaveiro público (*pubring.pkr*) são armazenados juntos com os outros arquivos de programa na pasta “PGP Keyrings” na pasta “PGP 6.0”, mas você pode armazenar seus *backups* em qualquer local que queira.

Quando você especifica que você quer armazenar uma cópia *backup* de suas chaves, a janela “Salvar Como” aparece e lhe pede para especifique o local para os arquivos de *backup* dos chaveiros privados e públicos que serão criados.

Além de fazer cópias de segurança de suas chaves, você deve ter cuidado especial a respeito de onde você armazena sua chave privada. Embora sua chave privada seja protegida por uma frase-senha que só você deve saber, é possível que alguém possa descobrir sua frase-senha e então poderia usar sua chave privada para decifrar seu email ou forjar sua assinatura digital. Por exemplo, alguém possa espiar sobre seus ombros e ver as teclas que você pressiona ou interceptá-las numa rede ou até mesmo via ondas de ar.

Para se prevenir de qualquer um que possa interceptar sua frase-senha de usar sua chave privada, você deve armazenar sua chave privada somente em seu próprio computador. Se seu computador está ligado a uma rede, você deve também se certificar de que seus arquivos não serão incluídos automaticamente em um *backup* completo do sistema, onde outros poderiam ganhar acesso à sua chave privada. Dada a facilidade com que computadores são acessíveis em redes, se você está trabalhando com informações extremamente sensíveis, você pode querer manter sua chave privada em um disquete que

you will be able to insert as a “common key” whenever you want to read or sign private information.

As another security precaution, consider giving a different name to the key file and storing it in a different directory from the default (the PGP folder) so it won't be so easy to find. You use the “Files” area of the “Preferences” dialog of PGPkeys to specify a name and location for your private and public keys.

Distribuído sua chave pública

After you create your keys, you need to make them available to others so they can send you encoded information and verify your digital signature.

You have three options to distribute your public key:

- Make your public key available through a Public Key Server.
- Include your public key in an email message.
- Export your public key or copy it to a text file.

Your public key is basically composed of a block of text, so it's quite easy to make it available through a Public Key Server, include it in an email message, or export it by copying it to a file. The recipient can then use any of the methods that are most convenient to add your public key to their public keyring.

Tornando sua chave pública disponível através de um Servidor de Chaves

The best way to make your public key available is to put it in a Public Key Server where anyone can access it. In this way, people can email you without having to explicitly ask for a copy of your key. It also saves you and others the trouble of maintaining a large number of public keys that you rarely use. There are many key servers in the world, including those offered by Network Associates, Inc., where you can make your key available to anyone who wants access. Your Security Manager will normally configure the parameters of your key server so that everything works correctly for your workstation.

Para enviar sua chave pública a um Servidor de Chaves

1. Conecte-se à Internet.
2. Abra o programa PGPkeys.
3. Selecione o ícone que representa a chave pública que você quer postar no Servidor de Chaves.
4. Abra o menu “Server”, então selecione o Servidor de Chaves aonde você quer postar, através do submenu “Send To”.

Uma vez que você colocar uma cópia de sua chave pública em um Servidor de Chaves, você pode dizer às pessoas que querem enviar dados codificados a você ou verificar sua assinatura digital para obter uma cópia de sua chave através do servidor. Mesmo que você não explicitamente os indique sua chave pública, eles podem adquirir uma cópia procurando o seu nome ou endereço de email no Servidor de Chaves. Muitas pessoas incluem o endereço WWW para a chave pública deles ao término das mensagens de email; na maioria dos casos o destinatário pode simplesmente clicar duas vezes o endereço para ter acesso a uma cópia da chave no servidor. Algumas pessoas chegam a colocar a Impressão Digital de PGP (“PGP Fingerprint”) delas em seus cartões de visita para verificação mais fácil.

Atualizando sua chave em um Servidor de Chaves


Se você alguma vez precisar mudar seu endereço de email, ou se você adquirir novas assinaturas, tudo o que você tem que fazer para substituir sua chave antiga é enviar uma nova cópia para o servidor; a informação é atualizada automaticamente. Porém, você deve manter em mente que Servidores de Chaves Públicas só são capazes de atualizar novas informações, e não permitirão remover nomes de usuários ou assinaturas de sua chave. Para remover assinaturas ou o nomes de usuário de sua chave, veja [“Removendo assinaturas ou nomes de usuário associados com sua chave”](#) para instruções. Se sua chave estiver comprometida, você pode revogá-la, o que diz ao mundo para não mais confiar naquela versão de sua chave. Veja o [Capítulo 6, “Gerenciando Chaves e Configurando Preferências”](#) para mais detalhes sobre como revogar uma chave.

Removendo assinaturas ou nomes de usuário associados com sua chave

Servidores de Chaves Públicas só são capazes de atualizar novas informações, e não permitirão remover nomes de usuários ou assinaturas de sua chave. Se você quer remover assinaturas ou nomes de usuários associados com sua chave pública, você deve primeiro remover sua chave do servidor.

Para apagar sua chave de um Servidor de Certificados

1. Abra a janela de PGPkeys.

2. Escolha “Search” no menu “Server”, ou clique o botão Procurar () no menu de PGPkeys.

A janela “Search” aparece.

3. Escolha o servidor onde você deseja procurar, usando o menu “Search For Keys On”.
4. Especifique seu critério de procura para localizar sua chave pública:

O padrão é ID do usuário, mas você pode clicar as setas para selecionar ID da Chave, Status da Chave, Tipo de Chave, Tamanho da Chave, Data de Criação, ou Data de Expiração. Por exemplo, você poderia procurar todas as chaves que possuam ID de Usuário de Fred.

5. Para iniciar a procura, clique “Search”.

Os resultados da procura aparecem na janela.

6. Clique com o botão direito na chave que você quer remover do servidor, então selecione “Delete”.

A janela “Passphrase” aparece.

7. Entre a frase-senha para a chave você quer remover do servidor e então clique OK.

Uma janela de confirmação aparece e a chave é removida.

8. Se você quer enviar uma chave atualizada a um Servidor de Certificados, veja [“Tornando sua chave pública disponível através de um Servidor de Chaves”](#) para instruções.

ADVERTÊNCIA: Se você apagar sua chave de um Servidor de Certificado, você deve estar ciente de que alguém que possua sua chave pública em seu chaveiro pode enviá-la novamente para o servidor. Você deve conferir o servidor periodicamente para ver se a chave reapareceu - você pode ter que apagar sua chave do servidor mais de uma vez.

Incluindo sua Chave Pública em uma Mensagem de Email

Outro método conveniente para entregar sua chave pública a alguém é incluí-la junto a uma mensagem de email.

Para Incluir sua Chave Pública em uma Mensagem de Email

1. Abra o programa PGPkeys.
2. Selecione seu par de chaves e então escolha “Copy” no menu “Edit”.
3. Abra o editor que você usa para compor suas mensagens de email, coloque o cursor na área desejada, e então clique “Paste” no menu “Edit”. Em programas de email mais novos, você pode simplesmente arrastar sua chave da janela de PGPkeys no texto da mensagem de email para transferir as informações da chave.

Quando você enviar sua chave pública para alguém, certifique-se de assinar o email. Desta forma, o destinatário pode verificar sua assinatura e ter certeza de que ninguém alterou a informação no caminho. É claro, se sua chave ainda não foi assinada por algum apresentador de confiança, destinatários de sua assinatura podem apenas ter certeza de que a assinatura é sua verificando a impressão digital de sua chave.

Exportando sua chave pública para um arquivo

Outro método de distribuir sua chave pública é copiá-la para um arquivo e então tornar este arquivo disponível para a pessoa com que você quer se comunicar.

Para exportar sua chave pública para um arquivo

Há três formas de exportar ou armazenar sua chave pública em um arquivo:

- Selecione o ícone que representa seu par de chaves na janela de PGPkeys, então clique “Export” no menu “Keys” e entre o nome do arquivo para onde você quer que sua chave seja armazenada.
- Selecione o ícone que representa seu par de chaves na janela de PGPkeys, clique “Copy” no menu “Edit”, então clique “Paste” para inserir as informações da chave em um documento texto.

NOTA: Se você estiver enviando sua chave para colegas que estão usando PCs, entre o nome com no máximo oito caracteres iniciais e três caracteres adicionais para a extensão do tipo de arquivo (por exemplo, email.txt).

Obtendo as chaves públicas de outros

Da mesma forma que você precisa distribuir sua chave pública para aqueles que querem enviar email codificados para você, ou verificar sua assinatura digital, você precisa obter a chave pública dos outros de forma que você possa enviar a eles email codificado ou verificar as assinaturas digitais deles.

Para obter a chave pública de alguém

Há três formas de se obter a chave pública de alguém:

- Obter a chave de um servidor de chaves.
- Adicionar a chave pública a seu chaveiro diretamente de uma mensagem de email.
- Importar a chave pública usando um arquivo exportado.

Chaves públicas são apenas blocos de texto, portanto são fáceis de serem adicionadas a seu chaveiro importando-as de um arquivo ou copiando-as de uma mensagem de email, e então as colando em seu chaveiro público.

Obtendo uma Chave de um Servidor de Chaves Públicas

Se as pessoas para quem você quer enviar email codificado são usuários experientes de PGP, há chance de que eles tenham colocado uma cópia de sua chave pública em um servidor de chaves. Isto torna muito conveniente para que você adquira a cópia mais atualizada da chave da pessoa desejada sempre que você quer lhe enviar um email, e também lhe poupa o trabalho de ter que armazenar muitas chaves em seu chaveiro público.

Seu gerente de segurança pode direcioná-lo a usar um servidor de chaves corporativas que armazenam todas as chaves frequentemente usadas de sua organização. Neste caso, seu PGP provavelmente já estará configurado para acessar o servidor apropriado.

Você pode procurar por chaves em um servidor de chaves usando estes métodos:

- ID do usuário
- ID da chave
- Status da chave (revogada ou desabilitada)
- Tipo de chave (Diffie-Hellman ou RSA)


- Data de criação
- Data de expiração
- Chaves revogadas
- Chaves desabilitadas
- Tamanho da chave
- Chaves assinadas por uma chave em particular

O inverso da maioria destas operações também está disponível. Por exemplo, você pode pesquisar usando “ID do usuário não é Bob” como seu critério.

Existem vários Servidores de Chaves Públicas, como o que é mantido pela Network Associates, Inc, onde você pode localizar as chaves da maioria dos usuários de PGP. Se o destinatário não o apontou ao endereço WWW onde a chave dele(a) está armazenada, você pode acessar qualquer servidor de chaves e pesquisar pelo nome do usuário ou endereço de email, porque todos os servidores de chave são regularmente atualizados para incluir as chaves armazenadas em todos os outros servidores.

Para obter a chave pública de alguém através de um servidor de chaves

1. Abra o programa PGPkeys.

2. Escolha “Search Server” no menu “Keys”, ou clique () para abrir a caixa de diálogo “Search”.

A caixa de diálogo “Search” aparece.

3. Na caixa “Search For Keys On”, selecione a localização ou servidor aonde você deseja procurar.
4. Entre o critério de procura a ser usado para localizar a chave pública do usuário. Para refinar a procura, clique “More Choices” para especificar critérios adicionais.


Quando a chave pública for encontrada, você pode examiná-la na caixa de diálogo “Search” para certificar-se de que ela é válida. Se você decidir adicionar a chave a seu chaveiro público, arraste-a para a janela principal de PGPkeys.

Adicionando chaves públicas a partir de mensagens de email

Um modo conveniente de obter uma cópia da chave pública de alguém é fazer com que a pessoa a inclua em uma mensagem de email. Quando uma chave pública é enviada através de chave pública, ela aparece como um bloco de texto no corpo da mensagem.

Para adicionar uma chave pública a partir de uma mensagem de email

Execute um dos seguintes:

- Se você tem um aplicativo de email que é suportado pelo plug-in PGP, então clique () para adicionar a chave pública do emitente a seu chaveiro público.
- Se você está usando um aplicativo de email que não é suportado pelos plug-ins, você pode adicionar a chave pública ao chaveiro copiando o bloco de texto que representa a chave pública e colar a mesma na janela de PGPkeys.

Importando uma chave pública de um arquivo

Outro método de obter a chave pública de alguém é fazer com que a pessoa salve-a para um arquivo do qual você pode importá-la ou copiar e colá-la em seu chaveiro público.

Para importar uma chave pública de um arquivo

Há três métodos de extrair a chave pública de alguém e adicioná-la a seu chaveiro público:

- Clique “Import” no menu “Keys” e então localize o arquivo onde a chave pública está armazenada.
- Arraste o arquivo que contém a chave pública para a janela principal de PGPkeys.
- Abra o documento texto onde a chave pública está armazenada, selecione o bloco de texto que representa a chave, e então clique “Copy” no menu “Edit”. Vá à janela de PGPkeys e clique “Paste” no menu “Edit” para copiar a chave. A chave então é mostrada como um ícone na janela de PGPkeys.

Verificando a autenticidade de uma chave

Quando você troca chaves com alguém, às vezes é difícil dizer se a chave realmente pertence àquela pessoa. PGP provê vários recursos de segurança que lhe permitem checar a autenticidade de uma chave e certificar que a chave pertence a um usuário em particular (ou seja, *validá-la*). PGP também lhe avisa se você tentar usar uma chave que não é válida e também tem como padrão alertá-lo quando você for usar uma chave marginalmente válida.

Por quê verificar a autenticidade de uma chave?

Uma das maiores vulnerabilidades dos sistemas de criptografia por chave pública é a habilidade de espíões sofisticados montarem um ataque “homem no meio” através da substituição da chave pública de alguém por uma que eles possuem. Desta forma eles podem interceptar qualquer email codificado para esta pessoa, decifrá-la usando a chave deles mesmos, e então codificá-la novamente com a chave real da pessoa e enviá-la para ela como se nada houvesse acontecido. De fato, isto poderia ser feito automaticamente através de um programa de computador sofisticado que ficaria no meio e decifraria todas as suas correspondências.

Baseado neste cenário, você e aqueles com quem você deseja trocar email precisam de uma forma de determinar se vocês realmente possuem cópias legítimas da chave de cada um. A melhor forma de se estar absolutamente certo que uma chave pública realmente pertence a uma pessoa em particular é fazer com que o proprietário da chave a copie para um disquete e então fisicamente o entregue a você. Entretanto, você raramente está perto o suficiente para entregar pessoalmente o disquete a alguém; vocês geralmente trocam chaves públicas via email ou as obtêm através de um servidor de chaves públicas.

Verificando com uma impressão digital

Você pode determinar se uma chave realmente pertence a uma pessoa em particular checando a impressão digital da chave, que é uma série única de números gerados quando a chave é criada. Comparando a impressão digital da sua cópia da chave pública de alguém com a impressão digital da chave original, você pode estar absolutamente certo de que você realmente possui uma cópia válida daquela chave. Para aprender como verificar com uma impressão digital, veja [“Verificando a chave pública de alguém”](#).

Assinando a chave pública

Uma vez que você está absolutamente convencido de que possui uma cópia legítima da chave pública de alguém, você poderá então assinar a chave daquela pessoa. Assinando a chave pública de alguém com sua chave privada, você está certificando ter certeza de que aquela chave pertence ao usuário alegado. Por exemplo, quando você cria uma nova chave, ela é automaticamente certificada com sua própria assinatura digital. Por padrão, assinaturas que você cria em outras chaves não são exportáveis, o que significa que elas aplicam-se apenas à chave quando ela está em seu chaveiro local. Para instruções detalhadas sobre assinar uma chave, veja [“Assinando a chave pública de alguém”](#).

Obtendo chaves públicas a partir de apresentadores de confiança

Usuários de PGP geralmente possuem outros usuários de confiança para assinar suas chaves públicas para atestar sua autenticidade. Por exemplo, você poderia enviar a um colega de confiança uma cópia de sua chave pública, com um pedido de que ele/ela certifique-a e retorne-a a você, de forma que você possa incluir a assinatura quando postar sua chave em um servidor de chaves públicas. Usando PGP, quando alguém obtém uma cópia da sua chave pública, eles não precisam checar a autenticidade da chave eles mesmos, mas ao invés podem basear-se em o quanto eles confiam na(s) pessoa(s) que assinou/assinaram sua chave. PGP provê os meios de estabelecer um nível de validade para cada um das chaves públicas que você adiciona a seu chaveiro público, e mostra o nível de confiança e validade associado a cada chave na janela de PGPkeys. Isto significa que quando você obtém a chave de alguém cuja chave é assinada por um apresentador de confiança, você pode estar bem certo de que a chave pertence o usuário alegado. Para detalhes sobre como assinar chaves e validar usuários, veja [“Assinando a chave pública de alguém”](#).

Seu Gerente de Segurança pode agir como um apresentador de segurança, e você pode então confiar em qualquer chave assinada pela chave corporativa como sendo uma chave válida. Se você trabalha em uma grande companhia com diversos locais, você pode ter apresentadores regionais, e seu Gerente de Segurança pode ser um meta-apresentador, ou um apresentador de confiança de apresentadores de confiança.

Enviando e Recebendo Email Seguro

4

Este capítulo explica como codificar e assinar o email que você envia a outros e decifrar e verificar o email que outros enviam a você.

Codificando e assinando email

Há três formas de codificar e assinar mensagens de email. A forma mais rápida e fácil de codificar e assinar email é com um aplicativo suportado pelos plug-ins de email de PGP. Apesar dos procedimentos variarem um pouco entre diferentes aplicativos de email, você executa o processo de codificar e assinar clicando os botões apropriados na barra de ferramentas do aplicativo. Se você estiver usando um aplicativo de email que não é suportado pelos plug-ins de PGP, você pode codificar e assinar suas mensagens de email via Área de Transferência de Windows, selecionando a opção apropriada do ícone da fechadura na bandeja de sistema. Para incluir arquivos anexos, você codifica os arquivos através do Windows Explorer antes de anexá-los.

DICA: Se você está enviando email sensível, considere deixar a linha de assunto em branco ou criar uma linha de assunto que não revele o conteúdo da mensagem codificada.

Se você não possui um dos aplicativos de email suportados por PGP, veja o [Capítulo 5](#) para informações sobre como codificar arquivos.

Como alternativa ao uso dos plug-ins, você pode usar PGPtools para codificar e assinar seus textos de email e anexos antes de enviá-los, veja [“Para codificar e assinar usando PGPtools”](#).

Codificando e assinando com os aplicativos de email suportados

Quando você codifica e assina com um aplicativo de email que é suportado pelos plug-ins de PGP, você tem duas escolhas, dependendo do tipo de aplicativo de email que o destinatário está usando. Se você está se comunicando com outros usuários de PGP que possuem um aplicativo de email que suporta o padrão PGP/MIME, você pode tomar vantagem de um recurso de PGP/MIME para codificar e assinar suas mensagens de email e quaisquer arquivos anexos automaticamente quando os enviar. Se você está se



comunicando com alguém que não possui um aplicativo de email compatível com PGP/MIME, você deve codificar seu email com PGP/MIME desligado para evitar qualquer problema de compatibilidade. Veja a [tabela 4-1, “Recursos de Plug-in de PGP”](#), para uma lista de plug-ins e seus recursos.

Tabela 4-1. Recursos de Plug-in de PGP

	Eudora 3.0.x	Eudora 4.0.x	Exchange/ Outlook	Outlook Express
PGP/MIME	Sim	Sim	Não	Não
Auto-decifrar	Sim	Não	Sim	Sim
Codificar HTML	N/D	Sim	converte para texto puro antes de codificar	Não
Ver HTML decifrado como documento HTML	Não	Sim	Não	Não
Codificar anexos	Sim	Sim	Sim	Não
Padrões para codificar/assinar	Sim	Sim	Sim	Sim

Para codificar e assinar com aplicativos de email suportados

1. Use seu aplicativo de email para compor sua mensagem de email como normalmente faria.

- Quando tiver terminado de compor o texto da sua mensagem de email, clique () para codificar o texto de sua mensagem, e então clique () para assinar a mensagem.

NOTA: Se você sabe que irá usar PGP/MIME regularmente, você pode deixá-lo ativo selecionando a configuração apropriada no painel “email” da janela “Preferences”.

- Envie sua mensagem como normalmente faria.

Se você possui uma cópia das chaves públicas de cada um dos destinatários, as chaves apropriadas são usadas. Entretanto, se você especificar um destinatário para quem não há uma chave pública correspondente ou uma ou mais das chaves possuem validade insuficiente, a caixa de diálogo “PGP Key Selection” aparece ([Figura 4-1](#)) de forma que você possa especificar a chave correta.

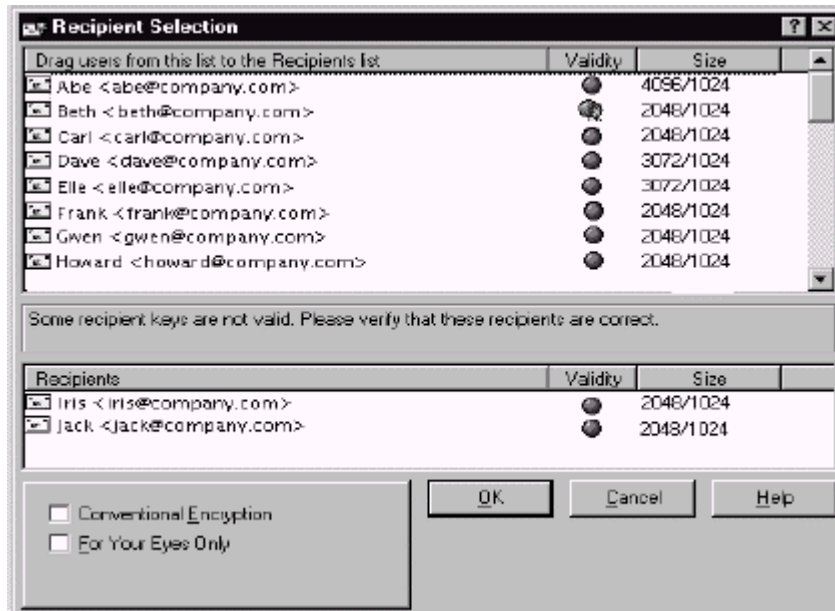


Figura 4-1. A janela “Recipients”

- Arraste as chaves públicas daqueles que irão receber uma cópia da mensagem de email codificada na lista de destinatários. Você pode também dar um duplo clique em qualquer uma das chaves para movê-las de uma área da tela para outra. O ícone de validade (“Validity”) indica o nível mínimo de confiança de que as chaves públicas na lista de Destinatários são válidas. A validade é baseada nas assinaturas associadas com a chave. Veja o [capítulo 6, “Gerenciando Chaves e Configurando Preferências”](#), para detalhes.
- Selecione a opção de criptografia convencional (“Conventional Encrypt”) para usar uma frase-senha comum ao invés da criptografia por chaves

públicas. Se você selecionar esta opção, o arquivo é codificado usando uma chave de sessão, que codifica (e decifra) usando uma frase-senha que lhe será pedida.

6. Selecione a opção de visualizador seguro (“Secure Viewer”) para proteger os dados de ataques “TEMPEST” quando da decifração. Se você selecionar esta opção, os dados decifrados são mostrados em uma fonte especial para prevenção de ataques TEMPEST que é ilegível para equipamentos de captura de radiação. Para mais informações sobre os ataques TEMPEST, veja [“Vulnerabilidades”](#).

NOTA: A opção do visualizador seguro pode não ser compatível com versões anteriores de PGP. Arquivos codificados com esta opção habilitada podem ser decifrados por versões anteriores de PGP, entretanto este recurso pode ser ignorado.

7. Clique OK para codificar e assinar seu email. Se você escolheu assinar os dados codificados, a caixa de diálogo “Signing Key Passphrase” aparece, como na [figura 4-2](#), pedindo sua frase-senha antes do email ser enviado.

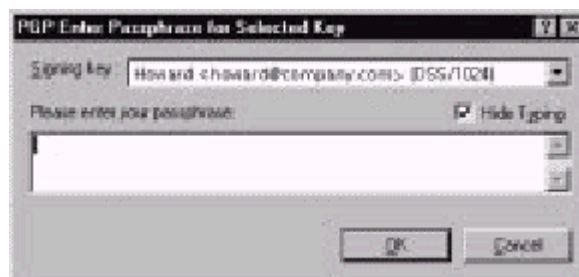


Figura 4-2. Caixa de diálogo “Signing Key Passphrase”

8. Entre sua frase-senha e então clique OK.

ATENÇÃO: Se você não enviar seu email imediatamente, mas ao invés armazená-lo em sua Caixa de Saída, você deve ficar ciente de que quando usando alguns aplicativos de email, a informação não é codificada até que o email seja realmente transmitido. Antes de colocar em fila mensagens codificadas, você deve verificar se seu aplicativo realmente codifica as mensagens em sua caixa de saída. Se não o fizer, você pode usar PGPTray para codificar sua mensagem antes de colocá-la em fila na caixa de saída.

Para codificar e assinar texto usando PGPtools

1. Copie o texto que você quer codificar e assinar para a Área de Transferência.
2. Arraste o texto para os botões “Encrypt” (codificar), “Sign” (assinar), ou “Encrypt and Sign” (codificar e assinar) na janela de PGPtools.

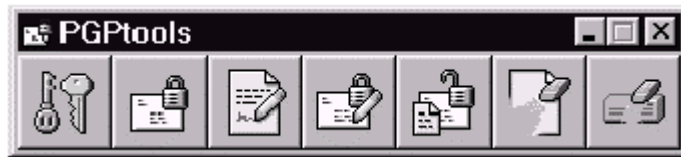


Figura 4-3. A janela de PGTools

A caixa de diálogo “PGP Key Recipients” (Destinatários das Chaves) aparece ([figura 4-1](#)).

3. Arraste as chaves públicas daqueles que irão receber uma cópia da mensagem de email codificada para a lista de Destinatários. Você também pode dar um duplo clique em qualquer uma das chaves para movê-la de uma área da tela para outra. O ícone de Validade indica o nível mínimo de confiança que aquela chave pública na lista de destinatários é válida. Esta validade é baseada nas assinaturas associadas com a chave. Veja o [Capítulo 6, “Gerenciando Chaves e Configurando Preferências”](#), para detalhes.
4. Selecione a opção “Conventional Encrypt” (codificação convencional) para usar uma frase-senha comum ao invés da criptografia por chave pública. Se você selecionar esta opção, o arquivo é codificado usando uma chave de sessão, que codifica (e decifra) usando uma frase-senha que lhe será pedida para escolher.
5. Selecione a opção “Secure Viewer” (visualizador seguro) para proteger os dados de ataques TEMPEST quando decifrando-os. Se você selecionar esta opção, os dados decifrados são exibidos em uma fonte especial que previne ataques TEMPEST que é ilegível para equipamentos de captura de radiação. Para mais informações sobre ataques TEMPEST, veja [“Vulnerabilidades”](#).

NOTA: A opção “Secure Viewer” pode não ser compatível com versões anteriores de PGP. Arquivos codificados com esta opção habilitada podem ser decifrados por versões anteriores de PGP, entretanto este recurso pode ser ignorado.

6. Clique OK para codificar e assinar sua correspondência.

Se você escolheu assinar os dados codificados, a caixa de diálogo “Signing Key Passphrase” irá aparecer, como mostrado na [figura 4-2](#), pedindo sua frase-senha antes de enviar a correspondência

7. Entre sua frase-senha e então clique OK.
8. Cole o texto em sua mensagem de email, então envie a mensagem.

Codificando email para grupos de destinatários

Você pode usar PGP para criar uma lista de grupos de distribuição. Por exemplo, se você quer enviar email codificado para 10 pessoas em `engenharia@companhia.com`, você poderia criar uma lista de distribuição com este nome. O menu “Groups” em PGPkeys contém uma opção “Show Groups” (exibir grupos) que alterna a exibição da janela de grupos em PGPkeys.

NOTA: Se você pretende codificar informações para todos os membros de uma lista de distribuição de email, você deve criar um grupo PGP com o mesmo nome da lista, e incluir os mesmos membros da lista de distribuição de email. Por exemplo, se há uma lista `staff@companhia.com` configurado em seu aplicativo de email, você deve criar um grupo `staff@companhia.com` em PGP.

Trabalhando com listas de distribuições

Use o recurso de grupos para criar listas de distribuições e para editar a lista de pessoas para quem você deseja enviar email codificado.

Para criar um grupo (lista de distribuição)

1. Escolha “Show Group” (Exibir Grupo) no menu “Groups”.
2. Escolha “New Group” (Novo Grupo) no menu “Groups”.
3. Entre o nome para a lista de distribuição. Opcionalmente, entre uma descrição para o grupo. Por exemplo, você pode nomear o grupo como “`todomundo@companhia.com`” com a descrição “Todos os funcionários”.
4. Clique OK para criar a lista de distribuição.

A lista de grupos de distribuição é salva como um grupo PGP na pasta “PGP Preferences” e a lista é adicionada a seu chaveiro.

Para adicionar membros a uma lista de distribuição

1. Na janela PGPkeys, selecione os usuários ou listas que você deseja adicionar à sua lista de distribuição.

2. Arraste os usuários da janela de PGPkeys para a lista de distribuição desejada, na janela de grupos.

NOTA: Membros em uma lista de distribuição podem ser adicionados a outras listas de distribuições.

Para remover membros de uma lista de distribuição

1. Dentro da lista de distribuição, selecione o membro a ser removido.
2. Pressione a tecla “Delete”.

PGP pede que você confirme sua escolha.

Para remover uma lista de distribuição

1. Selecione a lista de distribuição a ser removida na janela de grupos.
2. Pressione a tecla “Delete”.

Para adicionar uma lista de distribuição a outra lista de distribuição

1. Selecione a lista de distribuição que você deseja adicionar a outra lista.
2. Arrasta a lista selecionada para a lista aonde ela será adicionada.



Enviando email codificado e assinado para listas de distribuição

Você pode enviar email codificado para grupos de destinatários uma vez que suas listas de distribuição de PGP foram criadas. Veja [“Trabalhando com listas de distribuições”](#) para mais informações sobre criação e edição de listas de distribuição.

Para enviar email codificado e assinado a uma lista de distribuição

1. Aderece a correspondência para sua lista de distribuição de correspondências.

O nome da sua lista de distribuição codificada deve corresponder ao nome da listas de distribuição de email.

2. Use seu aplicativo de email para compor sua mensagem de email como normalmente faria.
3. Quando você tiver terminado de compor o texto da sua mensagem de email, clique () para codificar o texto da sua mensagem, então clique () para assinar a mensagem.

A caixa de diálogo “PGP Key Recipients” surge ([figura 4-1](#)). Você seleciona as chaves públicas dos destinatários para o texto que está codificando ou assinando. As opções disponíveis estão descritas em [“Para codificar e assinar com aplicativos de email suportados”](#).

4. Envie a mensagem.

Decifrando e verificando email

A forma mais rápida e fácil de decifrar e verificar email enviado a você é com um aplicativo suportado pelos plug-ins de email de PGP. Apesar dos procedimentos variarem um pouco entre diferentes aplicativos de email, quando você está usando um aplicativo de email suportado pelos plug-ins, você pode executar as operações de decifrar e verificar clicando o ícone do envelope em sua mensagem ou na barra de ferramentas do seu aplicativo. Em alguns casos você talvez irá precisar selecionar Decrypt/Verify do menu em seu aplicativo de email. Além disso, se você estiver usando um aplicativo que suporta o padrão PGP/MIME, você pode decifrar e verificar suas mensagens de email como também quaisquer arquivos anexos clicando o ícone anexado à sua mensagem.



Se você estiver usando um aplicativo de email que não é suportado pelos plug-ins de PGP, você pode decifrar e verificar suas mensagens de email via PGPTray. Além disso, se seu email inclui arquivos anexos codificados, você deve decifrá-los separadamente usando PGPtools ou PGPTray.

Para decifrar e verificar a partir de aplicativos de email suportados

1. Abra sua mensagem de email como você normalmente faria.

Você verá um bloco de texto cifrado ininteligível no corpo de sua mensagem de email.

2. Copie o texto cifrado para a Área de Transferência.

3. Para decifrar e verificar a mensagem, faça um dos seguinte:
 - o Se você está se comunicando com outros usuários de PGP, e eles codificaram e assinaram suas correspondências usando o padrão PGP/MIME, dê um clique duplo no ícone do envelope com cadeado ()
 - o Se você está recebendo email de alguém que não está usando um aplicativo de email compatível com PGP/MIME, clique o ícone do envelope aberto () na barra de ferramentas do seu aplicativo, ou clique “Decrypt/Verify Clipboard” (Decifrar/Verificar Área de Transferência) no menu “Plugins”.

Para decifrar e verificar arquivos anexados, decifre-os separadamente usando PGTools ou PGPTray.

A caixa de diálogo “PGP Enter Passphrase” aparece, como na [figura 4-4](#), pedindo que você insira sua frase-senha.

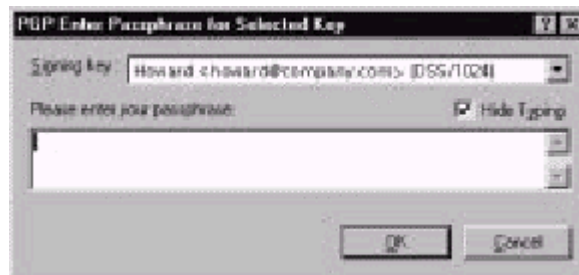


Figura 4-4. A caixa de diálogo “PGP Enter Passphrase”

4. Entre sua frase-senha, então clique OK.

A mensagem é decifrada. Se ela foi assinada e você possui a chave pública do emissor, uma mensagem aparece indicando se a assinatura é válida.

Se a mensagem foi codificada usando a opção “Secure Viewer” (Visualizador Seguro) habilitada, uma mensagem de aviso aparece. Clique OK para continuar. A mensagem decifrada aparece em uma tela segura de PGP usando uma fonte especial para prevenir ataques TEMPEST.

5. Você pode salvar a mensagem em estado decifrado, ou pode salvar a versão original codificada de forma que ela permaneça segura.

NOTA: Mensagens codificadas com a opção Secure Viewer habilitada não podem ser armazenadas em seu estado decifrado.

Para decifrar e verificar a partir de aplicativos de email não suportados

1. Abra sua mensagem de email como você normalmente faria.

Você verá um bloco de texto cifrado ininteligível no corpo de sua mensagem de email.

2. Em PGPTray, selecione “Decrypt/Verify”.

Se a mensagem de email inclui arquivos anexos codificados, decifre-os separadamente usando PGPtools ou PGPTray.

A caixa de diálogo “PGP Enter Passphrase” aparece, como na [figura 4-4](#), pedindo que você insira sua frase-senha.

3. Entre sua frase-senha, então clique OK.

A mensagem é decifrada. Se ela foi assinada, uma mensagem aparece indicando se a assinatura é válida.

Se a mensagem foi codificada usando a opção “Secure Viewer” (Visualizador Seguro) habilitada, uma mensagem de aviso aparece. Clique OK para continuar. A mensagem decifrada aparece em uma tela segura de PGP usando uma fonte especial para prevenir ataques TEMPEST.

4. Você pode salvar a mensagem em estado decifrado, ou pode salvar a versão original codificada de forma que ela permaneça segura.

NOTA: Mensagens codificadas com a opção Secure Viewer habilitada não podem ser armazenadas em seu estado decifrado.

Usando PGP para Armazenamento Seguro de Dados

5

Este capítulo descreve como usar PGP para manter arquivos com segurança. Ele descreve como usar PGP para codificar, decifrar, assinar e verificar arquivos tanto para email quanto para armazenagem segura em seu computador. Ele também descreve as funções de PGP para Eliminação (“Wipe”) e Eliminação de Espaço Livre (“Free Space Wipe”), que apagam arquivos removendo seus conteúdos completamente de seu computador.

Usando PGP para codificar e decifrar arquivos

Você pode usar PGP para codificar e assinar arquivos para uso como anexos de email. Você também pode usar as técnicas descritas neste capítulo para codificar e assinar arquivos de forma que você os armazena com segurança em seu computador.

Usando o menu de PGP do botão direito para codificar e assinar

Use o menu de PGP do botão direito para enviar um arquivo codificado como um anexo com sua mensagem de email, ou para codificar um arquivo para protegê-lo em seu computador.

Para codificar e assinar usando o menu do botão direito

1. No Windows Explorer, clique com o botão direito no arquivo ou arquivos que você quer codificar.
2. Escolha uma das seguintes opções a partir do menu de PGP do botão direito:

- **Encrypt.** Selecione esta opção para apenas codificar o arquivo ou arquivos que você selecionou.
- **Sign.** Selecione esta opção para apenas assinar o arquivo ou arquivos que você selecionou.
- **Encrypt and Sign.** Selecione esta opção para codificar e assinar o arquivo ou arquivos que você selecionou.

A caixa de diálogo “PGP Key Selection” aparece, como mostrado na [Figura 5-1](#).

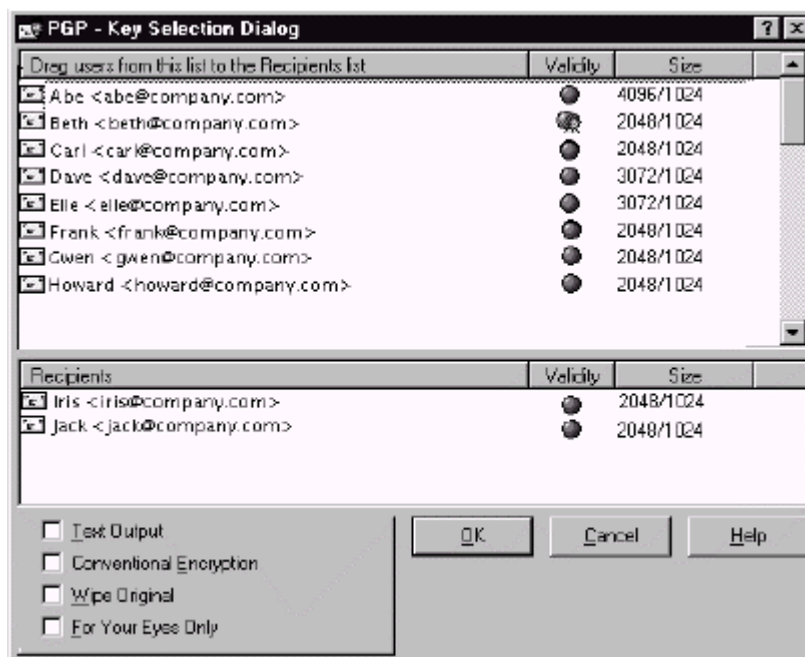


Figura 5-1. Caixa de diálogo “PGP Recipients” (Destinatários)

Você pode selecionar as chaves públicas dos destinatários para o arquivo que você está codificando ou assinando.

3. Selecione as chaves públicas arrastando-as para a lista de destinatários, então clique OK.

Você pode escolher as seguintes opções de codificação, dependendo do tipo de dados que você está codificando:

- **Conventional Encrypt** (Codificação Convencional). Selecione esta caixa para usar uma frase-senha comum ao invés da criptografia por chave pública. O arquivo é codificado usando uma chave de sessão, que codifica (e decifra) usando uma frase-senha que lhe será pedida para escolher.

- **Text Output** (Saída de Texto). Quando enviando arquivos como anexos com alguns aplicativos de email, você talvez precise selecionar a caixa “Text Output” para salvar o arquivo como texto ASCII. Isto às vezes é necessário de forma a enviar arquivos binários usando antigos aplicativos de email. A seleção desta opção aumenta o tamanho do arquivo codificado em cerca de 30 por cento.
- **Wipe Original** (Eliminar o Original). Selecione esta caixa para sobrescrever o documento original que você está codificando ou assinando, de forma que suas informações sensíveis não sejam legíveis por qualquer um que possa acessar seu disco rígido.
- **Secure Viewer** (Visualizador Seguro). Selecione esta opção para proteger o texto de ataques TEMPEST quando decifrando-os. Se você selecionar esta opção, os dados são exibidos em uma fonte especial que previne ataques TEMPEST que é ilegível a equipamentos de captura de radiação quando decifrando-os. Para maiores informações sobre ataques TEMPEST, veja [“Vulnerabilidades”](#).

NOTA: Esta opção está somente disponível quando codificando texto ou arquivos texto.

Se você está assinando os arquivos, lhe será pedida sua frase-senha.

Após a codificação, se você olhar a pasta onde o arquivo original estava, você encontrará um arquivo com o nome especificado representado por um entre dois ícones:



codificado com saída de
texto



codificado com saída
padrão

Se você está codificando ou assinando uma pasta (diretório), a saída pode estar em uma nova pasta, dependendo da opção que você selecionou.

Usando PGTools para codificar e assinar

Para codificar e assinar usando PGTools

1. Abra o programa PGTools.

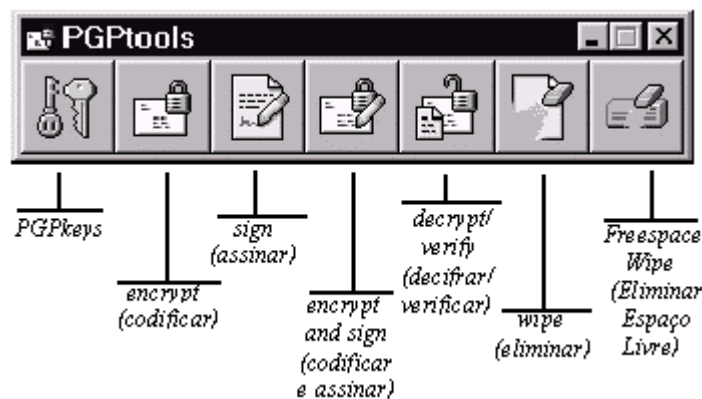


Figura 5-2. menu PGTools

2. No Windows Explorer, selecione o arquivo ou arquivos que você quer codificar.

Você pode selecionar vários arquivos, mas deve codificar e assinar cada um individualmente.

3. Arraste o(s) arquivo(s) para o botão Encrypt, Sign, ou Encrypt and Sign na janela de PGTools.

A caixa de diálogo “PGP Recipients” aparece, como mostrado na [Figura 5-1](#).

4. Selecione as chaves públicas arrastando-as para a lista de destinatários.
5. Você pode escolher as seguintes opções de codificação, dependendo do tipo de dados que você está codificando:
 - o **Conventional Encrypt** (Codificação Convencional). Selecione esta caixa para usar uma frase-senha comum ao invés da criptografia por chave pública. O arquivo é codificado usando uma chave de sessão, que codifica (e decifra) usando uma frase-senha que lhe será pedida para escolher.

- **Text Output** (Saída de Texto). Quando enviando arquivos como anexos com alguns aplicativos de email, você talvez precise selecionar a caixa “Text Output” para salvar o arquivo como texto ASCII. Isto às vezes é necessário de forma a enviar arquivos binários usando antigos aplicativos de email. A seleção desta opção aumenta o tamanho do arquivo codificado em cerca de 30 por cento.
- **Wipe Original** (Eliminar o Original). Selecione esta caixa para sobrescrever o documento original que você está codificando ou assinando, de forma que suas informações sensíveis não sejam legíveis por qualquer um que possa acessar seu disco rígido.
- **Secure Viewer** (Visualizador Seguro). Selecione esta opção para proteger o texto de ataques TEMPEST quando decifrando-os. Se você selecionar esta opção, os dados são exibidos em uma fonte especial que previne ataques TEMPEST que é ilegível a equipamentos de captura de radiação quando decifrando-os. Para maiores informações sobre ataques TEMPEST, veja [“Vulnerabilidades”](#).

NOTA: Esta opção está somente disponível quando codificando texto ou arquivos texto.

6. Clique OK.

Se você está assinando os arquivos, lhe será pedida sua frase-senha.

Após a codificação, se você olhar a pasta onde o arquivo original estava, você encontrará um arquivo com o nome especificado representado por um entre dois ícones:



codificado com saída de
texto



codificado com saída
padrão

Se você está codificando ou assinando uma pasta (diretório), a saída pode estar em uma nova pasta, dependendo da opção que você selecionou.

Usando PGPtray para decifrar e verificar

Se o email que você receber possuir arquivos anexos, e você não estiver usando um aplicativo de email compatível com PGP/MIME, você deve decifrá-lo usando a Área de Transferência de Windows.

Para decifrar e verificar arquivos usando PGPtray

1. No Windows Explorer, selecione o arquivo ou arquivos que você quer decifrar e verificar.
2. Escolha “Decrypt/Verify” de PGPtray.

A janela “Enter Passphrase” (Entre a Frase-Senha) aparece, como mostrado na [figura 5-3](#).

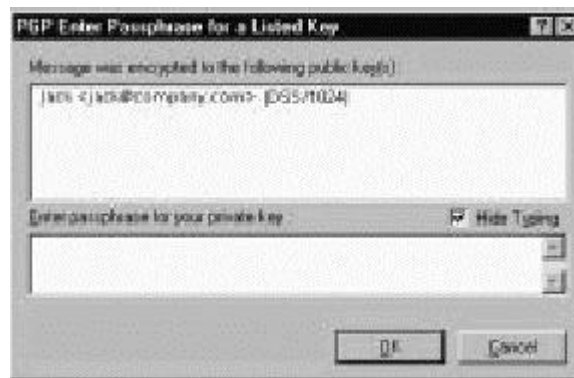


Figura 5-3. A janela “Enter Passphrase”

3. Entre sua frase-senha e então clique OK.

O arquivo é decifrado. Se ele foi assinado, uma mensagem aparece indicando se a assinatura é válida.

Se o arquivo texto foi codificado com a opção de Visualizador Seguro (“Secure Viewer”) habilitada, uma mensagem de aviso aparecerá.

Clique OK para continuar. O texto decifrado aparece em uma tela segura de PGP em uma fonte especial de prevenção de ataques TEMPEST.

4. Você pode salvar a mensagem em seu estado decifrado, ou pode salvar a versão codificada original de forma a mantê-la segura.

NOTA: Mensagens codificadas com a opção “Secure Viewer” habilitada não podem ser salvas em seu estado decifrado. Elas são apenas visíveis na janela segura de PGP após decifradas.

Usando PGTools para decifrar e verificar

Para decifrar e verificar usando PGTools

1. No Windows Explorer, selecione o arquivo ou arquivos que você quer decifrar e verificar.
2. Arraste o arquivo para o botão “Decrypt/Verify” na janela de PGTools ([figura 5-2](#)).

A janela “Enter Passphrase” (Entre a Frase-Senha) aparece, como mostrado na [figura 5-3](#), pedindo que você insira sua frase-senha.

3. Entre sua frase-senha e então clique OK.

Se o arquivo foi assinado, uma mensagem aparece indicando se a assinatura é válida.

Se o arquivo texto foi codificado com a opção de Visualizador Segura (“Secure Viewer”) habilitada, uma mensagem de aviso aparecerá. Clique OK para continuar. O texto decifrado aparece em uma tela segura de PGP em uma fonte especial de prevenção de ataques TEMPEST.

4. Você pode salvar a mensagem em seu estado decifrado, ou pode salvar a versão codificada original de forma a mantê-la segura.

NOTA: Mensagens codificadas com a opção “Secure Viewer” habilitada não podem ser salvas em seu estado decifrado. Elas são apenas visíveis na janela segura de PGP depois de decifradas.

Assinando e decifrando arquivos com uma chave dividida

Uma vez que uma chave é dividida entre vários proprietários, tentativas de assinar ou decifrar com ela irá fazer com que PGP automaticamente tente reunir a chave. Há duas formas de reunir a chave, localmente e remotamente.

Reunir partes da chave localmente requer a presença dos proprietários junto ao computador que fará a reunião da chave. Cada proprietário deve entrar sua frase-senha para sua parte da chave.

Reunir partes da chave remotamente requer que os proprietários remotos autentiquem e decifrem suas chaves antes de enviá-las pela rede. O Transport Layer Security (TLS) de

PGP provê uma ligação segura para transmissão das partes da chave, que permitem que vários indivíduos em localidades distantes seguramente assinem ou decifrem com suas partes da chave.

IMPORTANTE: Antes do recebimento das partes da chave através da rede, você deve certificar a impressão digital da chave de cada um dos proprietários e assinar suas chaves públicas para ter certeza de que suas chaves de autenticação são legítimas. Para aprender como verificar um par de chaves, veja [“Verificando com uma impressão digital”](#).

Para assinar ou decifrar arquivos com uma chave dividida

1. Contate cada um dos proprietários da chave dividida. Para reunir partes da chave localmente, os proprietários devem estar presentes.

Para obter as partes da chave através da rede, certifique-se de que os proprietários remotos estão preparados para enviar suas partes da chave. Os proprietários remotos devem ter:

- suas partes da chave e senha
 - uma chave pública (para autenticação no computador que está obtendo as partes da chave)
 - uma conexão de rede
 - o endereço IP ou Nome de Domínio do computador que está obtendo as partes da chave
2. No computador que está unindo as partes, use o Windows Explorer para selecionar o(s) arquivo(s) que você quer assinar ou decifrar com a chave dividida.
 3. Clique com o botão direito no(s) arquivo(s) e selecione “Sign” (Assinar) ou “Decrypt” (Decifrar) no menu de PGP. A caixa de diálogo de PGP “Enter Passphrase for Selected Key” (Entre Frase-Senha para a Chave Selecionada) aparece com a chave dividida selecionada.
 4. Clique OK para reconstituir a chave selecionada.

A caixa de diálogo “Key Share Collection” aparece, como mostrado na [figura 5-4](#).



Figura 5-4. A caixa de diálogo “Key Share Collection”

- Se você está obtendo as partes da chave localmente, clique “Select Share File” e então localize os arquivos das partes associadas à chave dividida. Os arquivos das partes podem ser obtidos de um disco rígido, disquete, ou drive montado. Siga ao passo 6.

Se você está obtendo as partes da chave através da rede, clique “Start Network”. A caixa de diálogo “Passphrase” aparece. Na caixa “Signing Key”, selecione o par de chaves que você quer usar para autenticação ao sistema remoto e entre sua frase-senha. Clique OK para preparar o computador para receber as partes da chave.

O status da transação é exibido na caixa “Network Shares”. Quando o status muda para “Listening” (Escutando), o programa PGP está pronto para receber as partes da chave.

Neste momento, os proprietários devem enviar suas partes da chave. Para aprender como enviar partes da chave para o computador que irá uni-las, veja [“Enviando sua parte da chave através da rede”](#). Quando uma chave é recebida, a caixa de diálogo “Remote Authentication” (Autenticação Remota) aparece, como mostrado na [figura 5-5](#).

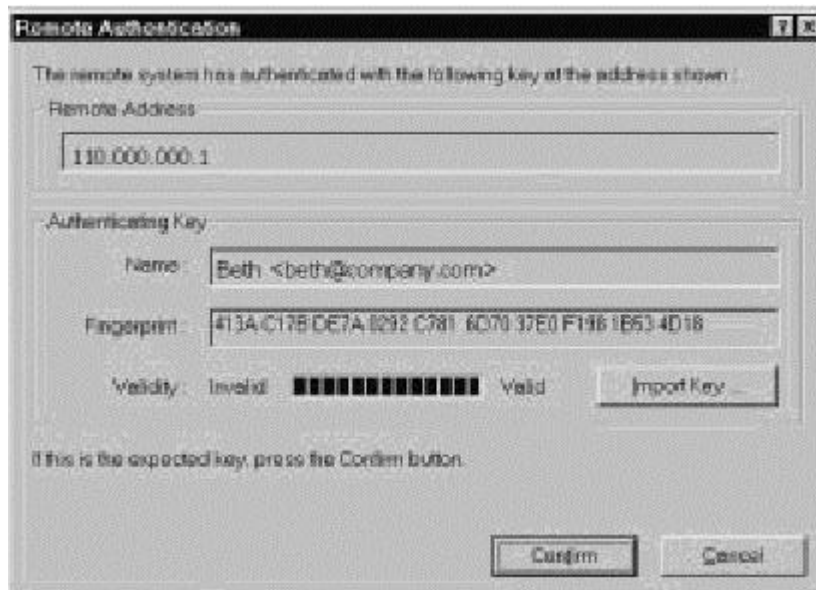


Figura 5-5. A caixa de diálogo “Remote Authentication”

Se você não assinou a chave que está sendo usada para autenticar o sistema remoto, a chave será considerada inválida. Apesar de você poder reunir a chave dividida com uma chave de autenticação inválida, isto não é recomendado. Você deve verificar a “impressão digital” de cada proprietário, e assinar suas chaves públicas para certificar-se de que a chave de autenticação é legítima.

Clique “Confirm” para aceitar o arquivo da parte.

6. Continue obtendo partes da chave até que o valor para “Total Shares Collected” seja igual ao valor para “Total Shares Needed” na janela “Key Shares Collection”.
7. Clique OK.

O arquivo é assinado ou decifrado com a chave dividida.

Para enviar sua parte da chave através da rede

1. Quando você é contactado pela pessoa que está unindo a chave dividida, certifique-se de ter os seguintes itens:
 - o o arquivo com suas parte da chave e senha
 - o um par de chaves (para autenticação no computador que está obtendo as partes da chave)

- o uma conexão de rede
 - o o endereço IP ou Nome de Domínio do computador que está obtendo as partes da chave
2. Selecione “Send Key Shares” (Enviar Parte da Chave) no menu “File” de PGPkeys.

A caixa de diálogo “Select Share File” aparece.

3. Localize sua parte da chave e clique “Open”.

A caixa de diálogo “Enter Passphrase” aparece.

4. Entre sua frase-senha e então clique OK.

A caixa de diálogo “Send Key Shares” aparece, como mostrado na [figura 5-6](#).

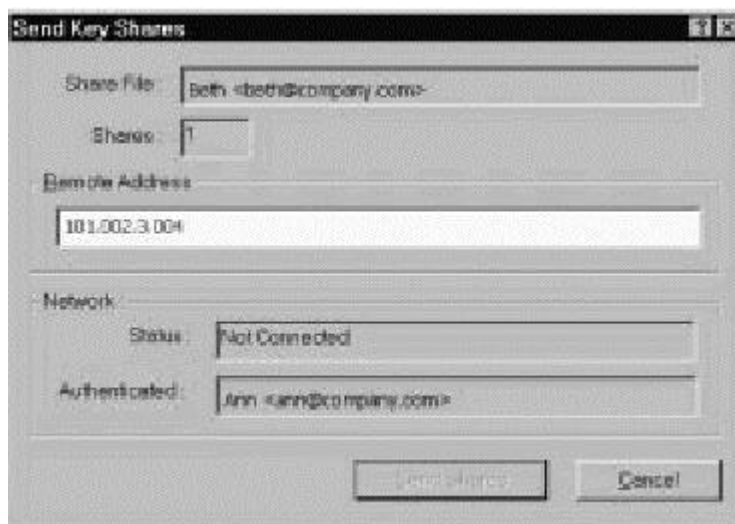


Figura 5-6. A caixa de diálogo “Send Key Shares”

5. Entre o endereço IP ou Nome de Domínio do computador que está fazendo a união das chaves na caixa de texto “Remote Address”, então clique “Send Shares”.

O status da transação é exibido na caixa “Network Shares”. Quando o status muda para “Connected” (Conectado), lhe é pedido para autenticar-se ao computador que está fazendo a união.

A caixa de diálogo “Remote Authentication” (Autenticação Remota) aparece pedindo que você confirme que o computador remoto é aquele para quem você quer enviar sua parte da chave.

6. Clique “Confirm” para completar a transação.

Após o computador remoto receber sua parte da chave e confirmar a transação, uma mensagem aparece dizendo que as partes foram enviadas com sucesso.

7. Clique OK.

8. Clique “Done” na janela “Key Shares” quando você tiver completado o envio da sua parte da chave.

Usando PGP Wipe para apagar arquivos

O item “Wipe” (Eliminar) em PGTools apaga arquivos e seus conteúdos. O recurso de Eliminação é uma forma segura de permanentemente remover um arquivo e seu conteúdo do disco rígido de seu computador. Quando você apaga um arquivo normalmente, colocando-o na Lixeira, o nome do arquivo é removido do diretório do arquivo, mas os dados do arquivo permanecem no disco. “Wipe” remove todos os traços dos dados de um arquivo de forma que ninguém possa usar uma ferramenta de software para recuperar o arquivo.

Para apagar permanentemente um arquivo usando o menu do botão direito

1. No Windows Explorer, selecione o arquivo ou arquivos que você deseja eliminar.


Para parar a eliminação do arquivo antes da tarefa estar completa, clique “Cancel”.

NOTA: Clicando “Cancel” durante a eliminação do arquivo pode deixar restos do arquivo para trás.

2. Clique no arquivo com o botão direito e então escolha “Wipe” a partir do menu. Uma caixa de diálogo de confirmação aparece.
3. Clique OK para apagar permanentemente o arquivo.

Para apagar permanentemente um arquivo usando PGPtools

1. No Windows Explorer, selecione o arquivo ou arquivos que você deseja eliminar.

2. Arraste o arquivo no botão “Wipe” () na janela de PGPtools.

Uma caixa de diálogo de confirmação aparece.

3. Clique OK para apagar permanentemente o arquivo.

Para parar a eliminação do arquivo antes da tarefa estar completa, clique “Cancel”.

NOTA: Clicando “Cancel” durante a eliminação do arquivo pode deixar restos do arquivo para trás.

Mesmo em sistemas com memória virtual, PGP corretamente escreve sobre todo o conteúdo do arquivo. Vale a pena notar que alguns aplicativos salvam o arquivo antes de codificá-los e podem deixar fragmentos do arquivo em seu disco, em locais onde eles não são mais considerados parte do arquivo. Para maiores informações, veja [“Arquivos de troca ou memória virtual”](#). Você pode usar o recurso de PGP “Freespace Wipe” (Eliminar Espaço Livre) para eliminar todo o espaço livre em seu disco para solucionar este problema. Veja a próxima seção para informações sobre o Freespace Wipe. Também, esteja ciente de que muitos programas automaticamente salvam arquivos em progresso, portanto pode haver cópias *backup* do arquivo que você está querendo apagar.

Usando PGP Free Space Wiper para limpar espaço livre em seus discos

Conforme você cria e apaga arquivos em seu computador, os dados contidos nestes arquivos permanecem no drive. PGPtools pode ser usado para eliminar com segurança os dados em um arquivo antes dele ser apagado para negar a possibilidade deles em algum momento serem recuperados.

Muitos programas criam arquivos temporários enquanto você edita o conteúdo de documentos. Estes arquivos são apagados quando você fecha os documentos, mas os dados do documento são deixados jogados em lugares do seu disco. Para ajudar reduzir a chance de que os dados de seus documentos possam mais tarde serem recuperados, a Network Associates recomenda que você elimine com segurança o espaço livre em seus drives como também apague com segurança documentos sensíveis.

Para eliminar espaço livre de seus discos

ATENÇÃO: Antes de executar o PGP Free Space Wiper, compartilhamento de arquivos deve ser desligado e todos os arquivos no volume ou disco que você deseja eliminar devem ser fechados.

1. Abra o programa PGTools.

2. Clique o botão “Wipe Free Space” () na janela de PGTools.

A tela de boas vindas do “PGP Free Space Wiper” aparece.

3. Leia as informações cuidadosamente, então clique “Next” para avançar à próxima caixa de diálogo.

O “PGP Free Space Wiper” pede-lhe para selecionar o volume que você deseja eliminar e o número de passos a serem executados.

4. Na caixa “Volume”, selecione o disco ou volume que você quer que PGP elimine.

Então, selecione o número de passos que você quer que PGP execute. Os níveis recomendados são:

- 3 passos para uso pessoal.
- 10 passos para uso comercial.
- 18 passos para uso militar.
- 26 passos para máxima segurança.

NOTA: Companhias comerciais de recuperação de dados são conhecidas por recuperar dados que foram sobrescritos até 9 vezes. PGP usa padrões altamente sofisticados durante cada eliminação para certificar de que seus dados sensíveis não possam ser recuperados.

5. Clique “Next” para continuar.

A caixa de diálogo “Perform Wipe” (Executar Eliminação) aparece, como mostrado na [figura 5-7](#), e exibe informações estatísticas sobre o drive ou volume que você selecionou.

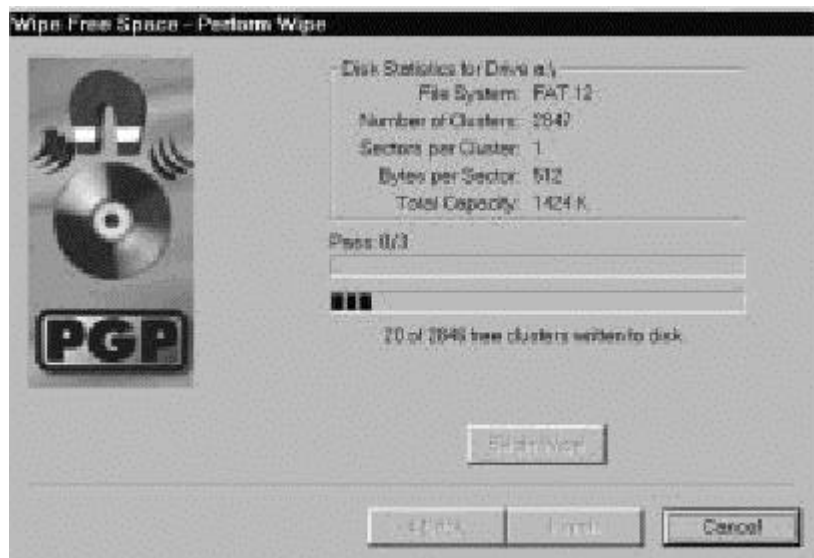


Figura 5-7. Eliminação de Espaço Livre (caixa de diálogo “Perform Wipe”)

6. Clique o botão “Begin Wipe” para iniciar a eliminação do espaço livre em seu disco ou volume.

O “PGP Free Space Wiper” procura e elimina fragmentos que sobraram de seu disco ou volume.

7. Quando a sessão de eliminação terminar, clique “Finish”.

Gerenciando Chaves e Configurando Preferências

6

Este capítulo explica como examinar e gerenciar as chaves armazenadas em seus chaveiros. Ele também descreve como configurar suas preferências para servir seu ambiente de computação particular.

Gerenciando suas chaves

As chaves que você cria, como as que obtêm de outros, são armazenadas em chaveiros, que são essencialmente arquivos armazenados em seu disco rígido ou em um disquete. Normalmente suas chaves privadas são armazenadas em um arquivo chamado `secring.skr` e suas chaves públicas são armazenadas em outro arquivo chamado `pubring.pkr`. Estes arquivos estão geralmente localizados na pasta “PGP Keyrings”.

NOTA: Como resultado de sua chave privada ser codificada automaticamente e sua frase-senha estar segura, não há perigo em deixar seus chaveiros em seu computador. Entretanto, se você não está confortável armazenando suas chaves nos locais padrão, você pode escolher um nome de arquivo ou local diferentes. Para detalhes, veja [“Configurando suas preferências”](#) mais à frente neste capítulo.

Ocasionalmente, você pode querer examinar ou alterar os atributos associados à suas chaves. Por exemplo, quando você obtém a chave pública de alguém, você pode querer identificar seu tipo (RSA ou Diffie-Hellman/DSS), checar sua impressão digital, ou determinar sua validade baseada em qualquer assinatura digital incluída com a chave. Você pode também querer assinar a chave pública de alguém para indicar que você acredita que ela seja válida, associar um nível de segurança ao proprietário da chave, ou alterar a frase-senha da sua chave privada. Você pode até querer procurar pela chave de alguém em um servidor de chaves. Você executada todas essas funções de gerenciamento de chaves através da janela de PGPkeys.

A janela de PGPkeys

Para abrir o programa PGPkeys, clique Iniciar → Programas → PGP → PGPkeys, ou clique o ícone de PGPtray na sua bandeja de sistema (“system tray”) e então clique “Launch PGPkeys”. A janela de PGPkeys ([figura 6-1](#)) exibe as chaves que você criou para você mesmo, como também quaisquer chaves públicas que você adicionou ao seu chaveiro público.

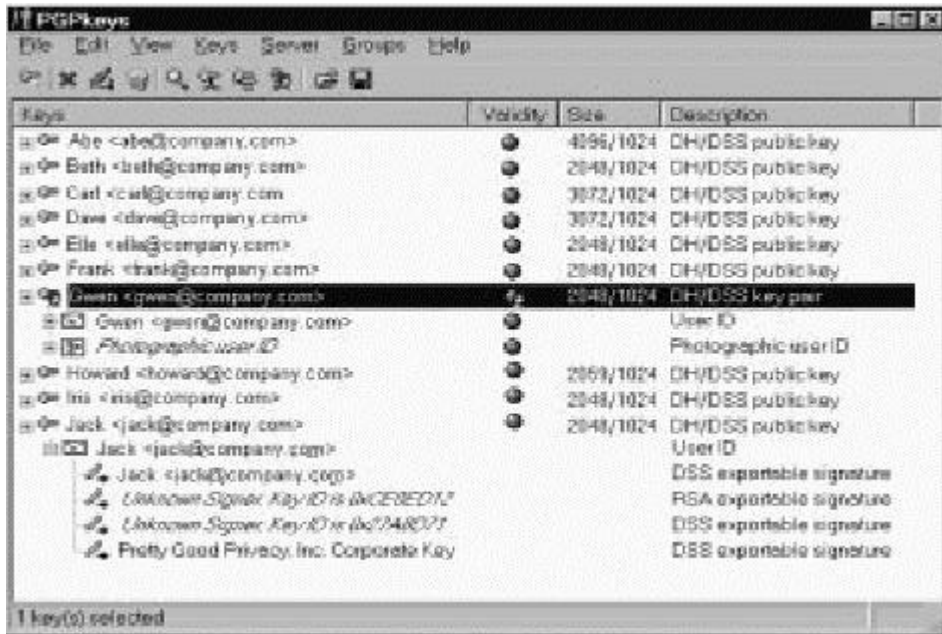





Figura 6-1. A janela de PGPkeys

Um ícone de uma chave e usuário () representa os pares de chave privada e pública que você criou para você mesmo, e chaves simples () representam as chaves públicas que você obteve de outros. Se você tem mais de um tipo de chave, você notará que chaves do tipo RSA são prateadas e chaves Diffie-Hellman/DSS são douradas.

Clicando no sinal “+” do lado esquerdo do ícone da chave, você pode expandir as entradas para exibir o ID do usuário (“user ID”) e endereço de email do proprietário da chave, como representado pelos ícones de envelope (). Clicando o sinal + próximo do ícone do envelope, você pode ver as assinaturas de quaisquer usuários que certificaram o ID do usuário. Se você não quer expandir cada chave individualmente, simplesmente selecione as chaves de interesse e escolha “Expand Selection” (Expandir Seleção) através do menu “Edit”.

Definição dos atributos de PGPkeys

Alguns dos atributos associados com chaves podem ser mostradas na janela principal de PGPkeys. Você pode escolher que atributos deseja tornar visíveis selecionando-os no menu “View”. Para cada item selecionado no menu “View”, PGPkeys exibe uma coluna na janela principal. Se você quiser alterar a ordem destas colunas, clique e arraste o cabeçalho da coluna que deseja mover.

Keys (Chaves)

Exibe uma representação icônica da chave juntamente com o nome do usuário e o endereço de email do proprietário, e os nomes dos assinantes da chave.

Indica o nível de confiança que esta chave realmente pertence ao usuário alegado. A validade é baseada em quem assinou a chave e o quanto você confia no(s) assinante(s) para certificar a autenticidade de uma chave. As chaves públicas que você mesmo assina possuem o maior nível possível de validade, baseado na suposição que você somente assina a chave de alguém se você está totalmente convencido de que ela é válida. A validade de quaisquer outras chaves, que você mesmo não assinou, depende do nível de confiança que você deu a quaisquer outros usuários que assinaram a chave. Se não há assinaturas associadas à chave, ela não é considerada válida, e uma mensagem indicando este fato aparece sempre que você codificar para aquela chave.

Validity (Validade)

Validade é indicada tanto por um círculo quanto por uma barra, dependendo da configuração que você fez em “Advanced Preferences” (Preferências Avançadas), em “Display marginal validity level” (Exibir nível de validade marginal). Veja [“Para configurar preferências avançadas”](#) mais tarde neste capítulo. Se configurada, a validade aparece como:



, uma barra vazia para chaves inválidas



, uma barra cheia pela metade para chaves marginalmente válidas



, uma barra cheia para chaves válidas que você não possui



, uma barra com faixas para chaves válidas que você possui

Se não configurada, então a validade aparece como:



, um círculo cinza para chaves inválidas e chaves marginalmente válidas se a Preferência Avançada “Treat marginally valid keys as invalid” (Tratar chaves marginalmente válidas como inválidas) estiver configurada



possui

Em um ambiente corporativo, seu gerente de segurança pode assinar as chaves dos usuários com a Chave de Assinatura Corporativa. Chaves assinadas com a Chave de Assinatura Corporativa são geralmente assumidas serem completamente válidas. Veja o [Capítulo 3, “Criando e Trocando Chaves”](#), para mais informações.

Size
(Tamanho)

Mostra o número de bits usados para construir a chave. Geralmente, quanto maior a chave, menos chances ela tem de ser comprometida. Entretanto, chaves maiores requerem um pouco mais de tempo para codificar e assinar dados que chaves menores. Quando você cria uma chave Diffie-Hellman/DSS, há um número para a porção Diffie-Hellman e outro número para a porção DSS. A porção DSS é usada para assinar, e a porção Diffie-Hellman para codificar.

Description
(Descrição)

Descreve o tipo de informação exibida na coluna “Keys” (Chaves): tipo de chave, tipo de ID, ou tipo de assinatura.

Additional
Decryption
Key (Chave
de
Decifração
Adicional)

Exibe se a chave possui uma Chave de Decifração Adicional (“Additional Decryption Key”) associada.

Key ID (ID
da Chave)

Um número identificador único associado com cada chave. O número de identificação é útil para distinguir duas chaves que compartilham o mesmo nome de usuário e endereço de email.

Trust
(Confiança)

Indica o nível de confiança que você deu ao proprietário da chave, para servir como apresentador para chaves públicas de outros. Esta confiança fica em jogo quando você está incapacitado de verificar a validade da chave pública de alguém por você mesmo, e ao invés acredita no julgamento de outros usuários que assinaram a chave. Quando você cria um par de chaves, elas são consideradas implicitamente confiáveis, como mostrado pelas faixas nas barras de validade e confiança, ou por um ícone de um ponto verde e usuário.

Quando você recebe uma chave pública que foi assinada por outra das chaves do usuário em seu chaveiro público, o nível

assinante daquela chave. Você associa um nível de confiança, podendo ser Trusted (Confiada), Marginal, ou Untrusted (Não Confiada), na caixa de diálogo "Key Properties" (Propriedades da Chave).

Expiration (Expiração)

Mostra a data que a chave irá expirar. A maioria das chaves é configurada para "Never" (Nunca); entretanto, pode haver casos quando o proprietário de uma chave quer que ela seja usada por apenas um período fixo de tempo.

Creation (Criação)

Mostra a data da criação original da chave. Você às vezes pode fazer uma suposição sobre a validade de uma chave baseado em quanto tempo ela tem estado em circulação. Se a chave tem sido usada por algum tempo, é menos provável que alguém irá tentar trocá-la, porque pode haver muitas outras cópias em circulação. Nunca confie em datas de criação como única indicação de validade.

Examinando as propriedades de uma chave

Além dos atributos gerais mostrados na janela de PGPkeys, você pode também examinar e alterar outras propriedades de chaves e subchaves. Para acessar as Propriedades para uma chave em particular, selecione a chave desejada e então escolha “Properties” do menu “Keys”.

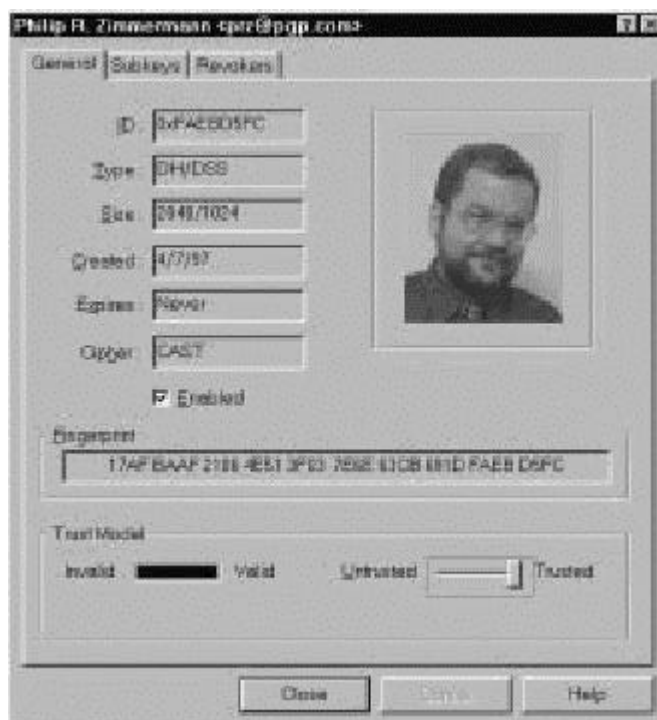


Figura 6-2. Página de propriedades de PGPkeys (caixa de diálogo Propriedades Gerais, ou “General properties”)

Janela de propriedades gerais da chave

Key ID (Identificador da Chave)	Um número identificador único associado com cada chave. Este número de identificação é útil para distinguir duas chaves que compartilham o mesmo nome de usuário e endereço de email.
Key Type (Tipo da Chave)	O tipo de chave, RSA ou Diffie-Hellman/DSS.
Key Size (Tamanho da Chave)	O tamanho da chave
Created (Criada)	A data quando a chave foi criada
Expires (Expira)	A data quando a chave expirar. Proprietários especificam esta data quando eles criam suas chaves, e o valor é geralmente configurado em "Never" (Nunca). Entretanto, algumas chaves são configuradas para expirar em uma data particular se o proprietário quer que elas sejam usadas por um período limitado de tempo.
Cipher (Cifra)	CAST, Triple DES, ou IDEA. Este é o algoritmo "preferido" de codificação, pelo qual o proprietário da chave requer que você codifique para sua chave pública. Se este algoritmo estiver permitido em suas preferências Avançadas, ele será usado sempre que codificando para esta chave.
Join Key (Chave de Junção)	Abre a caixa de diálogo "Key Share Collection". Apenas disponível para chaves divididas. Veja "Assinando e Decifrando arquivos com uma chave dividida" para informações sobre reunir chaves divididas.
Enabled (Habilitada)	Indica se a chave está atualmente habilitada. Quando uma chave está desabilitada, ela fica "escurecida" na janela de PGPkeys e não está disponível para executar quaisquer funções PGP exceto Decifrar e Verificar.

pode habilitá-la novamente a qualquer momento. Para habilitar ou desabilitar uma chave, marque ou desmarque a caixa "Enabled" (a caixa não é visível para chaves implicitamente confiáveis). Este recurso é útil para prevenir que chaves usadas raramente "encham" a caixa de diálogo "Key Selection" (Seleção de Chave) quando você está enviando email codificado.

Change Passphrase (Alterar Frase- Senha)

Altera a frase-senha de uma chave privada. Se você alguma vez pensar que sua frase-senha não é mais um segredo, clique este botão para inserir uma nova frase-senha.

É uma boa idéia alterar sua frase-senha a cada 6 meses mais ou menos. Para instruções sobre alteração de frases-senha, veja "Alterando sua frase-senha", mais tarde neste capítulo.

Fingerprint (Impressão Digital)

Um número de identificação único que é gerado quando a chave é criada. Esta é a forma primária pela qual você pode checar pela autenticidade de uma chave. A melhor forma de checar uma impressão digital é pedir ao proprietário que ele a leia para você pelo telefone de forma que você possa compará-la com a impressão digital exibida para sua cópia da chave pública da pessoa.

Trust Model (Modelo de Confiança)

Indica a validade de uma chave baseado na certificação e no nível de segurança que você tem no proprietário para garantir a autenticidade da chave pública de alguém. Você configura o nível de confiança deslizando a barra para o nível apropriado: Trusted (Confiável), Marginal, ou Untrusted (Não Confiável). A barra estará desabilitada para chaves revogadas, expiradas, e implicitamente confiadas.

Janela de propriedades de subchaves

Valid From (Válido a partir de)	A data quando a subchave torna-se ativa.
Expires (Expira)	A data quando a subchave expira. Proprietários especificam esta data quando eles criam suas subchaves. Subchaves são geralmente ativas por um período limitado de tempo.
Key Size (Tamanho da Chave)	O tamanho da subchave.
New (Nova)	Cria uma nova subchave. Para informações sobre criação de uma nova subchave, veja "Criando novas subchaves" .
Revoke (Revogar)	Revoga a subchave de criptografia atualmente selecionada. Após você revogar a subchave e redistribuir sua chave, outros não estarão mais capacitados de codificar dados para esta subchave.
Remove (Remover)	<p>Permanentemente remove a subchave de codificação atualmente selecionada. Este procedimento não pode ser desfeito. Quaisquer dados que forem codificados para a subchave selecionada não poderão mais ser decifradas.</p> <p>DICA: Use a opção "Revoke" (descrita acima) se você quer desabilitar a subchave e atualize o servidor de chaves. Uma vez que uma subchave tenha sido enviada ao servidor, ela não pode ser removida.</p>

Especificando um par de chaves padrão

Quando codificando mensagens ou arquivos, PGP lhe dá a opção de adicionalmente codificar para um par de chaves que você especifica como seu par de chaves padrão. Quando você assina uma mensagem ou a chave pública de alguém, PGP irá usar este par de chaves por padrão. Seu par de chaves padrão é exibido em negrito para distingui-las de suas outras chaves. Se você possui apenas um par de chaves em seu chaveiro, ele é

automaticamente designado como seu par de chaves padrão. Se você possui mais de um par de chaves, você pode querer designar especificamente um par como seu par padrão.

Para especificar seu par de chaves padrão

1. Abra o programa PGPkeys.
2. Selecione o par de chaves que você quer designar como seu par padrão.
3. Escolha “Set Default” (Configurar como Padrão) do menu “Keys”.

O par de chaves selecionado é exibido em negrito, indicando que ele agora foi designado como seu par de chaves padrão.

Adicionando um novo nome de usuário ou endereço para um par de chaves

Você pode ter mais de um nome de usuário ou endereço de email para o qual quer usar o mesmo par de chaves. Após criar um novo par de chaves, você pode adicionar nomes alternativos e endereços às chaves. Você pode adicionar um novo nome ou endereço de email apenas se você possuir tanto a chave privada quanto a pública.

Para adicionar um novo nome de usuário ou endereço a uma chave existente

1. Abra o programa PGPkeys.
2. Selecione o par de chaves para o qual você quer adicionar outro nome de usuário ou endereço.
3. Escolha “Add/Name” (Adicionar/Nome) no menu “Keys”.

A caixa de diálogo “New User Name” (Novo Nome de Usuário) aparece ([figura 6-3](#)).

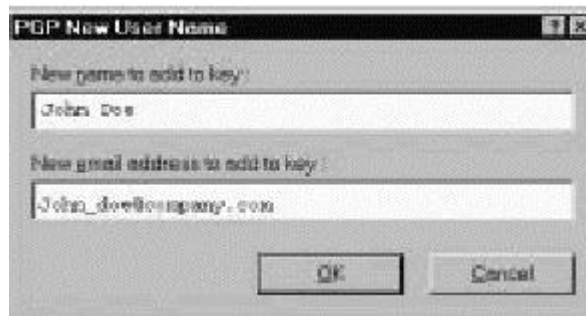


Figura 6-3. A caixa de diálogo “New User Name”

4. Entre o novo nome e endereço de email nos campos apropriados, e então clique OK.

A caixa de diálogo “Enter Passphrase” é aberta.

5. Entre sua frase-senha, então clique OK.

O novo nome é adicionado ao fim da lista de nomes de usuários associados com a chave. Se você quer configurar o novo nome de usuário e endereço como identificadores primários para sua chave, selecione o nome e endereço e então escolha “Set as Primary Name” (Configurar como Nome Primário) no menu “Keys”.


Verificando a chave pública de alguém

No passado era difícil saber com certeza se uma chave pertencia a uma pessoa em particular, a não ser que a pessoa fisicamente entregasse a chave para você em um disquete. Trocar chaves desta maneira não é usualmente prático, especialmente para usuários que estão localizados a muitos quilômetros de distância.

Há várias formas de se checar a impressão digital de uma chave, mas a mais segura é chamar a pessoa e pedir a ela que leia a impressão digital para você pelo telefone. A não ser que a pessoa seja alvo de um ataque, é muito difícil que alguém fosse capaz de interceptar esta chamada aleatória e imitar a pessoa que você espera ouvir do outro lado. Você também pode comparar a impressão digital ou fotografia em sua cópia da chave pública de alguém com a impressão digital ou fotografia na chave original em um servidor público.

Para checar uma chave pública com a impressão digital da chave

1. Abra o programa PGPkeys.
2. Selecione a chave pública que você deseja verificar.

3. Escolha “Properties” (Propriedades) do menu “Keys” ou clique () para abrir a janela de Propriedades.

A janela de propriedades se abre, como mostrado na [figura 6-4](#).

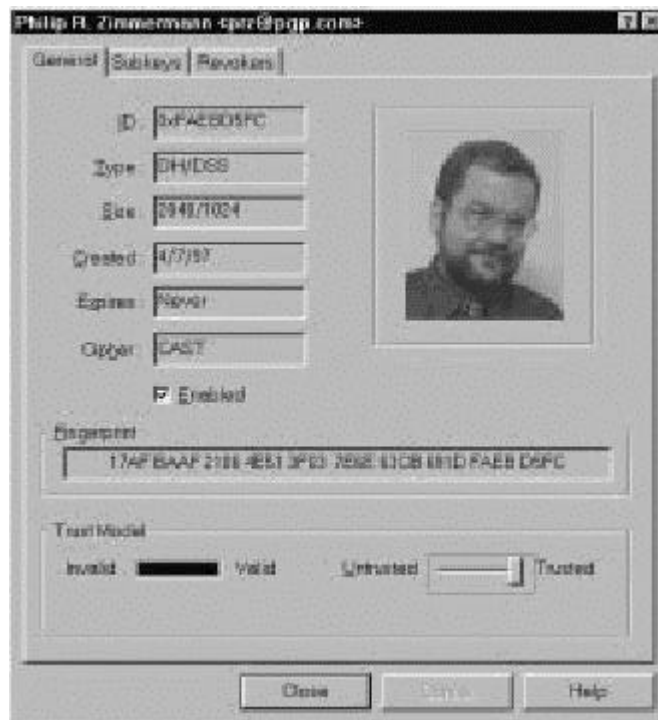


Figura 6-4. Janela de Propriedades

4. Use os caracteres exibidos na caixa de texto “Fingerprint” para comparar com a impressão digital original.

Assinando a chave pública de alguém

Quando você cria um conjunto de chaves, as chaves são automaticamente assinadas usando sua chave pública. Da mesma forma, uma vez que você está certo de que uma chave pertence à pessoa correta, você pode assinar a chave pública desta pessoa, indicando que você está certo de que ela é uma chave válida. Quando você assina a chave pública de alguém, um ícone associado com seu nome de usuário é exibido para aquela chave.

Para assinar a chave pública de alguém

1. Abra o programa PGPkeys.
2. Selecione a chave pública que você quer assinar.

3. Escolha “Sign” no menu “Keys” ou clique para abrir a janela “Sign Keys”.

A janela “Sign Keys” aparece ([figura 6-5](#)) com a chave pública e a impressão digital exibida em uma caixa de texto.

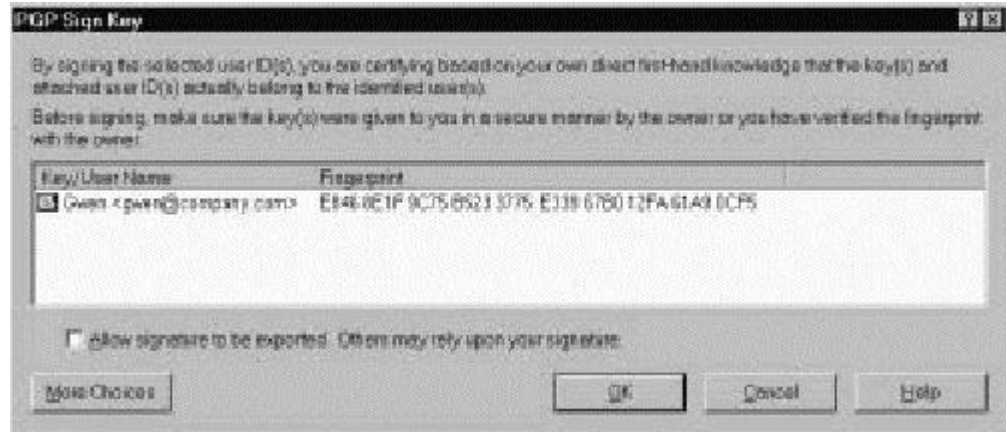


Figura 6-5. Janela “Sign Keys” (menos opções)

4. Clique a caixa “Allow signature to be Exported...” (Permitir que a assinatura seja exportada), para permitir que sua assinatura seja exportada com esta chave.

Uma assinatura exportável é aquela pode ser enviada aos servidores e viajar com a chave sempre que ela é exportada, como arrastando-a para uma mensagem de email. A caixa “Allow signature to be Exported...” é uma forma rápida de indicar que você quer exportar sua assinatura.

Ou

Clique o botão “More Choices” (Mais Opções) para configurar opções, como tipo de assinatura e expiração da assinatura ([Figura 6-6](#)).

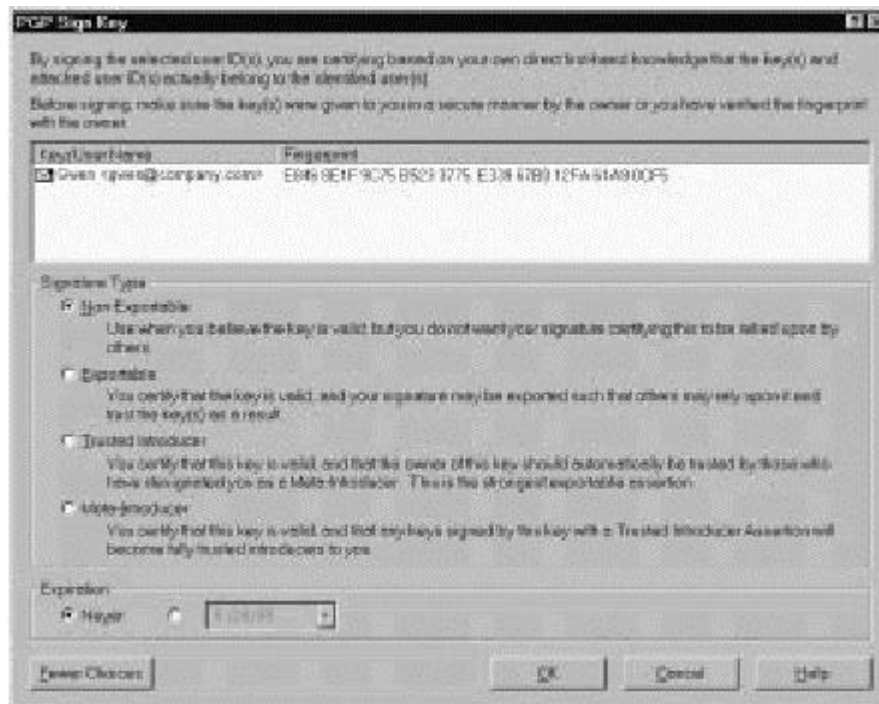


Figura 6-6. Janela “Sign Keys” (mais opções)

Escolha um tipo de assinatura com a qual assinar a chave pública. Suas opções são:

- **Não exportável.** Use esta assinatura quando você acredita que a chave é válida, mas não quer que outros se baseiem em sua certificação. Este tipo de assinatura não pode ser enviado com a chave associada para um servidor de chaves, ou exportada de qualquer forma.
- **Exportável.** Use assinaturas exportáveis em situações onde sua assinatura é enviada com a chave para um servidor de chaves, de forma que outros possam basear-se em sua assinatura e confiar em suas chaves como resultado. Isto é equivalente a marcar a caixa “Allow signature to be exported...” no menu “Sign Keys”.
- **Meta-Apresentador.** Certifica que esta chave e quaisquer chaves assinadas por esta chave com uma Assertiva de Validade de um Apresentador Confiável são apresentadores completamente confiáveis para você. Este tipo de assinatura não é exportável.
- **Apresentador Confiável.** Use esta assinatura em situações onde você certifica que esta chave é válida, e que o proprietário da chave deve ser completamente confiado para certificar outras chaves. Este tipo de assinatura é exportável. Você pode restringir as capacidades de validação do apresentador confiável para um domínio particular de email.

5. Clique o botão “Sign” (Assinar).

A janela de “Passphrase” aparece.

6. Insira sua frase-senha, então clique OK.

Um ícone associado com seu nome de usuário agora é incluído com a chave pública que você acaba de assinar.

Concedendo confiança a validação de chaves

Além de certificar que uma chave pertence a alguém, você pode associar um nível de confiança ao usuário das chaves indicando o quanto você confia neles para agir como um apresentador para outros cujas chaves você pode obter no futuro. Isto significa que se você alguma vez obter uma chave de alguém que foi assinada por uma pessoa para quem você designou como confiável, a chave é considerada válida mesmo que você mesmo não tenha feito a checagem.

Para conceder confiança a uma chave

1. Abra o programa PGPkeys.
2. Na janela PGPkeys, selecione a chave para qual você quer alterar o nível de segurança.

NOTA: Você deve assinar a chave antes de configurar o nível de confiança para ela. Se você não assinou a chave ainda, veja [“Assinando a chave pública”](#) para instruções.


3. Escolha “Properties” (Propriedades) do menu “Keys” ou clique () para abrir a janela de Propriedades, como mostrado na [figura 6-4](#).
4. Use a barra deslizante “Trust Level” (Nível de Confiança) para escolher o nível apropriado de segurança para o par de chaves.



Figura 6-7. Caixa de diálogo “Trust Level”

5. Feche a caixa de diálogo para aceitar a nova configuração.

Desabilitando e habilitando chaves

Às vezes você pode querer temporariamente desabilitar uma chave. A habilidade de desabilitar chaves é útil quando você quer manter uma chave pública para uso futuro, mas não quer que elas “encham” sua lista de destinatários a cada vez que você envia email.

Para desabilitar uma chave

1. Abra o programa PGPkeys.
2. Na janela de PGPkeys, selecione a chave que você deseja desabilitar.
3. Selecione “Disable” (Desabilitar) no menu “Keys”.

A chave é escurecida e está temporariamente desabilitada para uso.

Para habilitar uma chave

1. Abra o programa PGPkeys.
2. Selecione a chave que você deseja habilitar.
3. Selecione “Enable” (Habilitar) no menu “Keys”.

A chave torna-se visível e pode ser usada como antes.


Apagando uma chave, assinatura, ou ID de usuário

Em algum momento você pode querer remover uma chave, uma assinatura, ou um ID de usuário associado com uma chave em particular.

NOTA: Quando você apaga uma chave, uma assinatura, ou um ID de usuário de uma chave, ela é removida e não é recuperável. Assinaturas e IDs de usuário podem ser re-adicionadas a uma chave, e uma chave pública importada pode ser re-importada para seu chaveiro. Entretanto, uma chave privada que exista apenas em seu chaveiro não pode ser recriada, e todas as mensagens codificadas para as cópias de sua respectiva chave pública não poderão mais ser decifradas.

Para apagar uma chave, uma assinatura, ou um ID de usuário

1. Abra o programa PGPkeys.
2. Selecione a chave, assinatura, ou ID de usuário que você deseja apagar.

3. Escolha “Delete” do menu “Edit” ou clique () na barra de ferramentas de PGPkeys.


A caixa de diálogo “Confirmation” (Confirmação) aparece.

4. Clique o botão OK.

Alterando sua Frase-Senha

É uma boa prática alterar sua frase-senha em intervalos regulares, talvez a cada três meses. Mais importante, você deve alterar sua frase-senha no momento que crer que ela foi comprometida, por exemplo, por alguém olhando por sobre seus ombros enquanto você a digitou.

Para alterar sua frase-senha

1. Abra o programa PGPkeys.
2. Selecione sua chave listada na janela de PGPkeys.
3. Escolha “Properties” do menu “Keys” ou clique () para abrir a caixa de diálogo “Properties” (Propriedades).

A caixa de diálogo “Properties” aparece (veja [figura 6-4](#)).

4. Clique “Change Passphrase” (Alterar Frase-Senha).

A caixa de diálogo “Passphrase” aparece.

NOTA: Se você quer alterar a frase-senha para uma chave dividida, você deve primeiro reunir as partes da chave. Clique “Join” (Juntar) para obter as partes da chave. Veja [“Assinando e decifrando arquivos com uma chave dividida”](#) para informações sobre obtenção de partes de chaves.

5. Entre sua frase-senha atual no espaço provido, então clique OK.

A caixa de diálogo “Change Passphrase” aparece.

6. Insira sua nova frase-senha na primeira caixa de texto. Pressione a tecla “Tab” para avançar à próxima caixa de texto e confirmar sua entrada inserindo sua nova frase-senha novamente.
7. Clique OK.

ATENÇÃO: Se você está alterando sua frase-senha porque sente que sua frase-senha foi comprometida, você deve eliminar todos os chaveiros de *backup* e eliminar seu espaço livre.

Importando e Exportando Chaves

Apesar de você frequentemente distribuir sua chave pública e obter as chaves públicas de outros cortando e colando o texto puro de um servidor de chaves público ou corporativo, você também pode trocar chaves importando-as e exportando-as como arquivos texto separados. Por exemplo, alguém poderia entregar-lhe um disco contendo sua chave pública, ou você poderia tornar sua chave pública disponível em um servidor FTP.

Para importar uma chave de um arquivo

1. Abra o programa PGPkeys.
2. Escolha “Import” (Importar) no menu “Keys”.

A caixa de diálogo “Import” aparece.

3. Selecione o arquivo que contém a chave que você quer importar, então clique “Open” (Abrir).

A caixa de diálogo “Import Selection” (Importar Seleção) é aberta.

4. Selecione a(s) chave(s) que você deseja importar para seu chaveiro, então clique o botão “Import”.
5. A(s) chave(s) importada(s) aparece(m) na janela de PGPkeys, onde você pode usá-la(s) para codificar dados ou para verificar a assinatura digital de alguém.

Para adicionar uma chave de uma mensagem de email

Se um colega enviar-lhe uma mensagem de email com sua chave dentro (como um bloco de texto) você pode adicioná-la a seu chaveiro.

1. Enquanto a janela da mensagem de email está aberta, abra a janela de PGPkeys.
2. Coloque as duas janelas lado a lado de forma que você possa ver parte da janela de PGPkeys atrás da janela da mensagem.
3. Selecione o texto da chave, incluindo o texto “BEGIN PGP PUBLIC KEY BLOCK” e “END PGP PUBLIC KEY BLOCK”, e arraste o texto na janela de PGPkeys.

A caixa de diálogo “Import Selection” (Importar Seleção) é aberta.

4. Selecione a(s) chave(s) que você deseja importar para seu chaveiro, então clique o botão “Import”.
5. A(s) chave(s) importada(s) aparece(m) na janela de PGPkeys, onde você pode usá-la(s) para codificar dados ou para verificar a assinatura digital de alguém.

Para exportar uma chave para um arquivo

1. Abra o programa PGPkeys.
2. Selecione a chave que você quer exportar para um arquivo.
3. Escolha “Export” (Exportar) no menu “Keys”.

A caixa de diálogo “Export” aparece.

4. Insira o nome do arquivo ou navegue ao arquivo para onde você quer que a chave seja exportada, e clique “Save”.

A chave exportada é salva no arquivo com o nome dado na pasta especificada.

Revogando uma chave

Se alguma vez acontecer de você não mais confiar em seu par pessoal de chaves, você pode emitir uma revogação para o mundo dizendo para pararem de usar sua chave pública.

A melhor forma de circular uma chave revogada é colocá-la em um servidor de chaves públicas .

Para revogar uma chave

1. Abra o programa PGPkeys.
2. Selecione o par de chaves que você quer revogar.
3. Escolha “Revoke” no menu “Keys”.

A caixa de diálogo “Revocation Confirmation” (Confirmação de Revogação) aparece.

4. Clique OK para confirmar seu intuito de revogar a chave selecionada.

A caixa de diálogo “Enter Passphrase” aparece.

5. Insira sua frase-senha, então clique OK.

Quando você revoga uma chave, ela é cruzada com uma linha vermelha para indicar que ela não é mais válida.

6. Envie a chave revogada ao servidor de forma que todos saberão que não devem mais usar sua chave antiga.

É possível que você se esqueça sua frase-senha algum dia ou perca sua chave privada. Em qualquer desses casos, você nunca mais poderá usar sua chave novamente, e você não terá como revogar sua chave antiga quando criar uma nova chave. Para se prevenir contra esta possibilidade, você pode apontar uma outra pessoa como revogador da chave em seu chaveiro público, para revogar sua chave. Esta pessoa que você designar poderá revogar sua chave DH/DSS, enviá-la ao servidor e será como se você a tivesse revogado você mesmo.

Para apontar um revogador designado

1. Abra o programa PGPkeys.
2. Selecione o par de chaves para o qual você quer designar um revogador.

3. Selecione “Add/Revoker” (Adicionar/Revogador) do menu “Keys”.

Uma caixa de diálogo é aberta e mostra uma lista de chaves.

4. Selecione a(s) chave(s) na lista de “User ID” que você quer apontar como um revogador designado.

5. Clique OK.

Uma caixa de diálogo de confirmação aparece.

6. Clique OK para continuar.

A caixa de diálogo “Passphrase” aparece.

7. Insira sua frase-senha, então clique OK.

8. A(s) chave(s) selecionada(s) agora está(ão) autorizada(s) a revogar sua chave. Para um gerenciamento efetivo de chaves, distribua uma cópia atual de sua chave para o(s) revogador(es) ou envie sua chave para o servidor. Veja [“Distribuindo sua chave pública”](#) para instruções.

Configurando suas preferências

PGP é configurado para acomodar as necessidades da maioria dos usuários, mas você tem a opção de ajustar algumas das configurações para adequá-las a seu ambiente particular de computação. Você especifica estas configurações através da caixa de diálogo “Preferences” (Preferências) do menu “Edit” de PGPkeys.

Para configurar preferências gerais

1. Abra o programa PGPkeys.
2. No menu “Edit” de PGPkeys, escolha “Preferences”.

O menu “Preferences” se abre com a aba “General” (Geral) aparecendo ([figura 6-8](#)).



Figura 6-8. Caixa de diálogo “Preferences” (aba General)

3. Selecione as configurações gerais de codificação na aba “General”. Suas opções são:
 - o **Always Encrypt to Default Key** (Sempre Codificar para a Chave Padrão). Quando esta configuração está habilitada, todas as mensagens de email e arquivos anexados que você codificar com a chave pública de um destinatário também serão codificadas para você, usando sua chave pública padrão. É útil deixar esta configuração habilitada, para que você tenha a opção de decifrar

os conteúdos de quaisquer emails ou arquivos que você codificou anteriormente.

- **Faster Key Generation** (Geração Mais Rápida de Chave). Quando esta configuração está habilitada, é necessário menos tempo para gerar um novo par de chaves Diffie-Hellman/DSS. Este processo é acelerado usando um conjunto previamente calculado de números primos, ao invés de passar pelo demorado processo de criá-los a partir do zero a cada vez que uma nova chave é gerada. Entretanto, lembre-se de que a geração mais rápida de chaves está implementada apenas para as opções de tamanhos fixos e pré-definidos de chaves acima de 1024 e abaixo de 4096 quando se cria uma chave, e não é útil se você entrar outro valor qualquer. Apesar de ser difícil para qualquer um quebrar sua chave baseado no conhecimento desses números primos pré-preparados, algumas pessoas podem querer gastar este tempo extra para criar um par de chaves com nível máximo de segurança.

A crença geral da comunidade criptográfica é que usar números primos pré-preparados não provê diminuição de segurança para algoritmos Diffie-Hellman/DSS. Se este recurso o deixa desconfortável, você pode desabilitá-lo. Para maiores informações, leia o FAQ localizado no website da Network Associates.

- **Cache Decryption Passphrases for...** (Guardar Frases-Senhas de Decifração por...) Quando esta configuração está habilitada, sua frase-senha de decifração é automaticamente armazenada na memória de seu computador. Especifique a frequência (em horas: minutos: segundos) na qual você deseja salvar sua frase-senha. O valor padrão é 2 minutos.
- **Cache Signing Passphrases for...** (Guardar Frases-Senhas de Assinatura por...) Quando esta configuração está habilitada, sua frase-senha de assinatura é automaticamente armazenada na memória de seu computador. Especifique a frequência (em horas: minutos: segundos) na qual você deseja salvar sua frase-senha de assinatura. O valor padrão é 2 minutos.
- **Comment Block** (Bloco de Comentário). Você pode adicionar um texto de comentário nesta área. O texto sempre será incluído em mensagens e arquivos que você codificar ou assinar.
- **Warn Before Wiping Files** (Avisar Antes de Eliminar Arquivos). Quando esta configuração está habilitada, uma caixa de diálogo aparece antes de você eliminar um arquivo, para lhe dar uma última chance de mudar de idéia antes que PGP sobrescreva

seguramente o conteúdo do arquivo e apague-o de seu computador.

4. Clique OK para salvar suas alterações e retornar ao menu PGPkeys, ou escolha outra aba para continuar a configurar suas preferências de PGP.

Para configurar preferências de arquivos

Use a aba “Files” (Arquivos) para especificar a localização dos chaveiros utilizados para armazenar suas chaves privadas e públicas.

1. Abra o programa PGPkeys.
2. Selecione “Preferences” no menu “Edit” de PGPkeys, então escolha a aba “Files”.

O menu “Preferences” se abre com a aba “Files” (Arquivos) aparecendo ([figura 6-9](#)).

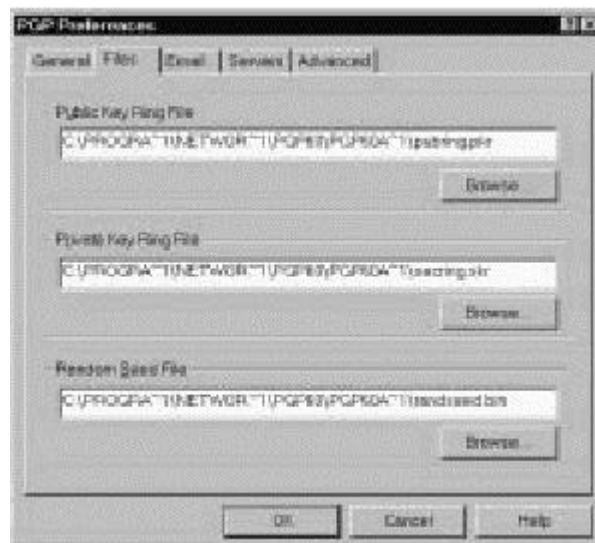


Figura 6-9. Caixa de diálogo “Preferences” (aba Files)

3. Use os botões listados na aba “Arquivos” para configurar os locais apropriados para seus chaveiros públicos e privados, e/ou o arquivo de inicialização de números aleatórios:
 - o **Public Keyring File** (Arquivo do Chaveiro Público). Exibe o local atual e o nome do arquivo onde PGP espera encontrar o arquivo de seu chaveiro público. Se você pretende armazenar suas

chaves públicas em um arquivo com um nome diferente, ou em algum outro local, você especifica esta informação aqui. O local que você especificar também será usado para armazenar todos os *backups* automáticos de seu chaveiro público.

- **Private Keyring File** (Arquivo do Chaveiro Privado). Exibe o local atual e o nome do arquivo onde PGP espera encontrar o arquivo de seu chaveiro privado. Se você pretende armazenar suas chaves privadas em um arquivo com um nome diferente, ou em algum outro local, você especifica esta informação aqui. Alguns usuários gostam de manter suas chaves privadas em um disquetes, que eles então inserem como uma chave “real” sempre que precisam assinar ou decifrar arquivos. O local que você especificar também será usado para armazenar todos os *backups* automáticos de seu chaveiro privado.
 - **Set Random Seed Location** (Configurar Localização do Arquivo de Inicialização de Números Aleatórios). Exibe a localização do arquivos de inicialização de números aleatórios. Alguns usuários podem desejar manter seu arquivo de inicialização de números aleatórios em um local seguro para prevenir-se de alterações. Já que este método de ataque é bastante difícil, e já foi antecipado por PGP, mover o arquivo de inicialização de números aleatórios de seu local padrão é de pouca vantagem.
4. Clique OK para salvar suas alterações e retornar ao menu PGPkeys, ou escolha outra aba para continuar a configurar suas preferências de PGP.

Para configurar preferências de email

Use a aba “Email” para especificar as preferências que afetam a forma que as funções de PGP são implementadas para seu aplicativo particular de email. Lembre-se de que nem todas as seleções podem se aplicar a seu programa particular de email.

1. Abra o programa PGPkeys.
2. Selecione “Preferences” no menu “Edit” de PGPkeys, e clique a aba “Email”.

O menu “Preferences” abre-se, com a aba “Email” aparecendo ([Figura 6-10](#)).

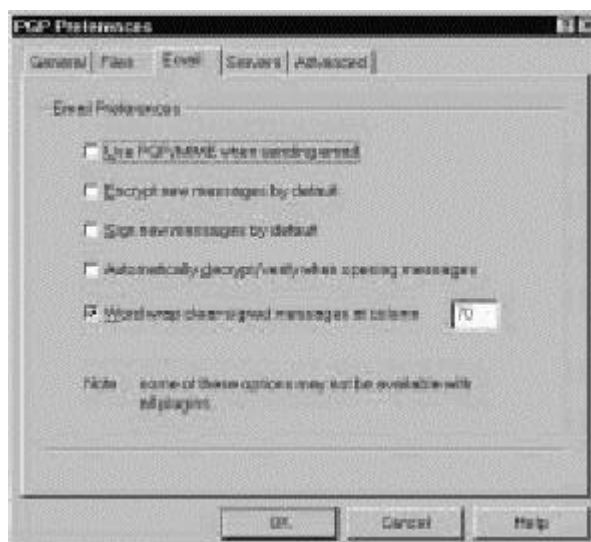


Figura 6-10. Caixa de diálogo “Preferences” (aba Email)

3. Selecione suas preferências de codificação de email na aba “Email”. Suas opções são:
 - **Use PGP/MIME when sending mail** (Usar PGP/MIME quando enviando correspondência). Se você estiver usando Eudora e habilitar esta configuração, todas as suas mensagens de email e arquivos anexados serão automaticamente codificados para os destinatários especificados. Esta configuração não tem efeito em outras codificações que você fizer através da Área de Transferência ou com o Windows Explorer e não deve ser usada se você planeja enviar email para destinatários cujo aplicativo de email não suporte o padrão PGP/MIME. Usando Eudora, anexos sempre serão codificados seja qual for esta configuração, mas se o destinatário não possuir PGP/MIME, o processo de decifração será mais manual.
 - **Encrypt new messages by default** (Codificar novas mensagens por padrão). Se você habilitar esta configuração, todas as suas mensagens de email e anexos de arquivos são automaticamente codificadas. Alguns aplicativos de email não suportam este recurso.
 - **Sign new messages by default** (Assinar novas mensagens por padrão). Se você habilitar esta configuração, todas as suas mensagens de email e anexos de arquivos são automaticamente assinadas. Alguns aplicativos de email não suportam este recurso. Este recurso não tem efeito em outras assinaturas que você adicionar através da Área de Transferência ou com o Windows Explorer.

- **Automatically decrypt/verify when opening messages**
(Automaticamente decifrar/verificar quando abrindo mensagens). Se você habilitar esta configuração, todas as suas mensagens de email e anexos de arquivos que estão codificados e/ou assinados são automaticamente decifrados e verificados. Alguns aplicativos de email não suportam este recurso.

- **Word wrap clear-signed messages at column []** (Quebrar linha em mensagens de texto na coluna []). Esta configuração especifica o número da coluna onde um sinal “carriage return” é usado para quebrar o texto em sua assinatura digital para a próxima linha. Este recurso é necessário porque nem todos os aplicativos manipulam a quebra de linha da mesma forma, o que poderia fazer com que as linhas em sua mensagem assinada digitalmente fossem quebradas de uma forma que não poderiam ser facilmente lidas. A configuração padrão é 70, o que previne problemas com a maioria dos aplicativos.

ATENÇÃO: Se você alterar a configuração de quebra de linha em PGP, certifique-se de que ela é menor que a configuração de quebra de linha em seu aplicativo de email. Se você a configurar para um tamanho igual ou maior, sinais de “carriage return” podem ser adicionados e invalidar sua assinatura PGP.

4. Clique OK para salvar suas alterações e retornar ao menu PGPkeys, ou escolha outra aba para continuar a configurar suas preferências de PGP.

Para configurar preferências de servidores

Use a aba “Server” (Servidor) para especificar configurações para os servidores de chaves públicas que você está usando para enviar e obter chaves públicas, com os quais você automaticamente sincroniza chaves.

1. Abra o programa PGPkeys.
2. Selecione “Preferences” no menu “Edit” de PGPkeys, então escolha a aba “Server”.
3. O menu “Preferences” se abre com a aba “Server” (Servidor) aparecendo ([figura 6-11](#)).

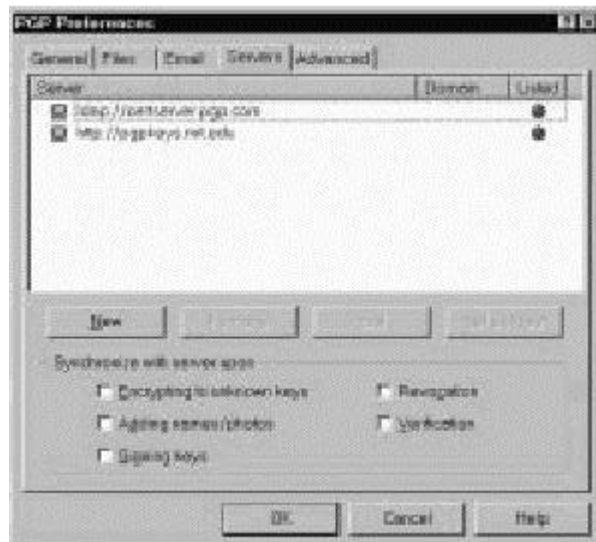


Figura 6-11. Caixa de diálogo “Preferences” (aba Server)

A coluna “Domain” (Domínio) lista o domínio Internet (algo como “companhia.com”) do(s) servidor(es) disponível(is). Quando enviando chaves a um servidor, PGP tenta encontrar o domínio da chave nesta lista, e assim encontrar a entrada apropriada no servidor. Se o domínio não for encontrado, um servidor para o primeiro servidor de domínio mundial que serve todas as chaves será usado, e outros servidores de domínio mundial a seguir na lista poderão ser procurados se a primeira procura não for bem sucedida.

4. Para configurar suas preferências de servidores, use estes botões:
 - **New** (Novo). Adiciona um novo servidor à sua lista.
 - **Remove** (Remover). Remove o servidor atualmente selecionado de sua lista.
 - **Edit** (Editar). Permite que você edite informações do servidor para o servidor atualmente selecionado.
 - **Set root server** (Especificar servidor raiz). Identifica o servidor raiz que é usado para operações específicas de corporações, como atualizar listas de grupos, enviar listas de grupos, atualizar apresentadores etc. Em configurações corporativas, seu gerente de segurança já terá configurado isto.

5. Na área “Synchronize with server upon:” (Sincronizar com o servidor quando:), selecione as opções para usar quando sincronizando seu chaveiro privado com seu(s) servidor(es) de chaves. Suas opções são:

- **Encrypting to unknown keys** (Codificando para chaves desconhecidas). Selecione esta opção para fazer com que PGP automaticamente procure destinatários desconhecidos no servidor, para localizar usuários que não estão em seu chaveiro quando codificado email.
 - **Adding names/photos/revokers** (Adicionando nomes/fotos/revogados). Selecione esta opção para fazer com que chaves para as quais você adicionou nomes, fotografias, ou revogados sejam primeiro atualizadas a partir do servidor e então suas alterações enviadas ao servidor após completar a atualização. Atualizar a chave antes certifica que, por exemplo, a chave não foi revogada desde a última vez que você a atualizou.
 - **Signing keys** (Assinando chaves). Selecione esta opção para fazer com que chaves para as quais você está adicionando sua assinatura sejam primeiro atualizadas a partir do servidor e então suas alterações enviadas ao servidor após completar a atualização.
 - **Revocations** (Revogações). Selecione esta opção para fazer com que chaves que você está revogando sejam primeiro atualizadas a partir do servidor e então suas alterações enviadas ao servidor após completar a atualização.
 - **Verification** (Verificação). Selecione esta opção para fazer com que PGP automaticamente procure e importe a partir do servidor de chaves quando verificando um email ou arquivo assinado para o qual você não possui a chave pública do emitente.
6. Clique OK para salvar suas alterações e retornar ao menu PGPkeys, ou escolha outra aba para continuar a configurar suas preferências de PGP.

Para adicionar um servidor de chaves à lista de servidores

1. Abra a janela de preferências (“Preferences”). então clique a aba “Servers”.
2. Clique o botão “New” (Novo).

A caixa de diálogo “Add New Server” (Adicionar Novo Servidor) aparece, como mostrado na [figura 6-12](#).

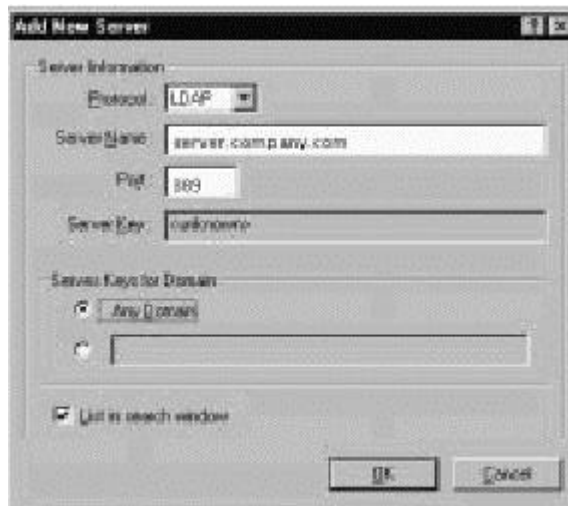


Figura 6-12. Caixa de diálogo “Add New Server”

3. Na caixa “Protocol” (Protocolo), selecione um protocolo para usar para acessar o servidor. Suas opções são LDAP, LDAPS, e HTTP.
4. Na caixa “Server Name” (Nome do Servidor), entre o nome de domínio ou endereço IP do servidor. Por exemplo, servidor.companhia.com ou 123.445.67.
5. Digite o número da porta do servidor na caixa “Port” (Porta). Por exemplo, 11371 é usada por servidores de certificação HTTP antigos, 389 é comumente usada para servidores de certificação LDAP usados comumente.
6. A caixa “Server Key” (Chave do Servidor) é usada por servidores LDAPS. A chave do servidor é usada pelo servidor para autenticar uma conexão (informações sobre chaves não são exibidas até que você se conecte ao servidor).
7. Selecione a opção “Any Domain” (Qualquer Domínio) para permitir que PGP envie chaves a partir de qualquer domínio para este servidor de chaves. Esta opção está habilitada por padrão.

Se você quer que PGP envie apenas chaves de um domínio específico para este servidor de chaves, selecione a opção abaixo de “Any Domain”. Então, insira o nome do domínio no espaço fornecido. Por exemplo, se você especificar o domínio companhia.com, apenas aquelas chaves cujo endereço de email terminem com companhia.com serão enviados para este servidor.

8. Selecione a caixa “List in Search Window” (Listar na Janela de Pesquisa) se você quer que este servidor de chaves seja listado na janela de pesquisa de PGPkeys.

Para configurar preferências avançadas

Use a aba “Advanced” para exibir a aba onde você selecione algoritmos de criptografia de chaves e opções de confiança para chaves.

PGP dá a você a opção de selecionar e/ou alterar algoritmos de criptografia de chaves. Você pode selecionar o algoritmo de criptografia para suas chaves PGP: CAST (o padrão), IDEA, ou Triple-DES. Se você deseja usar IDEA ou Triple-DES, você deve fazer a seleção antes de gerar suas chaves. CAST é um novo algoritmo no qual PGP e outros criptógrafos possuem uma confiança muito alta, e Triple-DES é um algoritmo do governo dos EUA que tem suportado o teste do tempo. IDEA é o algoritmo usado por todas as chaves RSA geradas por PGP. Para maiores informações sobre estes algoritmos, veja [“Os algoritmos simétricos de PGP”](#).

A escolha para “Preferred Algorithm” (Algoritmo Preferido) afeta o seguinte:

- Quando usando “codificação convencional”, a cifra preferida é usada para codificar.
- Quando criando uma chave, a cifra preferida é gravada como parte da chave de forma que outras pessoas irão usar este algoritmo quando codificando para você.

A escolha para “Allowed Algorithm” (Algoritmos Permitidos) afeta o seguinte:

- Quando criando uma chave, as cifras permitidas são gravadas como parte da chave de forma que outras pessoas irão usar um destes algoritmos quando codificando para você, se o algoritmo preferido não estiver disponível para eles.

NOTA: Codificação para uma chave pública irá falhar se nenhum dos algoritmos preferidos (“Preferred Algorithm”) ou nenhum dos algoritmos disponíveis (“Allowed Algorithms”) estiverem disponíveis para a pessoa que está codificando a mensagem.

ATENÇÃO: Use as caixas para CAST, IDEA, e Triple-DES apenas se você subitamente decidiu que um algoritmo em particular não é seguro. Por exemplo, se você ficar sabendo que Triple-DES foi quebrado, você pode deselegionar aquela caixa e todas as novas chaves que você gerar terão um registro que indicará que Triple-DES não deve ser usado quando codificando para você.

PGP lhe dá a opção de selecionar e/ou alterar como a confiança de uma chave é exibida, e se você deseja ou não ser avisando quando você codificar uma mensagem para uma chave


pública que possui uma Chave Adicional de Decodificação (ADK, “Additional Decryption Key”) associada. Na seção “Trust Model” (Modelo de Confiança), escolha uma das opções:

- **Display marginal validity level** (Exibir nível de validade marginal). Use esta caixa para especificar se chaves marginalmente válidas devem ser exibidas como tal, ou simplesmente exibir a validade como “on” (ativada) ou “off” (desativada). Validades marginais aparecem como ícones de barras possuindo diferentes padrões de sombra. Validade ativada/desativada aparece como ícones de círculos; verde para válidas, cinza para inválidas (a chave não foi validada, ela não foi assinada nem por um apresentador confiável nem por você).
- **Treat marginally valid keys as invalid** (Tratar chaves marginalmente válidas como inválidas). Use esta caixa para especificar se deve-se tratar todas as chaves marginalmente válidas como inválidas. A seleção desta opção causa a caixa de diálogo “Key Selection” (Seleção de Chaves) surgir sempre que você codificar para chaves marginalmente válidas.
- **Warn when encrypting to an ADK** (Avisar quando codificando para uma ADK). Use esta caixa para especificar se você quer que PGP emita um aviso sempre que uma chave com a qual se codificará possui uma Chave Adicional de Decodificação (ADK, “Additional Decryption Key”) associada.
- **Export format** (Formato de Exportação).
 - **Compatible** (Compatível): Exporta chaves em um formato compatível com versões anteriores de PGP.
 - **Complete** (Completa): Exporta para o novo formato de chaves, que inclui IDs fotográficos.

Procurando por uma chave

Você pode procurar por chaves em chaveiros locais e servidores remotos de chaves.

Para procurar pela chave de um usuário

1. Abra o programa PGPkeys.
2. Escolha “Search” (Procurar) a partir do menu “Server” ou clique o botão “Search” () no menu de PGPkeys.

A janela de procura de PGPkeys aparece.

3. Escolha o servidor que você deseja pesquisar através do menu “Search for Keys On” (Procurar por Chaves Em).
4. Especifique seu critério de procura:

O padrão é ID de usuário (“User ID”), mas você pode clicar as setas para selecionar “Key ID” (ID da Chave), “Key Status” (Status da Chave), “Key Type” (Tipo de Chave), “Key Size” (Tamanho da Chave), “Creation Date” (Data de Criação), ou “Expiration Date” (Data de Expiração). Por exemplo, você poderia procura por todas as chaves com o ID de usuário de Fred.

5. Especifique a condição pela qual você está procurando.

Você pode usar qualquer uma das seguintes condições:

- Contains (Contém)
- Does Not Contain (Não Contém)
- Is (É)
- Is Not (Não É)
- Is Signed By (É Assinado Por)
- Is Not Signed By (Não É Assinado Por)

- Is At Least (É Ao Menos) (para datas de criação ou expiração)
 - Is At Most (É No Máximo) (para datas de criação ou expiração)
6. Entre o valor pelo qual você quer pesquisar.
 7. Clique “More Choices” (Mais Opções) para adicionar critérios adicionais para sua pesquisa; por exemplo, IDs de chaves com o nome Fred criados em ou antes de 6 de outubro de 1997.
 8. Para iniciar a pesquisa, clique “Search”.

Uma barra de progresso exibe que a procura está sendo feita.

NOTA: Para cancelar uma procura em progresso, clique “Stop Search” (Parar Procura).

Os resultados da procura aparecem na janela.

9. Para importar as chaves, arraste-as para a janela principal de PGPkeys.
10. Clique “Clear Search” (Limpar Procura) para limpar seus critérios de pesquisa.

Este capítulo descreve PGPdisk, seus recursos, e provê instruções sobre como usá-lo.

O que é PGPdisk?

PGPdisk é um aplicativo de criptografia simples de usar, que permite que você configure uma área de espaço em disco para armazenar seus dados sensíveis. Este espaço reservado é usado para criar um arquivo chamado “volume PGPdisk”. Apesar de ser um único arquivo, um volume PGPdisk age de forma muito similar a um disco rígido em que ele provê espaço de armazenamento para seus arquivos e aplicativos. Você pode pensar nele como um disquete ou um disco rígido externo. Para usar os aplicativos e arquivos armazenados no volume, você o “monta”, ou o torna acessível a você. Quando um volume PGPdisk é montado, você pode usá-lo como usaria qualquer outro disco. Você pode instalar aplicativos no volume ou mover ou salvar seus arquivos neste volume. Quando o volume é desmontado ele fica inacessível para qualquer um que não conheça sua frase-senha secreta, que é uma versão maior de uma senha. Mesmo um volume montado é protegido: a não ser que um arquivo ou aplicativo esteja em uso, ele é armazenado em formato codificado. Se seu computador travar enquanto um volume estiver montado, o conteúdo do volume permanece codificado.

NOTA: Produtos PGP encorajam você a usar uma frase inteira ou uma longa seqüência de caracteres para proteger dados sensíveis. Tais “frases-senha” são geralmente mais seguras que as tradicionais senhas de 6 a 10 caracteres.

Recursos de PGPdisk

O programa PGPdisk:

- Permite que você crie volumes seguros de dados codificados que funcionam como quaisquer outros volumes com os quais você está acostumado a usar para armazenar seus arquivos.
- Provê codificação rápida e segura de seus dados com impacto mínimo na quantidade de tempo que leva para acessar seus programas e arquivos.

- Usa um algoritmo de criptografia forte, de nível militar, conhecido como CAST, que possui uma sólida reputação por sua habilidade de resistir a acesso não autorizado.
- Armazena o conteúdo de cada volume seguro em um arquivo codificado, que pode ter seu *backup* facilmente realizado e trocado com colegas.

Por que usar PGPdisk?

Enquanto outros produtos oferecem a você a habilidade de restringir acesso à arquivos em disco através de atributos de permissão e proteção de senhas simples, estas formas de segurança podem ser facilmente ser quebradas por alguém que estejam realmente intencionados a examinar seus dados. Apenas codificando seus dados você pode ter a certeza de que mesmo com as mais sofisticadas tecnologias de hoje, é quase impossível para qualquer pessoa decifrar o conteúdo de seus arquivos.

Aqui estão algumas razões para usar PGPdisk para dar segurança ao conteúdo de seus arquivos:

- Para proteger informações financeiras, médicas ou pessoais sensíveis que você simplesmente não quer que outros tenham acesso. Isto é particularmente importante no ambiente de redes de hoje, onde informações em seu computador pessoal estão expostos para o mundo enquanto você está surfando na rede.
- Para configurar áreas pessoais de trabalho em uma máquina compartilhada, onde a cada usuário é garantido um acesso exclusivo a seus próprios programas e arquivos. Cada usuário pode montar seus próprios volumes enquanto usando a máquina, e ter a certeza de que ninguém mais pode acessar os arquivos uma vez que os volumes forem desmontados.
- Para criar volumes de materiais que são acessíveis apenas a membros designados de um determinado grupo de trabalho. Um volume pode ser montado quando membros do time querem trabalhar em um determinado projeto e podem ser desmontados e armazenados em seu formato criptografado quando tiverem terminado.
- Para prevenir de que alguém obtenha acesso a informações proprietárias armazenadas em um computador “notebook”. Em geral, se você perder seu notebook (ou alguém roubá-lo), todas as suas informações pessoais (incluindo acesso e senhas para serviços on-line, contatos comerciais e pessoais, registros financeiros etc), estão sujeitos a uso indevido por aqueles que tenham intento criminoso e podem acabar lhe custando mais do que o preço do notebook perdido.

- Para dar segurança a conteúdo de mídias externas, como disquetes e cartuchos de armazenagem. A habilidade de criptografar mídias externas provê um nível adicional de segurança para armazenagem e troca de informações sensíveis.

Iniciando o programa PGPdisk

Para iniciar PGPdisk

1. Selecione Iniciar --> Programas --> PGP --> PGPdisk.

Isto abre a barra de ferramentas de PGPdisk como mostrado na [figura 7-1](#).



Figura 7-1. A barra de ferramentas de PGPdisk

A barra de ferramentas de PGPdisk provê uma forma conveniente de criar e montar volumes. Aqui está uma breve descrição de cada botão:

New (Novo)	Exibe o assistente de PGPdisk, que guia você através do processo de criação de um novo volume PGPdisk.
Mount (Montar)	Monta o volume PGPdisk especificado, desde que a frase-senha correta tenha sido inserida.
Unmount (Desmontar)	Desmonta o volume PGPdisk especificado.
Preferences (Preferências)	Especifica como você prefere desmontar seus volumes.

Trabalhando com volumes PGPdisk

Esta seção explica como criar, montar e desmontar volumes PGPdisk e como especificar as preferências que protegem o conteúdo dos volumes, desmontando-os sob certas circunstâncias.

NOTA: Você pode executar a maioria das operações de PGPdisk clicando com o botão direito sobre o ícone do arquivo do volume PGPdisk.

Criando um novo volume PGPdisk

Para criar um novo volume PGPdisk

1. Inicie PGPdisk. A barra de ferramentas de PGPdisk aparece.
2. Clique “New” (Novo). O Assistente de PGPdisk aparece em sua tela. Leia as instruções introdutórias.
3. Clique “Next”.
4. Especifique o nome e local do novo volume.
5. Clique “Save”.
6. Insira a quantidade de espaço que você deseja reservar para o novo volume (campo “PGPdisk Size”). Use números inteiros, sem casas decimais. Você pode usar as setas para aumentar ou diminuir o número exibido neste campo.

A quantidade de espaço livre em disco para o drive selecionado é mostrada acima do campo “Size”.

7. Clique o botão apropriado para selecionar kilobytes, megabytes, ou gigabytes.

Dependendo da quantidade de espaço em disco, você pode criar um volume de qualquer tamanho entre 100 kilobytes e 2 gigabytes.

8. Selecione a letra do drive onde você deseja montar seu volume PGPdisk (campo “PGPdisk Drive Letter”). Você pode usar a seta para exibir e selecionar uma letra de drive diferente.

9. Clique “Next”.
10. Insira a cadeia de letras e caracteres que servirão como sua frase-senha para acessar o novo volume (também chamada de “frase-senha mestra do volume”). Para confirmar sua entrada, pressione “Tab” para avançar ao próximo campo de texto, então insira a mesma frase-senha novamente. O tamanho mínimo para uma frase-senha é de 8 caracteres.

Normalmente, como nível adicional de segurança, os caracteres que você insere para a frase-senha não são mostrados na tela. Entretanto, se você está certo de que ninguém está olhando (fisicamente ou pela rede) e você quer ver os caracteres de sua frase-senha enquanto os digita, clique na caixa “Hide Typing” (Esconder Digitação).

NOTA: Sua segurança é apenas tão boa quanto sua frase-senha. Sua frase-senha deve conter mais de uma palavra, junto com espaços, números, e outros caracteres imprimíveis. A frase-senha é sensível a caso (difere maiúsculas de minúsculas). A senha mínima permitida é de 8 caracteres. Escolha algo com o qual você está bem familiar e que você já tenha armazenado em sua memória de longo prazo. Escolher uma frase-senha no calor do momento é algo que pode resultar em esquecê-la completamente. É vital que você *não se esqueça de sua frase-senha ou você irá perder seus dados!* Para maiores informações, veja [“Qualidade da frase-senha”](#).

11. Clique “Next”.
12. Mova seu mouse de forma aleatória dentro da janela do Assistente e/ou digite caracteres em seu teclado até que a barra de progresso mostrada na caixa de diálogo esteja completamente preenchida.

Seus movimentos do mouse e sua digitação são usadas para gerar números aleatórios usados pelo PGPdisk como parte do processo de codificação (mistura dos dados).
13. Clique “Next”. Uma barra de progresso indica quanto do volume PGPdisk já foi inicializado.
14. Clique “Next” para montar seu PGPdisk.
15. Clique “Finish”. A janela de formatação aparece em sua tela.
16. Insira um rótulo (label) para o novo volume (este rótulo identifica o volume em Windows Explorer).
17. Clique “Start”. Uma caixa de diálogo de aviso aparece.

18. Clique OK (não há dados no novo disco). O sistema lhe informa que a formatação está completa.

19. Clique “Close” na janela de formatação.

Seu volume PGPdisk aparece em uma janela do Explorer.

Um ícone representando seu volume aparece no local especificado. Dê um clique duplo no ícone para abrir o volume.

Um ícone representando seu volume codificado aparece no local que você especificou, como mostrado abaixo.



**Volume PGPdisk
montado**



**Volume PGPdisk
codificado**

Alterando uma frase-senha

Você pode alterar a frase-senha mestra ou alternativa para um arquivo PGPdisk.

Para alterar sua frase-senha

1. Certifique-se de que o arquivo PGPdisk não está montado. Você não pode alterar uma frase-senha se o arquivo PGPdisk estiver montado.
2. Selecione “Change Passphrase” (Alterar Frase-Senha) no menu “File”.
3. Selecione o arquivo PGPdisk de interesse.
4. Insira a frase-senha atual, como mostrado na [figura 7-2](#).

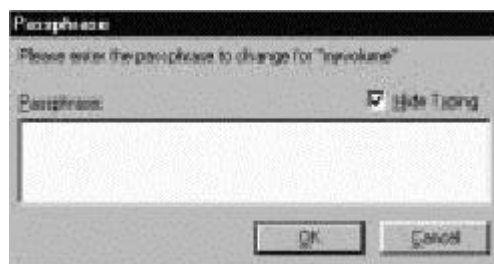


Figura 7-2. Caixa de diálogo “Passphrase”

Clique OK. A janela “New Passphrase” (Nova Frase-Senha) aparece.

5. Insira a série de palavras ou caracteres que servirão como sua nova frase-senha para acessar o novo volume (também chamada de “frase-senha mestra do volume”). Para confirmar sua entrada, pressione a tecla “Tab” para avançar à próxima caixa de texto, então insira a mesma frase-senha novamente. O tamanho mínimo para uma frase-senha é de 8 caracteres.
6. Clique OK.

A caixa de diálogo “New Passphrase” é fechada.

Adicionando frases-senhas alternativas

Uma vez que você inseriu a frase-senha mestra (aquela usada para criar o disco inicialmente), você pode adicionar até sete outras frases-senhas alternativas, que podem ser usadas para montar o volume. Você pode querer fazer isso se você usa a mesma frase-senha mestra regularmente, e deseja fazer com que o volume fique disponível para mais alguém com a frase-senha única destas pessoas. Apenas uma pessoa que conheça a frase-senha mestra pode adicionar frases-senhas alternativas.

Qualquer usuário que conheça uma frase-senha pode alterá-la, mas você sempre poderá acessar o conteúdo do volume se isso seja necessário. Você também tem a opção de associar um status “apenas para leitura” para o volume, o que permite às pessoas ler os arquivos, mas previne-os de alterar os arquivos de qualquer forma.

Para adicionar frases-senhas alternativas

1. Certifique-se de que o volume PGPdisk não está montado. Você não pode alterar uma frase-senha enquanto o volume PGPdisk estiver montado.
2. Selecione “Add Passphrase” (Adicionar Frase-Senha) no menu “File”.

A caixa de diálogo “Passphrase” aparece, pedindo que você insira a frase-

senha mestra do volume. Se você possuir vários volumes PGPdisk em sua máquina, você precisa selecionar um volume.

3. Insira a frase-senha mestra e clique OK.

A caixa de diálogo “New Passphrase” aparece, como mostrado na [figura 7-3](#).

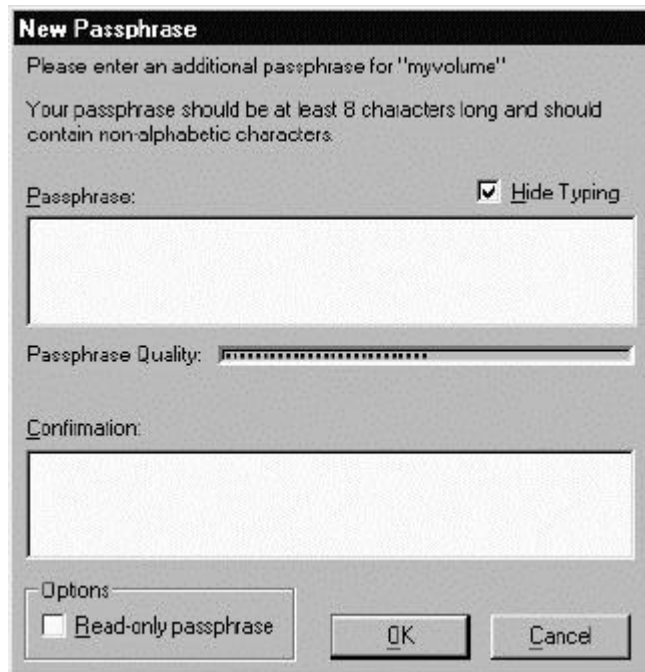


Figura 7-3. A caixa de diálogo “New Passphrase”

4. Insira uma frase-senha alternativa para o volume mostrado e então pressione a tecla “Tab”. Insira a frase-senha novamente para confirmá-la.

Neste ponto, você também tem a opção de marcar a caixa “Read-only passphrase” (Frase-senha apenas para leitura) para indicar que você quer que todo o conteúdo do volume seja designado como “apenas para leitura”.

5. Clique OK.

Uma vez que você criou uma frase-senha alternativa, você (ou qualquer um que a conheça) pode remover a frase-senha escolhendo o comando “Remove Passphrase” (Remover Frase-Senha) no menu “File”. Frases-senhas mestras não podem ser removidas (para maiores informações, veja [“Removendo uma frase-senha”](#), abaixo).

Removendo uma frase-senha

Remover uma frase-senha é similar a adicionar ou alterar uma frase-senha. Você não pode remover uma frase-senha mestra.

Para remover uma frase-senha

1. Certifique-se de que o volume PGPdisk não está montado. Você não pode alterar uma frase-senha enquanto o volume PGPdisk estiver montado.
2. Selecione “Remove Passphrase” (Remover Frase-Senha) no menu “File”.

Uma caixa de diálogo aparece, pedindo que você insira a frase-senha a ser removida.

3. Insira a frase-senha e então clique OK.

Removendo todas as frases-senhas alternativas

Você também pode remover todas as frases-senhas alternativas de uma vez. Isto poderia ser útil se outros usuários possuem frases-senhas alternativas para um volume PGPdisk, e você não quer mais que eles acessem o volume.

Para remover todas as frases-senhas alternativas

1. Certifique-se de que o volume PGPdisk não está montado. Você não pode alterar uma frase-senha enquanto o volume PGPdisk estiver montado.
2. Aperte e segure a tecla “Shift” e selecione “Remove Alternate Passphrases” (Remover Frases-Senhas Alternativas) no menu “File”.

Uma caixa de diálogo aparece, pedindo que você confirme que deseja remover todas as frases-senhas alternativas.

3. Clique “Yes” (Sim).

Uma caixa de diálogo aparece, dizendo a você que a remoção de todas as frases-senhas alternativas foi bem sucedida.

Adicionar/Remover Chaves Públicas

Você pode adicionar e remover chaves públicas para um arquivo PGPdisk. Este recurso permite que você e outros que conheçam a frase-senha para aquelas chaves usem as mesmas para montar o volume.

Para adicionar uma chave pública em seu volume PGPdisk

1. Certifique-se de que o volume PGPdisk não está montado. Você não pode alterar uma frase-senha enquanto o volume PGPdisk estiver montado.
2. Selecione “Add/Remove Public Keys” (Adicionar/Remover Chaves Públicas) do menu “File”.
3. Selecione o PGPdisk da barra de ferramentas “Select PGPdisk”.

É pedido que você insira a frase-senha mestra.

A janela de diálogo “Recipient Selection” (Seleção de Destinatário) aparece.

4. Arraste a chave ou chaves da parte superior na janela para a parte inferior.
5. Clique OK.

Para remover uma chave pública de seu volume PGPdisk

1. Certifique-se de que o volume PGPdisk não está montado. Você não pode alterar uma frase-senha enquanto o volume PGPdisk estiver montado.
2. Selecione “Add/Remove Public Keys” (Adicionar/Remover Chaves Públicas) do menu “File”.
3. Selecione o PGPdisk da barra de ferramentas “Select PGPdisk”.

É pedido que você insira a frase-senha mestra.

A janela de diálogo “Key Selection” (Seleção de Chave) aparece, como mostrado na [figura 7-4](#).

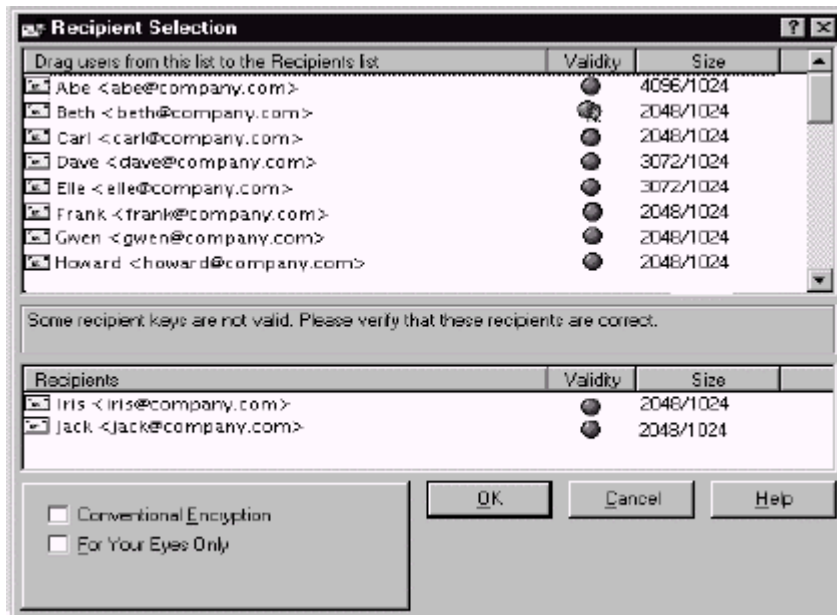


Figura 7-4. A caixa de diálogo “Key Selection”

4. Arraste a chave ou chaves da parte inferior na janela para a parte superior.
5. Clique OK.

Montando um volume PGPdisk

Quando você cria um novo volume, o programa PGPdisk automaticamente o monta de forma que você pode começar a usá-lo para armazenar seus arquivos. Quando você está pronto para dar segurança ao conteúdo do volume, você deve desmontá-lo. Uma vez que um volume é desmontado, seu conteúdo permanece seguro em um arquivo codificado, onde está inacessível até que o volume seja montado novamente.

Há quatro formas de montar um volume.

- Dê um clique duplo no ícone do volume.
- Arraste o ícone do volume para o ícone de PGPdisk na pasta de PGP 6.0.
- Arraste o ícone do volume para o botão “Mount” (Montar) na barra de ferramentas de PGPdisk.
- Clique com o botão direito no ícone do volume. Selecione PGPdisk --> Mount PGPdisk.
- Use o botão “Mount” na barra de ferramentas de PGPdisk.

Para montar um volume usando o botão “Mount”

1. Inicie PGPdisk.

A barra de ferramentas de PGPdisk aparece.

2. Clique “Mount” ou use a opção “Mount PGPdisk” (Montar PGPdisk) no menu “File”.

A caixa de diálogo “Mount PGPdisk” aparece.

3. Localize e selecione o volume codificado que você deseja montar, então clique “Open”.

É pedido que você insira a frase-senha para o volume selecionado.

4. Insira a frase-senha e clique OK. Se você não quer modificar os arquivos no volume, clique a caixa “read-only” (apenas para leitura). Se você inseriu a frase-senha correta, o volume é montado e os dados no arquivo codificado estarão acessíveis. O volume aparece na árvore de pastas do Windows Explorer.

Usando um volume PGPdisk montado

Você pode criar, mover, e apagar arquivos e pastas em um volume PGPdisk exatamente como faria com qualquer outro volume. Similarmente, qualquer um que tiver acesso ao volume (na mesma máquina ou talvez através da rede) também pode acessar os dados armazenados no volume. Os dados no arquivo codificado associado com o volume só estarão inacessíveis quando você desmontar o volume.

ATENÇÃO: Apesar do arquivo codificado associado a cada volume estar salvo de curiosos, ele ainda pode ser apagado. Se uma pessoa não autorizada pode acessar seus dados, ele ou ela poderia potencialmente apagar o arquivo codificado no qual o volume está baseado. É uma boa idéia manter uma cópia *backup* do arquivo codificado.

Desmontando um volume PGPdisk

Após acessar um determinado volume e você desejar trancar seu conteúdo, você precisa desmontar o volume. Você não pode desmontar um volume que possua arquivos abertos.

Para desmontar um volume PGPdisk

1. Feche todos os arquivos no volume PGPdisk que você deseja desmontar.
2. Selecione “Unmount PGPdisk” (Desmontar PGPdisk) no menu “File” de PGPdisk.

Outras formas de desmontar um volume PGPdisk incluem:

- Clique “Unmount” (Desmontar) na barra de ferramentas de PGPdisk
- Clique com o botão direito na letra do drive na janela do Explorer
- Clique com o botão direito no arquivo do volume

Uma vez que um volume é desmontado, seu conteúdo é travado no arquivo codificado associado com o volume. O conteúdo do volume é armazenado no arquivo codificado e seu conteúdo permanece inacessível até que o volume seja novamente montado. Pode ajudar visualizar volumes PGPdisk como uma janela que provê uma visão dos dados no arquivo codificado. O conteúdo de um arquivo de volume PGPdisk só se torna disponível quando o arquivo é montado como um volume, por alguém que conheça uma frase-senha válida.

Especificando Preferências

O botão “Preferences” na barra de ferramentas de PGPdisk permite que você especifique como você prefere desmontar e criar seus volumes.

Para especificar preferências

1. Clique “Preferences” na barra de ferramentas de PGPdisk ou selecione “Preferences” a partir do menu “File”.

A caixa de diálogo “Preferences” aparece.

2. Selecione as opções desejadas clicando as caixas e abas apropriadas.

Aba “Auto Unmount” (Auto Desmontar)

- **Auto unmount after [15] minutes of inactivity** (Auto desmontar após [15] minutos de inatividade). Quando selecionada, esta opção faz com que PGPdisk automaticamente desmonte quaisquer volumes PGPdisk montados quando seu computador estiver inativo pelo número de minutos na caixa. Você pode configurar este valor entre 1 a 999 minutos.

NOTA: PGPdisk não pode desmontar um volume PGPdisk automaticamente se qualquer dos arquivos no volume estiver aberto.

- **Auto unmount on computer sleep** (Auto desmontar quando computador estiver em estado de espera). Quando selecionada, esta opção faz com que PGPdisk automaticamente desmonte quaisquer volumes PGPdisk montados quando seu computador estiver em modo de Espera (nem todos os modelos de computador possuem um modo de espera).

A opção **Prevent sleep if any PGPdisks could not be unmounted** (evitar modo de espera se quaisquer PGPdisks não puderem ser desmontados) certifica-se de que seu computador não entrará em estado de espera caso um volume PGPdisk não possa ser desmontado.

NOTA: Estas duas opções (“Auto unmount on computer sleep” e “Prevent sleep if any PGPdisks could not be unmounted”) estão desabilitadas em sistemas NT .

- **Enable Unmount HotKey** (Habilitar Tecla de Atalho para Desmontagem). Quando você insere uma combinação de teclas na caixa de texto e marcar esta opção, você cria e habilita um atalho via teclado que permite que você desmonte todos os volumes PGPdisks no sistema com um simples toque.

Clique OK quando tiver terminado de especificar suas preferências.

NOTA: As configurações para auto desmontar são úteis se você precisa deixar seu computador por um período de tempo. Você deve ajustar o tempo destas configurações de acordo com quão seguro seu sistema é de acesso físico não autorizado. Você pode configurar todas estas preferências ao mesmo tempo.

Mantendo Volumes PGPdisk

Esta seção descreve como automaticamente montar volumes PGPdisk quando você iniciar seu sistema, e como fazer *backups* e trocar os dados nestes volumes com outros.

Montando arquivos PGPdisk em um servidor remoto

Você pode colocar volumes PGPdisk em qualquer tipo de servidor (NT, 95, 98 ou UNIX) e permitir que eles sejam montados por qualquer um com uma máquina Windows 95.

NOTA: A primeira pessoa a montar o volume localmente possui acesso para leitura e escrita ao volume. Ninguém mais poderá acessá-lo nesse momento. Se você quer que outros acessem arquivos que estão no volume, você deve montar o volume em modo apenas para leitura. Todos os usuários do volume terão, então, acesso apenas para leitura.

Se o volume estiver armazenado em um servidor Windows 95, você também pode montar o volume remotamente no servidor, e permitir que as pessoas compartilhem o volume montado. Entretanto, esta ação não provê segurança alguma aos arquivos no volume.

Montando automaticamente volumes PGPdisk

Se você quiser, você pode automaticamente montar volume PGPdisk quando você inicia pela primeira vez seu sistema.

Para montar automaticamente volumes PGPdisk

1. Crie um atalho para um dos arquivos PGPdisk que você deseja montar quando iniciar seu computador.
2. Coloque o(s) atalho(s) na pasta WinNT --> Profiles --> {Nome do usuário atual} --> Menu Iniciar --> Programas (em sistemas WindowsNT) ou em Windows --> Menu Iniciar --> Programas (em sistemas Windows 95/98).

Uma vez que você colou os atalhos nesta pasta, os volumes PGPdisk são montados sempre que você inicia seu computador. É pedido a você para entrar a frase-senha para cada volume PGPdisk quando ele é montado.

Realizando *backups* de volumes PGPdisk

Você pode desejar realizar *backups* do conteúdo de seu PGPdisk para salvaguardar suas informações de corrupções do sistema ou falhas de disco. Enquanto é possível realizar o *backup* de todo o conteúdo de um volume PGPdisk montado, como você faria com qualquer volume, esta não é provavelmente uma boa idéia porque o conteúdo não está codificado e assim estaria acessível a qualquer um que pudesse restaurar o *backup*. Ao invés de realizar o *backup* do conteúdo do volume PGPdisk montado, você deve fazer um *backup* do volume PGPdisk codificado.

Para efetuar *backup* de volumes PGPdisk

1. Clique no ícone do volume PGPdisk. Selecione a opção “Unmount PGPdisk” (Desmontar PGPdisk).
2. Copie o arquivo codificado e desmontado para um disquete, fita, ou cartucho removível como faria com qualquer outro arquivo. Mesmo se uma pessoa não autorizada tiver acesso a seus *backups*, ele ou ela não poderão decifrar seu conteúdo.

Trocando volumes PGPdisk

Você pode trocar volumes PGPdisk com colegas que possuam seus próprios programas PGPdisk enviando a eles uma cópia do arquivo codificado que contém os dados associados ao volume. Aqui estão algumas formas que você pode trocar volumes PGPdisk:

- Como anexo de email
- Em disquetes ou cartuchos
- Através de uma rede

DICA: Você deve considerar cuidadosamente o método que usará para prover a alguém a frase-senha usada para ter acesso a um volume PGPdisk. Em geral, a não ser que você use algum outro produto de criptografia para proteger sua mensagem, email não é uma boa forma de trocar frases-senhas. Linhas telefônicas também são vulneráveis à monitoração, e sua conversação poderia ser espionada. Quanto mais precauções de segurança você tomar, maiores as chances de suas informações permanecerem confidenciais. Se você não possuir um email seguro, então é provavelmente mais seguro dizer à outra pessoa a frase-senha em um encontro face-a-face ou mesmo usando correio postal regular.

Uma vez que a parte intencionada possui uma cópia do arquivo codificado, tudo que ela precisa fazer para acessar o conteúdo do volume é montá-lo usando a frase-senha correta,

ou, se o volume foi codificado para sua chave pública, sua chave. Ela também precisa de uma cópia do programa PGPdisk. Para maiores informações sobre como montar um volume PGPdisk, veja [“Montando um volume PGPdisk”](#).

Alterando o tamanho de um volume PGPdisk

Apesar de você não poder alterar o tamanho de um volume PGPdisk uma vez que ele foi criado, você pode criar um volume maior ou menor e então copiar o conteúdo do volume antigo para o novo.

Para alterar o tamanho de um volume PGPdisk

1. Crie um novo volume PGPdisk e especifique o tamanho desejado.
2. Copie o conteúdo do volume PGPdisk montado existente para o volume recém criado.
3. Desmonte o volume PGPdisk antigo e então apague o arquivo codificado associado ao volume, para liberar espaço em disco.

Detalhes Técnicos e Considerações de Segurança

Esta seção discute as questões sobre codificação e segurança e provê dicas ao usuário e outras informações técnicas sobre PGPdisk.

Sobre volumes PGPdisk

Você pode usar volumes PGPdisk para organizar seu trabalho, manter nomes de arquivos similares separados, ou manter múltiplas versões dos mesmos documentos ou programas separados.

Apesar dos volumes que você cria com PGPdisk funcionarem como qualquer outro volume com o qual você está acostumado a trabalhar, os dados são na verdade armazenados em um grande arquivo codificado. Apenas após você montar o arquivo que seu conteúdo é apresentado na forma de um volume. É importante saber que todos os seus dados permanecem seguros no arquivo codificado, e são decifrados apenas quando você acessa um dos arquivos. Manter os dados para um volume armazenado desta maneira torna simples de manipular e trocar volumes PGPdisk com outros, mas também torna mais fácil perder dados se o arquivo for apagado de alguma forma. É sábio manter uma cópia *backup* destes arquivos codificados de forma que os dados possam ser recuperados no caso de algo acontecer ao original. É também importante notar que você não pode comprimir um arquivo compactado em uma tentativa de reduzir seu tamanho, mas pode comprimir os arquivos individuais contidos no volume montado, e assim armazenar mais dados codificados no volume. Você também pode armazenar um volume PGPdisk seguro dentro de outro, e assim aninhar diversos volumes para um nível adicional de segurança.

O algoritmo de criptografia de PGPdisk

Codificação aplica uma fórmula matemática para misturar seus dados de forma que ninguém mais possa usá-los. Quando você aplica a chave matemática correta, você reorganiza seus dados. A fórmula de codificação de PGPdisk usa dados aleatórios para parte do processo de codificação. Alguns destes dados aleatórios vêm do movimento do seu mouse durante a codificação e alguns dados aleatórios também vêm diretamente de sua frase-senha.

O processo de codificação de PGPdisk é uma fórmula matemática complexa que, ao tanto que sabemos, é atualmente inquebrável. Alguém pode desenvolver um método de quebrar esta fórmula alguns anos no futuro, mas informação sensível é geralmente sensível por apenas um tempo limitado. O programa PGPdisk usa um algoritmo de codificação sofisticado, chamado de CAST, que é considerado uma excelente cifra de blocos porque é rápido e inquebrável — ao tanto que alguém saiba. Seu nome é derivado das iniciais de

seus projetistas, Carlisle Adams e Stafford Tavares da Northern Telecom (Nortel). Nortel pediu uma patente para CAST, mas eles se comprometeram a fazer CAST disponível a qualquer um sem pagamento de “royalties”. CAST parece ser excepcionalmente bem projetado, por pessoas com boa reputação no campo. O projeto é baseado em uma aproximação bastante formal, com um número de assertivas formalmente prováveis, que dão boas razões para acreditar que ele provavelmente requer exaustão de chaves para quebrar sua chave de 128 bits. CAST não possui chaves fracas. Há fortes argumentos que CAST é imune tanto à criptoanálise linear e diferencial, as duas formas mais poderosas de criptoanálise na literatura publicada, onde ambas foram efetivas em quebrar o “Data Encryption Standard” (DES).

Qualidade da Frase-Senha

Sua segurança é apenas tão boa quanto sua frase-senha. Entretanto, codificar um arquivo e depois se achar impossibilitado de decifrá-lo é uma dolorosa lição para aprender a escolher uma frase-senha da qual você se lembrará.

A maioria das aplicações requer uma senha entre três e oito letras. Uma senha de uma só palavra é vulnerável a um “ataque de dicionário”, que consiste em fazer um computador tentar todas as palavras de um dicionário até achar sua senha. Para proteger-se contra esta maneira de ataque, é amplamente recomendado que você crie uma frase que inclua uma combinação de letras maiúsculas e minúsculas, números, marcas de pontuação, e espaços. Isto resulta em uma senha mais forte, mas obscura, que é improvável que se lembre facilmente. Nós não recomendamos que você use uma frase-senha de uma só palavra.

Uma frase-senha é menos vulnerável a um ataque de dicionário. Isto é realizado facilmente usando várias palavras em sua frase-senha, ao invés de tentar contrariar um ataque de dicionário inserindo arbitrariamente montes de caracteres engraçados não-alfabéticos, que têm o efeito de fazer sua frase-senha muito fácil de se esquecer e poder conduzir a uma perda desastrosa de informações porque você não pode decifrar seus próprios arquivos. Porém, a menos que a frase-senha que você escolher seja algo que é facilmente gravável em sua memória de longo prazo, é pouco provável que você irá se lembrar dela literalmente. É provável que a escolha de uma frase no calor de um determinado momento resulte em seu esquecimento por completo. Escolha algo que já está gravado em sua memória de longo prazo. Não deve ser algo que você repetiu recentemente a outros, nem uma frase famosa, porque você quer que ela seja dura para um atacante sofisticado adivinhar. Se já estiver profundamente enraizado em sua memória de longo prazo, você provavelmente não a esquecerá. *Não a escreva!*

Sua frase-senha é parte dos dados aleatórios usados para codificar seus arquivos PGPdisk files. A barra “Passphrase Quality” (Qualidade da Frase-Senha) deve ser preenchida ao menos até a metade quando você inserir uma frase-senha. A não ser que você preencha toda a barra, você não está conseguindo segurança máxima.

Você pode criar uma frase-senha separada ou alternativa para cada volume PGPdisk que criar. Isto torna possível você permitir que alguns usuários acessem os arquivos no PGPdisk selecionado, de acordo com o volume. Você pode usar uma frase-senha para

arquivos PGPdisk que você envia a um colega, e ainda assim prevenir que este colega acesse qualquer um de seus outros arquivos PGPdisk.

Precauções especiais de segurança tomadas por PGPdisk

PGPdisk toma cuidados especiais para evitar problemas de segurança que outros programas talvez não tomem. Estes incluem os seguintes:

Apagamento da frase-senha

Quando você insere uma frase-senha, PGPdisk a usa apenas por um breve tempo, então a apaga da memória. PGPdisk também evita fazer cópias da frase-senha. O resultado é que sua frase-senha tipicamente permanece na memória por apenas uma fração de segundo. Este recurso é crucialmente importante — se a frase-senha ficasse na memória, alguém poderia procurar por ela na memória de seu computador enquanto você estivesse longe da máquina. Você não saberia disso, mas eles teriam acesso completo a qualquer volume PGPdisk protegido por essa frase-senha.

Proteção de memória virtual

Sua frase-senha ou outras chaves poderia ser escrita no disco como parte das transferências da memória para o disco, feitas pelo sistema de memória virtual. PGPdisk cuida para que as frases-senhas e chaves nunca sejam escritas em disco. Este recurso é importante porque alguém poderia pesquisar o arquivo de memória virtual procurando por frases-senhas.

Proteção de memória contra migração de íons estáticos

Quando você monta um PGPdisk, sua frase-senha é transformada em uma chave. Esta chave é usada para codificar e decifrar os dados em seu volume PGPdisk. Apesar da frase-senha ser apagada da memória imediatamente, a chave (da qual sua frase-senha não pode ser derivada) permanece na memória enquanto o disco é montado. Esta chave é protegida da memória virtual, entretanto, se uma certa seção da memória armazenar os mesmos dados iguais por períodos extremamente longos de tempo sem ser limpadado ou reiniciado, aquela memória tende a reter carga estática, que poderia ser lida por atacantes. Se seu PGPdisk está montado por longos períodos, de tempos em tempos traços detectáveis de sua chave poderiam ficar retidas na memória. Você não vai encontrar tais dispositivos na loja de aparelhos eletrônicos da vizinhança, mas os maiores governos possivelmente têm alguns.

PGPdisk protege contra isto mantendo duas cópias da chave na RAM, uma cópia normal e uma cópia com os bits invertidos, e inverte ambas as cópias a cada poucos segundos.

Outras considerações de segurança

Em geral, a habilidade de proteger seus dados depende das precauções que você toma, e nenhum programa de codificação pode protegê-lo de práticas de segurança descuidadas. Por exemplo, se você deixar seu computador ligado com arquivos sensíveis abertos quando você deixar sua mesa, qualquer um pode acessar aquela informação ou mesmo obter a chave usada para acessar os dados. Aqui estão algumas dicas para manter uma segurança ótima:

- Certifique-se de desmontar volumes PGPdisk quando deixar o computador. Desta forma, o conteúdo estará armazenado com segurança no arquivo codificado associado ao volume até que você esteja pronto para acessá-lo novamente.
- Use uma proteção de tela (“screen saver”) com uma opção de senha, de forma que seja mais difícil para alguém acessar sua máquina ou ver sua tela quando você estiver longe de sua mesa.
- Certifique-se de que seus volumes PGPdisk não podem ser vistos por outros computadores na rede. Você pode precisar conversar com as pessoas de gerenciamento da sua rede para garantir isto. Os arquivos em volumes PGPdisk montados podem ser acessados por qualquer um que possa vê-lo pela rede.
- Nunca escreva sua frase-senha. Use algo que você possa se lembrar. Se você tiver problemas em lembrar-se de sua frase-senha, use algo que mexa com sua memória, com um poster, uma música, um poema, uma piada, mas não escreva suas frases-senha.
- Se você usa PGPdisk em casa e compartilha seu computador com outras pessoas elas provavelmente poderão ver seus arquivos PGPdisk. Enquanto você desmontar seus volumes PGPdisk quando tiver terminado de usá-los, ninguém mais poderá ler seu conteúdo.
- Se outro usuário tiver acesso físico à sua máquina, esta pessoa pode apagar seus arquivos PGPdisk como também quaisquer outros arquivos ou volumes. Se o acesso físico é uma questão, tente criar arquivos *backup* dos arquivos de seu PGPdisk ou mantê-los em um dispositivo externo, sobre o qual apenas você possui controle físico.
- Saiba que cópias de seu volume PGPdisk usam as mesmas chaves secretas que a original. Se você trocar uma cópia de seu volume com outros e ambos alterarem suas senhas mestras, ambos ainda estarão usando a mesma chave para codificar os dados. Enquanto não é uma operação trivial recuperar a chave, não é impossível.

Solucionando Problemas com PGP

A

Este capítulo apresenta informações sobre problemas potenciais e sugere soluções.

Erro	Causa	Solução
Administrative preferences file not found (Arquivo de preferências administrativas não encontrado)	O arquivo de preferências que contém a configuração ajustada por seu administrador de PGP, geralmente alguém de IS/IT, está faltando.	Re-instale PGP em outra máquina. Se a mensagem continuar a aparecer após re-instalar, contacte seu administrador de PGP e informe a ele esta mensagem. Ele precisará gerar um novo instalador de PGP para você.
Authentication rejected by remote SKEP connection (autenticação rejeitada pela conexão SKEP remota)	O usuário do lado remoto da conexão via rede rejeitou a chave que você proveu como autenticação.	Use uma chave diferente para autenticar-se na conexão, ou contacte o usuário remoto para certificar-se de que a chave que você está usando é válida.
Cannot perform the requested operation because the output buffer is too small (não é possível	A saída é maior que a capacidade do buffer interno.	Se você está codificando ou assinando, você talvez precise quebrar a

requisitada porque o buffer de saída é muito pequeno)

codificar/assinar partes menores de cada vez. Se você está decifrando ou verificando, peça ao emitente para codificar/assinar partes menores e re-enviá-las a você.

Could not encrypt to specified key because it is a sign-only key (Não foi possível codificar para a chave especificada porque ela é uma chave apenas para assinatura)

A chave selecionada só pode ser usada para assinar.

Escolha uma chave diferente, ou gere uma nova chave que possa codificar dados.

Could not sign with specified key because it is an encrypt-only key (Não foi possível assinar com a chave especificada porque ela é uma chave apenas para codificação)

A chave selecionada só pode ser usada para codificar.

Escolha uma chave diferente, ou gere uma nova chave que possa assinar dados.

Error in domain name systemic (Erro no nome de domínio sistêmico)

O endereço de destino que você forneceu está incorreto, ou sua conexão de rede tem algum problema de configuração.

Verifique que o endereço de destino que você forneceu é o correto. Se você estiver certo disso, verifique sua conexão à rede.

Identical shares cannot be combined

Você tentou combinar o mesmo

Se você recebeu as partes de um arquivo

(partes idênticas não podem ser combinadas)

parte duas vezes.

de partes, tente escolher um arquivo de partes diferente. Se você recebeu as partes através da rede, você talvez precise contactar o usuário na localidade remota e dizer-lhe para enviar um conjunto diferente de partes.

No secret keys could be found on your keyring

(nenhuma chave secreta pôde ser encontrada em seu chaveiro)

Não há chaves privadas em seu chaveiro.

Gere seu próprio par de chaves em PGPkeys.

Socket is not connected. (Soquete não está conectado)

A conexão de rede para o servidor de certificados PGP ou para o arquivo de partes foi interrompida.

Tente restabelecer a conexão repetindo o procedimento que você usou para iniciá-la. Se isto falhar, cheque sua conexão com a rede.

The action could not be completed due to an invalid file operation (a ação

não pôde ser completada devido à uma operação de arquivo ilegal)

O programa não conseguiu ler ou escrever dados em um certo arquivo.

O arquivo está provavelmente corrompido. Tente alterar suas preferências de PGP para usar um arquivo diferente, se possível.

The evaluation time for PGP encrypting and signing has passed. Operation aborted (o tempo de

O tempo de avaliação do produto expirou.

Faça o “download” da versão “freeware” ou compre a versão comercial do

codificação e assinatura de PGP passou. Operação abortada)

produto.

The keyring contains a bad (corrupted) PGP packet (o chaveiro contém um pacote PGP ruim [corrompido]).

A mensagem PGP com a qual você está trabalhando foi corrompida, ou seu chaveiro foi corrompido.

Peça ao emitente para reenviar a mensagem se esta for a mensagem com a qual você estava trabalhando. Se for seu chaveiro, tente restaurá-lo de seu chaveiro de *backup*.

The keyring file is corrupt (o arquivo do chaveiro está corrompido)

O programa não conseguiu ler ou escrever dados em um certo arquivo.

Há um arquivo que está provavelmente corrompido ou faltando. Ele pode ou não ser o arquivo de seu chaveiro. Tente usar um caminho e nome de arquivos diferente, se possível.

The message/data contains a detached signature (A mensagem/dados contém uma assinatura separada)

A assinatura para a mensagem/arquivo está localizada em um arquivo separado.

Dê um duplo clique no arquivo com a assinatura separada primeiro.

The passphrase you entered does not match the passphrase on the key (a frase-senha

A frase-senha que você inseriu está incorreta.

Você talvez deixou a tecla "CAPS LOCK" ligada, ou simplesmente pode ter digitado

corresponde à frase-senha da chave)

senha. Tente novamente.

The PGP library has run out of memory (a biblioteca de PGP não tem mais memória)

O sistema operacional está sem memória.

Feche outros programas que estejam sendo executados. Se isso não funcionar, você talvez precise de mais memória em sua máquina.

The specified user ID was not added because it already exists on the selected key (o ID de usuário especificado não foi adicionado porque ele já existe na chave selecionada)

Você não pode adicionar um ID de usuário em uma chave se este ID já existir na chave.

Tente adicionar um ID de usuário diferente, ou apague o ID correspondente primeiro.

The specified key could not be found on your keyring (a chave especificada não pôde ser encontrada em seu chaveiro)

A chave necessária para decifrar a mensagem atual não está em seu chaveiro.

Peça ao emitente da mensagem para reenviar a mensagem e certificar-se de que ele codificou a mensagem para sua chave pública.

The specified input file does not exist (o arquivo de entrada especificado não existe)

O nome de arquivo inserido não existe.

Localize o caminho e nome de arquivo exatos para o arquivo que você deseja.

There is not enough random data currently available (não há dados

O gerador de números aleatórios precisa de mais entrada de forma

Quando pedido, mova seu mouse, ou pressione teclas aleatórias de

aleatórios suficientes atualmente disponíveis)

gerar bons números aleatórios.

forma a gerar entrada.

There was an error during the writing of the keyring or the exported file (houve um erro durante a escrita do chaveiro ou do arquivo exportado)

O programa não conseguiu ler ou escrever dados em um certo arquivo.

Seu disco rígido pode estar cheio, ou se o arquivo estiver em um disquete, o disquete não está inserido no drive.

There was an error opening or writing the keyring or the output file (houve um erro abrindo ou escrevendo o chaveiro ou o arquivo de saída)

Um arquivo que era necessário não pôde ser aberto.

Certifique-se de que as configurações em “PGP Preferences” estão corretas. Se você recentemente apagou arquivos no diretório onde instalou PGP, você talvez precise re-instalar o produto.

This key is already signed by the specified signing key (esta chave já está assinada pela chave de assinatura especificada)

Você não pode assinar uma chave que você já assinou.

Você talvez acidentalmente escolheu a chave errada. Se for isso, escolha uma chave diferente para assinar.

Unable to perform operation because this file is read-only or otherwise protected. If you store your keyring files on removable media the media may not be inserted (não foi possível

Um arquivo que era necessário foi configurado para “apenas para leitura” ou está sendo usado por outro programa.

Feche outros programas que podem estar acessando os mesmos arquivos que o programa que você está executando. Se você mantém seus arquivos de

porque este arquivo é apenas para leitura, ou então protegido. Se você armazena seus arquivos de chaves em uma mídia removível, a mídia pode não estar inserida)

disquete, certifique-se de que o disquete está no drive.

Transferindo Arquivos entre MacOS e Windows B

Transferência de arquivos para e de MacOS é um problema clássico no uso de quase qualquer tipo de software de troca de dados, como aplicativos de email, FTP, utilitários de compressão, e PGP. Este apêndice pretende documentar como este problema é finalmente resolvido por PGP Versão 6.0, e discutir como comunicar com versões anteriores de PGP.

O MacOS armazena arquivos diferentemente de outros sistemas operacionais. Até mesmo o formato de arquivo de texto do MacOS é diferente. Arquivos de MacOS são na verdade dois arquivos que consistem em um “segmento de dados” e um “segmento de recursos”. Para enviar um arquivo de MacOS para Windows sem perder dados, os dois segmentos devem ser fundidos em um. O método padrão pelo qual um arquivo de MacOS é convertido em um único arquivo, de forma que possa ser transferido a outro Macintosh ou PC sem perder qualquer uma das metades, é chamado MacBinary.

O problema é que, sem software especial, Windows e outras plataformas não podem entender o formato MacBinary. Se acontecer uma situação onde o software receptor falhar em converter um arquivo em formato MacBinary em um arquivo Windows, o arquivo resultante é inutilizável. Utilitários de terceiros existem para Windows para converter estes os arquivos em um arquivo utilizável, mas isso pode ser bastante inconveniente.

Versões anteriores de PGP e a maioria dos utilitários disponível no mercado hoje tentam geralmente ignorar este problema o máximo possível e deixar todas as decisões para o usuário, como codificar ou não um arquivo com MacBinary quando enviando de MacOS. Isto coloca o fardo de decidir enviar com MacBinary, e não perder quaisquer dados, ou enviar sem MacBinary, e esperar que nenhum dado importante seja perdido, nas mãos do usuário, que freqüentemente não tem nenhuma idéia sobre qual é a decisão correta. A decisão geralmente deveria ser baseada em se o arquivo está sendo enviado a Windows ou a MacOS. Mas e se você está enviando ao mesmo tempo a ambos? Não há nenhuma boa solução para este problema com versões mais antigas de PGP e muitos outros utilitários. Isto resultou em grande confusão e inconveniência para usuários. O contrário, enviar um arquivo de Windows para MacOS, também tem sido um grande problema. Windows usa extensões para nomes de arquivo, como “.doc”, para identificar o tipo de um arquivo. Isto não tem sentido para MacOS. Estes arquivos são enviados a um computador Macintosh sem qualquer “tipo” de arquivo ou informação sobre o criador. O processo de fazê-los legíveis depois de recebidos geralmente envolve vários movimentos enigmáticos na caixa de diálogo “Abrir” do aplicativo do criador, ou em muitos casos exige que o usuário entenda o costume de MacOS sobre criador e tipos de códigos, fixando-os manualmente com um utilitário de terceiros.

Felizmente, as versões mais recentes de PGP (versão 5.5 e superiores) acabaram com esta

confusão. Se todos os usuários de PGP fossem usar as mais recentes versões, ninguém teria que pensar como enviar arquivos de MacOS para Windows e vice-versa.

Enviando do MacOS ao Windows

No MacOS, há três opções quando codificando ou assinando um arquivo:

- **MacBinary: Yes.** Esta é a opção recomendada para todas as codificações quando enviando a outro usuário de PGP Versão 5.5 ou superior em qualquer plataforma. Isto significa que usuários de MacOS receberão o arquivo exatamente como intencionado, e a versão de Windows decodificará o MacBinary automaticamente e até mesmo adicionar a extensão de arquivo apropriada, como “.doc” para Microsoft Word ou “.ppt” para Microsoft PowerPoint. PGP inclui informação sobre extensões de nomes de arquivos dos aplicativos mais populares e códigos de criador de Macintosh. Em casos onde o tipo é desconhecido ou se sabe que se trata de ser um arquivo apenas para MacOS, como um aplicativo de MacOS, o arquivo permanece em formato MacBinary, de forma que possa ser remetido depois completamente intacto a um Macintosh.
- **MacBinary: No.** Se você está se comunicando com usuários que têm uma versão mais antiga de PGP, a decisão de se geralmente enviar com MacBinary acaba nas mãos do remetente, como na maioria dos outros programas e em versões anteriores de PGP para MacOS. Quando enviando a um PC que usa uma versão mais antiga, se você sabe que o arquivo que você está enviando pode ser lido através de aplicações para Windows quando MacBinary não é usado, selecione esta opção. Isto inclui a maioria dos arquivos que geralmente são inter-plataformas, como os criados pelos aplicativos de Microsoft Office, arquivos de gráficos, arquivos comprimidos, e muitos outros. O remetente ou o destinatário terá que renomear o arquivo manualmente, para ter a extensão de arquivo correta em Windows. Isto é requerido porque o destinatário Windows não tem as informações de criador normalmente codificadas com MacBinary.
- **MacBinary: Smart.** Há alguns casos muito limitados onde esta opção pode ser útil quando comunicando com usuários que não estão usando versões mais recentes de PGP. Esta opção toma uma decisão sobre se deve codificar com MacBinary, baseado em uma análise dos dados atuais no arquivo. Se o arquivo é um dos tipos a seguir, não será codificado com MacBinary, sendo assim legível em um PC com qualquer versão de PGP:
 - arquivo comprimido PKzip
 - arquivo comprimido Lempel-Ziv

- formato de arquivo musical MIDI
- arquivo comprimido PackIt
- arquivo gráfico GIF
- arquivo comprimido StuffIt_
- arquivo comprimido Compactor
- arquivo comprimido Arco
- arquivo gráfico JPEG

Como mostrado, só uma seleção limitada de arquivos resultará em um arquivo legível por versões antigas de PGP em outras plataformas, quando usando a opção “Smart”. Qualquer outro arquivo recebido em um PC com uma versão mais antiga de PGP será ilegível, se não se remover o MacBinary que o codifica com um utilitário de terceiros. Também, o arquivo não terá a extensão de nome de arquivo correta no PC, a menos que aquela extensão fosse adicionada manualmente pelo usuário no lado que o envia. Se usando o modo “Smart”, o arquivo resultante pode não estar igual ao original quando enviado a um Macintosh, porque pode perder seu criador e tipos de códigos. Este modo permanece no produto principalmente devido ao fato que estava em PGP Versão 5.0, e alguns usuários podem ter apenas a necessidade de enviar os tipos de arquivo acima. Esta opção não é recomendada na maioria dos casos.

Em resumo, se você está enviando apenas para as Versões 6.0 ou superiores, sempre selecione “MacBinary: Yes” (o padrão). Assim, você não precisa ficar pensando, se seu ambiente está usando exclusivamente PGP Versão 6.0. Quando enviando aos usuários com versões mais antigas, você deve selecionar “MacBinary: No” para tipos de arquivos inter-plataformas e “MacBinary: Yes” para arquivos que simplesmente não seriam legíveis para usuários de PC de qualquer maneira (como um aplicativo MacOS).

NOTA: PGP Versão 5.0 não teve uma opção “MacBinary: No”. Para enviar tipos de arquivo sem MacBinary, que não está incluído na lista para “MacBinary: Smart” para um PC que usa 5.0, o arquivo deve ser configurado manualmente para um dos criadores e tipos de código na lista “Smart” antes de ser enviado.

Recebendo arquivos Windows no MacOS

Quando decifrando, PGP Versão 6.0 tenta automaticamente traduzir extensões de nomes de arquivo para arquivos não-MacBinary em informações de criador e tipo para MacOS. Por exemplo, se você receber um arquivo de Windows com uma extensão “.doc”, o arquivo será salvo como um documento Microsoft Word. A mesma lista de aplicações usada quando adicionando extensões de nomes de arquivos na recepção de um arquivo MacBinary em Windows é usada para traduzir extensões de nomes de arquivos de volta ao equivalente MacOS quando recebido em um computador Macintosh. Em quase todos os casos, isto resulta em arquivos que são imediatamente legíveis e que podem ser duplamente clicáveis em MacOS.

Versões anteriores de PGP para MacOS não têm esta característica. O usuário precisa determinar manualmente que um arquivo de nome “relatório.doc” é um arquivo Microsoft Word. Depois de determinar o aplicativo criador, no caso de Microsoft Word, a pessoa pode simplesmente usar a caixa de diálogo “Abrir” para abrir o arquivo selecionando “Exibir Todos os Arquivos” no menu popup. Muitos outros aplicativos também têm esta característica, mas alguns não. Se o documento não pode ser aberto de dentro do aplicativo, o usuário tem que descobrir qual o programa criador no Macintosh apropriado e tipos de código para o arquivo e manualmente os fixar com um utilitário de terceiros. Há muitos utilitários gratuitos para se fazer isto. Atualizando para a Versão 6.0 provavelmente é a opção mais fácil neste caso, já que elimina este problema.

Aplicativos Suportados

A seguinte lista de principais aplicativos produzem documentos que são automaticamente traduzidos por PGP 6.0 quando enviados de Windows para MacOS e vice-versa. Neste momento, não há uma forma de um usuário adicionar ou alterar estas conversões, entretanto, nós poderemos adicionar tal funcionalidade no futuro.

- Photoshop (GIF, documentos nativos do Photoshop, TGA, JPEG)
- PageMaker (Versões 3.X, 4.X, 5.X, 6.X)
- Microsoft Project (arquivos de projeto e modelos)
- FileMaker Pro
- Adobe Acrobat
- Lotus 123

- Microsoft Word (texto, RTF, modelos)
- PGP
- Microsoft PowerPoint
- StuffIt
- QuickTime
- Corel WordPerfect
- Microsoft Excel (muitos diferentes tipos de arquivos)
- Quark XPress

As seguintes extensões gerais de nomes de arquivos também são convertidas:

.cvs	.arj	.ima	.eps	.mac	.cgm
.dl	.fli	.ico	.iff	.img	.lbm
.msp	.pac	.pbm	.pcs	.pcx	.pgm
.plt	.pm	.ppm	.rif	.rle	.shp
.spc	.sr	.sun	.sup	.wmf	.flc
.gz	.vga	.hal	.lzh	.Z	.exe
.mpg	.dvi	.tex	.aif	.zip	.au
.mod	.svx	.wav	.tar	.pct	.pic
.pit	.txt	.mdi	.pak	.tif	.eps

Phil Zimmermann sobre PGP C

Este capítulo contém informações introdutórias e originais sobre criptografia e PGP, como escrito por Phil Zimmermann.

Por que escrevi PGP

“Tudo que você fizer será insignificante, mas o importante é que você faça.” - Mahatma Gandhi.

É pessoal. É particular. E não interessa a ninguém além de você. Você pode estar planejando uma campanha política, discutindo seus impostos, ou tendo um romance secreto. Ou você pode estar se comunicando com um dissidente político em um país repressor. Seja o que for, você não quer que sua correspondência eletrônica particular (email) ou documentos confidenciais sejam lidos por qualquer um. Não há nada de errado em reivindicar sua privacidade. Privacidade é tão importante quanto a Constituição.

O direito à privacidade está divulgado implicitamente através da Lei de Direitos. Mas quando a constituição dos Estados Unidos estava sendo criada, os fundadores não viram a necessidade de explicitamente afirmar o direito à uma conversa privada. Isso seria tolice. Duzentos anos atrás, todas as conversas eram privadas. Se alguém mais estivesse ao alcance da voz, você poderia simplesmente ir para trás do pátio e ter sua conversa lá. Ninguém poderia ouvir sem seu conhecimento. O direito à conversa privada era um direito natural, não apenas em um sentido filosófico, mas um sentido de lei da física, dada a tecnologia da época.

Mas com a chegada da era da informação, começando com a invenção do telefone, tudo isto mudou. Agora a maioria de nossas conversas é conduzida eletronicamente. Isto permite que nossas conversas mais íntimas estejam expostas sem nosso conhecimento. Chamadas de telefones celulares podem ser monitorados por qualquer um com um rádio. Correspondência eletrônica, enviada através da Internet, não é mais segura que uma chamada de telefone celular. Email está rapidamente substituindo a correspondência postal, tornando-se norma para todos, não a novidade que era no passado. E email pode ser pesquisado de forma rotineira e automática por palavras-chave interessantes, em uma larga escala, sem detecção. É como pescaria com rede.

Talvez você ache que seu email é suficientemente legítimo e que a criptografia seja injustificável. Se você realmente é um cidadão obediente à lei e que não tem nada a esconder, então, por que você não envia sempre o conteúdo de suas correspondências em cartões postais? Por que não se submete a teste de drogas quando pedido? Por que pedir um mandato judicial para que a polícia entre em sua casa? Você está tentando esconder algo? Se você esconde sua correspondência dentro de envelopes, isto significa que você

deve ser um subversivo ou um traficante, ou talvez um louco paranóico? Algum cidadão obediente à lei tem necessidade de criptografar seu email?

E se todo mundo acreditasse que os cidadãos obedientes à lei deveriam usar cartões postais para suas correspondências? Se algum não-conformista tentasse assegurar sua privacidade usando um envelope para sua correspondência, isto despertaria suspeitas. Talvez as autoridades abrissem sua correspondência para ver o que ele está escondendo. Felizmente, não vivemos neste tipo de mundo, porque todos protegem a maioria de suas correspondências com envelopes. Assim, ninguém desperta suspeita quando garante sua privacidade com um envelope. Há segurança nos números. De forma análoga, seria bom se todos habitualmente usassem a criptografia em todos os seus emails, inocentes ou não, de modo que ninguém levantasse suspeita quando assegurasse sua privacidade de email com codificação. Pense nisso como uma forma de solidariedade.

Até agora, se o governo quisesse violar a privacidade de cidadãos comuns, teria que gastar uma certa quantia de dinheiro e trabalho para interceptar, abrir e ler correspondências em papel. Ou teria que ouvir e possivelmente transcrever conversas por telefone, ao menos antes da tecnologia de reconhecimento automático de voz estar disponível. Este tipo de monitoração trabalhosa não é prático em larga escala. Isto era feito somente em casos importantes quando parecia valer a pena.

A Lei 266 do Senado, uma lei anticrime de 1991, tinha uma medida não muito clara escondida nela. Se esta resolução não obrigatória tivesse se tornado uma lei de verdade, teria forçado que fabricantes de equipamentos de comunicação segura a inserir “armadilhas” especiais em seus produtos, de forma que o governo pudesse ler mensagens criptografadas de qualquer pessoa. Esta lei diz: “É decisão do Congresso que fornecedores de serviços de comunicação eletrônica e fabricantes de equipamentos de serviço de comunicação eletrônica assegurem que os sistemas de comunicações permitam que o governo obtenha o conteúdo integral de voz, dados, e outras comunicações quando apropriadamente autorizados por lei”. Foi esta medida que me levou a publicar eletronicamente PGP de forma gratuita naquele ano, pouco tempo após a medida ser anulada após vigorosos protestos de civis liberais e grupos industriais.

Em 1994 a Lei de Telefonia Digital ordenava que as companhias telefônicas instalassem portas de escuta remota em seus aparelhos digitais nos escritórios centrais, criando uma nova infra-estrutura tecnológica para “apontar-e-clicar” escutas, de forma que agentes federais não precisam mais sair e colocar presilhas (“jacarés”) às linhas telefônicas. Agora eles podem sentar em seus escritórios centrais e escutar suas chamadas telefônicas. Claro, a lei ainda requer uma ordem da Corte para uma escuta. Mas enquanto a infra-estrutura tecnológica pode persistir por gerações, leis e polícias podem mudar do dia para a noite. Uma vez que uma infra-estrutura de comunicações otimizada para vigilância se torna entrincheirada, uma guinada nas condições políticas levar ao abuso deste novo poder. Condições políticas podem mudar com a eleição de um novo governo, ou mesmo de forma mais abrupta como o bombardeamento de um prédio federal.

Um ano após a Lei de Telefonia Digital passar, o FBI revelou planos de exigir às companhias telefônicas que construíssem em sua infra-estrutura a capacidade para monitorar simultaneamente um por cento de todos os telefonemas feitos em todas as principais cidades norte-americanas. Isto representaria um aumento superior a mil vezes

sobre níveis anteriores no número de telefones que poderiam ser monitorados. Em anos anteriores, havia apenas cerca de mil monitoramentos ordenados pelos tribunais nos Estados Unidos por ano, em nível federal, estadual e local combinados. É duro ver como o governo pode empregar suficientes juízes até mesmo para assinar ordens de monitoramento suficientes para monitorar 1 por cento de todos nossos telefonemas, muito menos contratar agentes federais suficientes para sentarem e escutar todo aquele tráfego em tempo real. O único modo plausível de processar essa quantidade de tráfego é um enorme aplicativo Orwelliano de tecnologia de reconhecimento de voz automatizado para peneirar tudo isso, procurar palavras-chave interessantes ou procura pela voz de um locutor em particular. Se o governo não acha seu alvo na primeira amostra de 1 por cento, o monitoramento pode ser alterado para outro 1 por cento diferente até o alvo ser achado, ou até a linha telefônica de todo mundo for verificada por tráfego subversivo. O FBI diz que eles precisam desta capacidade para planejar para o futuro. Este plano causou tal revolta que foi derrotado no Congresso, pelo menos desta vez, em 1995. Mas o mero fato do FBI ter pedido tais grandes poderes revela o programa de trabalho deles. E a derrota deste plano não é tão tranquilizante assim, quando você considera que a Lei de Telefonia Digital de 1994 também foi derrotada na primeira vez em que foi introduzida, em 1993.

Avanços na tecnologia não irão permitir a manutenção deste status quo, ao menos ao quanto diz respeito à privacidade. O status quo é instável. Se não fazemos nada, novas tecnologias darão ao governo novas capacidades de vigilância automática que Stalin jamais teria sonhado. A única forma de manter a linha na privacidade na era da informação é a criptografia forte.

Você não precisa duvidar do governo se quer usar criptografia. Seus negócios podem ser monitorados por rivais nos negócios, crime organizado, ou governos estrangeiros. Diversos governos estrangeiros, por exemplo, admitem usar seus sinais de inteligência contra companhias de outros países para dar à suas próprias corporações uma margem competitiva. Ironicamente, as restrições do governo dos Estados Unidos à criptografia têm enfraquecido as defesas das corporações americanas contra inteligências estrangeiras e o crime organizado.

O governo sabe que regra central a criptografia está destinada a ter nas poderosas relações com seu povo. Em abril de 1993, a administração Clinton revelou uma nova e grande iniciativa política de codificação, que estava em desenvolvimento na Agência de Segurança Nacional, (National Security Agency - NSA) desde o início da administração Bush. A peça central desta iniciativa é um dispositivo de criptografia planejado pelo governo, chamado de chip “Clipper”, contendo um novo algoritmo de criptografia secreto da NSA. O Governo tentou incentivar a indústria privada a projetá-lo em todos os seus produtos de comunicação segura, como telefones seguros, fax seguros etc. AT&T colocou “Clipper” em seus produtos de voz seguros. A tramóia: na hora da fabricação, cada chip Clipper é carregado com sua única chave própria, a qual o Governo terá uma cópia, que é colocada em juízo. Nada com o que se preocupar, porque o governo promete que usará estas chaves para ler seu tráfego apenas “quando devidamente autorizado por lei”. Claro, para tornar “Clipper” completamente efetivo, o próximo passo lógico seria considerar ilegal outras formas de criptografia.

O governo inicialmente afirmou que o uso de “Clipper” seria voluntário, que ninguém seria forçado a usá-lo ao invés de outros tipos de criptografia. Mas a reação pública contra

o chip “Clipper” tem sido forte, ainda mais forte que o governo antecipou. A indústria de computadores afirmou em uma só voz sua oposição contra o uso de “Clipper”. O diretor do FBI Louis Freeh respondeu à uma pergunta em uma conferência da imprensa em 1994 dizendo que se “Clipper” falhasse em obter suporte do público, e os monitoramentos do FBI fossem terminados por criptografia não controlada pelo governo, seu escritório não teria escolha além de procurar auxílio legislativo. Mais tarde, na consequência da tragédia de Oklahoma City, o sr. Freeh testemunhou ao Comitê Judiciário do Senado que a disponibilidade pública de criptografia forte deveria ser reduzida pelo governo (embora ninguém houvesse sugerido que criptografia era usada pelos bombardeiros).

O Centro de Informações de Privacidade Eletrônica (Electronic Privacy Information Center - EPIC) obteve alguns documentos esclarecedores sob o Ato de Liberdade de Informação. Em um breve documento intitulado “Codificação: A Ameaça, Aplicações e Soluções Potenciais”, e enviado ao Conselho de Segurança Nacional em fevereiro de 1993, o FBI, NSA, e o Departamento de Justiça (DOJ) concluíram que “soluções técnicas, como elas são, só funcionarão se elas estiverem incorporadas em todos os produtos de codificação. Para assegurar que isto aconteça, requer-se legislação que designe o uso de produtos de codificação aprovados pelo governo ou aderência à critérios de codificação governamental”.

O governo tem um registro de passos que não inspira confiança em que eles nunca abusarão de nossas liberdades civis. O programa COINTELPRO do FBI tinha como alvo grupos que se opunham às políticas governamentais. Eles espionaram no movimento antibélico e o movimento de direitos civis. Eles grampearam o telefone de Martin Luther King Jr. Nixon teve sua lista de inimigos. E então houve a bagunça de Watergate. O congresso parece agora ter a intenção de votar leis que reduzem nossa liberdade civil na Internet. Em nenhum momento no século passado a desconfiança do público com o governo no espectro político tem sido tão amplamente distribuída, como é hoje.

Se nós quisermos resistir a esta obscura tendência do governo em proscrever a criptografia, uma medida que podemos aplicar é usar criptografia o máximo que pudermos agora enquanto ainda é legal. Quando o uso de criptografia forte se torna popular, é mais difícil para o governo criminalizá-la. Assim, o uso de PGP é bom para preservar a democracia.

Se privacidade for considerada ilegal, somente os criminosos terão privacidade. As agências de inteligência têm acesso a boa tecnologia criptográfica. Assim como os grandes traficantes de armas e drogas. Mas pessoas comuns e organizações políticas populares em sua maioria não tiveram acesso à tecnologia de criptografia por chave pública de “nível militar” disponível. Até agora.

PGP dá poderes às pessoas para colocar suas privacidades em suas próprias mãos. Existe uma crescente necessidade social por ela. Foi por isto que eu o criei.

Os algoritmos simétricos de PGP

PGP oferece uma seleção de diferentes algoritmos de chaves secretas para codificar a mensagem atual. Por algoritmo de chave secreta, queremos dizer uma cifra de blocos convencional, ou simétricos, que usa a mesma chave para codificar e para decifrar. As três cifras de blocos simétricos oferecidos por PGP são CAST, Triple-DES, e IDEA. Eles não são algoritmos “caseiros”. Todos eles foram desenvolvidos por times de criptógrafos de reconhecida reputação.

Para os criptograficamente curiosos, todas as três cifras operam em blocos de texto puro e texto cifrado de 64 bits. CAST e IDEA possuem chaves de 128 bits de tamanho, enquanto Triple-DES usa uma chave de 168 bits. Como o “Data Encryption Standard” (DES), qualquer uma dessas cifras pode ser usada em modos de Realimentação de Cifras (“cipher feedback”, ou CFB) e Ligações de Blocos de Cifras (“cipher block chaining”, ou CBC). PGP as usa em modo CFB de 64 bits.

Eu incluí o algoritmo de codificação CAST em PGP porque ele mostra promessas como uma boa cifra de blocos com sua chave de 128 bits de tamanho, é rápido, e é gratuito. Seu nome é derivado das iniciais de seus projetistas, Carlisle Adams e Stafford Tavares da Northern Telecom (Nortel). Nortel pediu uma patente para CAST, mas eles se comprometeram a tornar CAST disponível a qualquer um sem pagamento de “royalties”. CAST parece ser excepcionalmente bem projetado, por pessoas com boa reputação no campo. O projeto é baseado em uma aproximação bastante formal, com um número de assertivas formalmente prováveis, que dão boas razões para acreditar que ele provavelmente requer exaustão de chaves para quebrar sua chave de 128 bits. CAST não possui chaves fracas ou semifracas. Há fortes argumentos que CAST é imune tanto à criptoanálise linear e diferencial, as duas formas mais poderosas de criptoanálise na literatura publicada, onde ambas foram efetivas em quebrar o “Data Encryption Standard” (DES). CAST é muito novo para ter desenvolvido um longo registro de seus passos, mas seu projeto formal e a boa reputação de seus projetistas irão sem dúvida atrair as atenções e tentativas de ataques criptoanalíticos do resto da comunidade acadêmica de criptografia. Eu estou tendo a mesmo grau de confiança com CAST que tive anos atrás com IDEA, a cifra que selecionei para uso nas primeiras versões de PGP. Naquela época, IDEA também era muito novo para ter um registro de passos, mas têm suportado bem.

A cifra de blocos IDEA (“International Data Encryption Algorithm”, ou Algoritmo Internacional de Codificação de Dados) baseia-se no conceito de projeto de “misturar operações de grupos algébricos diferentes”. Isto foi desenvolvido na ETH em Zurique por James L. Massey e Xuejia Lai, e publicado em 1990. Documentos publicados anteriormente sobre o algoritmo o chamavam de IPES (“Improved Proposed Encryption Standard”, ou Padrão Melhorado de Codificação Proposto), mas eles mudaram o nome depois para IDEA. Até agora, IDEA tem resistido bem melhor a ataques, que outras cifras como FEAL, REDOC-II, LOKI, Snefru e Khafre. E IDEA é mais resistente que DES em ataques de criptoanálise diferencial de grande sucesso de Biham e Shamir, como também em ataques de criptoanálise linear. Como esta cifra continua atraindo esforços de ataque dos mais formidáveis cantos do mundo criptoanalítico, a confiança em IDEA está crescendo com a passagem do tempo. Tristemente, o obstáculo maior para a aceitação de IDEA

como um padrão foi o fato que Ascom Systec mantém a patente de seu projeto, e ao contrário de DES e CAST, IDEA não foi disponibilizado a todo o mundo em bases gratuitas.

Para finalizar, PGP inclui três chaves Triple-DES em seu repertório de cifras de bloco disponíveis. O DES foi desenvolvido pela IBM em meados dos anos setenta. Apesar de ter um bom projeto, sua chave de 56 bits de tamanho é muito pequena para os padrões de hoje. Triple-DES é muito forte, e tem sido bem estudado por muitos anos, assim poderia ser uma aposta mais segura que as cifras mais novas como CAST e IDEA. Triple-DES é o DES aplicado três vezes para o mesmo bloco de dados, usando três chaves diferentes, exceto que a segunda operação de DES é feita de trás para frente, em modo de decifragem. Apesar de Triple-DES ser muito mais lento que CAST ou IDEA, velocidade normalmente não é crítico para aplicativos de email. Embora Triple-DES use uma chave de 168 bits de tamanho, parece ter uma força efetiva de chave de pelo menos 112 bits contra um atacante, com uma capacidade impossivelmente imensa de armazenamento de dados para usar no ataque. De acordo com um documento apresentado por Michael Weiner na Crypto96, qualquer quantia remotamente plausível de armazenamento de dados disponível ao atacante permitiria um ataque que requereria tanto trabalho quanto a quebra de uma chave de 129 bits. Triple-DES não está amarrado por qualquer patente.

Chaves públicas PGP que foram geradas por PGP Versão 5.0 ou superiores possuem informações embutidas nelas que dizem ao emitente quais blocos de cifragem são entendidas pelo software do destinatário, de forma que o software do emitente saiba quais cifras podem ser usadas para codificação. Chaves públicas Diffie-Hellman/DSS aceitam CAST, IDEA, ou Triple-DES como cifra de bloco, com CAST sendo a seleção padrão. No presente, por motivos de compatibilidade, chaves RSA não possuem este recurso. Apenas a cifra IDEA é usada por PGP para enviar mensagens para chaves RSA, porque versões mais antigas de PGP apenas suportavam RSA e IDEA.

Sobre as rotinas de compressão de dados de PGP

PGP normalmente comprime (compacta) o texto puro antes de codificá-lo, porque é tarde demais comprimir o texto puro após ele ser codificado; dados codificados não são comprimíveis. Compressão de dados poupa tempo de transmissões via modem e espaço em disco e, mais importante, aumenta a força da segurança criptográfica. As maiorias das técnicas criptoanalíticas exploram redundâncias encontradas no texto puro para quebrar a cifra. Compressão de dados reduz esta redundância no texto puro, portanto melhorando bastante a resistência à criptoanálise. Leva tempo extra comprimir o texto puro, mas de um ponto de vista de segurança vale a pena.

Arquivos que são muito pequenos para comprimir, ou que não comprimem bem, não são comprimidos por PGP. Além disso, o programa reconhece arquivos produzidos pelos programas de compressão mais populares, como PKZIP, e não tenta comprimir um arquivo que já foi comprimido.

Para os tecnicamente curiosos, o programa usa as rotinas de compressão freeware ZIP escritas por Jean-Loup Gailly, Mark Adler, e Richard B. Wales. Este software ZIP usa

algoritmos de compressão que são funcionalmente equivalentes àqueles usados pela PKWare em PKZIP 2.x. Este software de compressão ZIP foi escolhido para PGP principalmente porque tem uma taxa de compressão realmente boa e porque é rápido.

Sobre os números aleatórios usados como chaves de sessão

PGP usa um criptograficamente forte gerador de números pseudo-aleatórios para criar chaves de sessão temporárias. Se este arquivo de inicialização de números aleatórios não existir, ele é automaticamente criado e iniciado com números realmente aleatórios derivados de seus eventos aleatórios, obtidos pelo programa PGP através do tempo de seu pressionar de teclas e movimentos do mouse.

Este gerador reinicializa o arquivo de inicialização a cada vez que é usado, misturando novo material parcialmente derivado da hora do dia e outras fontes verdadeiramente aleatórias. Ele usa algoritmos convencionais de codificação como motor para o gerador de números aleatórios. O arquivo de inicialização contém tanto material de inicialização aleatória quanto material de chaves aleatórias, usadas para tensionar o motor de codificação condicional para o gerador aleatório.

Este arquivo de inicialização aleatória deve ser protegido de descobertas, para reduzir o risco de um atacante derivar suas próximas ou anteriores chaves de sessão. O atacante teria um tempo muito duro para obter qualquer coisa útil através da captura deste arquivo de inicialização aleatória, porque o arquivo é criptograficamente limpo antes e depois de cada uso. De qualquer forma, parece ser prudente tentar mantê-lo longe de mãos erradas. Se possível, faça o arquivo legível apenas por você. Se não for possível, não deixe outras pessoas indiscriminadamente copiar discos de seu computador.

Sobre o sumário da mensagem

O sumário da mensagem (no original, “message digest”) é um “destilado” compacto (de 160 ou 128 bits) do “checksum” (um método de detecção de erros) de sua mensagem ou arquivo. Você pode pensar nele como a “impressão digital” da mensagem ou arquivo. O sumário da mensagem “representa” sua mensagem, de forma que se a mensagem fosse alterada de qualquer forma, um diferente sumário da mensagem seria computado dela. Isto torna possível detectar quaisquer alterações feitas em uma mensagem por um falsificador. Um sumário da mensagem é computado usando uma função hash de caminho único criptograficamente forte na mensagem. Deve ser computacionalmente impraticável para um atacante planejar uma mensagem substitua que produziria um sumário da mensagem idêntico. Neste respeito, um sumário da mensagem é muito melhor que um “checksum”, porque é fácil projetar uma mensagem diferente que produziria o mesmo “checksum”. Mas, como um “checksum”, você não pode derivar a mensagem original de seu sumário da mensagem.

O algoritmo de sumário da mensagem agora usado em PGP (versões 5.0 e posteriores) é chamado SHA, abreviação de “Secure Hash Algorithm” (ou Algoritmo de Hash Seguro),

projetado pela NSA para o “National Institute of Standards and Technology” (NIST). SHA é um algoritmo de hash de 160 bits. Algumas pessoas podem olhar qualquer coisa da NSA com suspeita, porque a NSA tem a função de interceptar comunicações e quebrar códigos. Mas tenha em mente que a NSA não tem interesse em forjar assinaturas, e o governo seria beneficiado com um bom padrão de assinaturas digitais infalsificáveis que iria impedir qualquer um de rejeitar suas assinaturas. Isto possui benefícios distintos para fazer cumprir a lei e reunir inteligência. Também, SHA tem sido publicado na literatura aberta e tem sido extensivamente e atentamente revisto pela maioria dos melhores criptógrafos no mundo, que se especializaram em funções hash, e a opinião unânime é que SHA é extremamente bem projetado. Ele possui algumas inovações de projeto que vencem todas as fraquezas observadas em algoritmos de sumários da mensagem anteriormente publicados por criptógrafos acadêmicos. Todas as novas versões de PGP usam SHA como algoritmo de “sumário da mensagem” para criar assinaturas com as novas chaves DSS que seguem o Padrão de Assinatura Digital do NIST. Por razões de compatibilidade, novas versões de PGP ainda usam MD5 para assinaturas RSA, porque versões antigas de PGP usavam MD5 para assinaturas RSA.

O algoritmo de sumário da mensagem usado por versões antigas de PGP é o Algoritmo de Sumário da Mensagem MD5, colocado em domínio público pela RSA Data Security, Inc. MD5 é um algoritmo hash de 128 bits. Em 1996, MD5 foi quebrado por um criptógrafo alemão, Hans Dobbertin. Apesar de MD5 não ter sido completamente quebrado na época, foi descoberto que ele possui fraquezas tão sérias que ninguém deveria continuar usando-o para gerar assinaturas. Maiores trabalhos nesta área poderão quebrá-lo completamente, permitindo que assinaturas sejam falsificadas. Se você não quer um dia descobrir sua assinatura digital PGP em uma confissão falsificada, aconselha-se que você migre para as novas chaves DSS de PGP como método preferido para criar assinaturas digitais, porque DSS usa SHA como seu algoritmo hash seguro.

Como proteger suas chaves públicas de falsificações

Num sistema de criptografia por chave pública, você não precisa proteger as chaves públicas da exposição. Na verdade, é melhor se elas forem largamente disseminadas. Mas é importante proteger as chaves públicas de falsificações, para ter a certeza de que uma determinada chave realmente pertence a quem ela aparenta pertencer. Talvez seja esta a vulnerabilidade mais importante de um sistema de criptografia por chave pública. Vamos primeiro considerar um desastre potencial, então ver como evitá-lo com segurança utilizando PGP.

Suponhamos que você quer enviar uma mensagem privada para a Alice. Você faz o “download” do certificado da chave pública de Alice de uma BBS (“Bulletin Board System”). Você codifica sua carta para Alice com esta chave pública, e a envia para ela através do serviço de email da BBS.

Infelizmente, sem que você e Alice saibam, um outro utilizador chamado Charlie infiltrou-se na BBS e gerou uma chave pública para ele com o ID de usuário de Alice anexado. Ele secretamente substitui sua chave falsa pela chave pública verdadeira de Alice. Você inadvertidamente usa esta chave falsa de Charlie ao invés da chave pública de Alice. Tudo

parece normal porque a chave falsa tem o ID de usuário de Alice. Agora Charlie pode decifrar a mensagem enviada para ela porque tem a chave privada correspondente. Ele pode até mesmo re-codificar novamente a mensagem decifrada com a chave pública verdadeira de Alice e enviar a mensagem para ela, de modo que ninguém suspeite algo errado. Além disso, ele pode mesmo forjar assinaturas aparentemente boas de Alice com esta chave privada, porque todo mundo estará usando a chave pública falsa para verificar as assinaturas de Alice.

O único jeito de evitar este desastre é prevenir qualquer um de falsificações de chaves públicas. Se você recebeu a chave pública de Alice diretamente dela, não há problema. Mas isto pode ser difícil se ela estiver a milhares de quilômetros de distância, ou estiver atualmente inacessível.

Talvez você pudesse obter a chave pública de Alice de um amigo confiado por ambos, David, que sabe que possui uma cópia boa da chave pública de Alice. David poderia assinar a chave pública de Alice, garantindo a integridade da chave pública. David criaria esta assinatura com sua própria chave privada.

Isto criaria um certificado assinado de chave pública, indicando que a chave de Alice não foi falsificada. Isto requer que você tenha uma cópia boa da chave pública de David para verificar a assinatura dele. Talvez David também pudesse fornecer a Alice uma cópia assinada de sua chave pública. David estaria assim servindo como um “Apresentador” entre você e Alice.

Este certificado assinado de chave pública para Alice poderia ser transferido por David ou Alice para a BBS, e você poderia fazer o “download” dele mais tarde. Você poderia então verificar a assinatura através da chave pública de David, e assim se certificar de que esta é realmente a chave pública de Alice. Nenhum impostor pode tentar enganá-lo mostrando sua própria chave falsa como sendo a de Alice, porque ninguém mais pode forjar assinaturas feitas por David.

Uma pessoa amplamente confiada poderia até especializar-se em fazer este serviço de “apresentar” usuários para outros, provendo assinaturas para seus certificados de chave pública. Esta pessoa confiada poderia ser considerada como uma “Autoridade de Certificação”. Quaisquer certificados de chave pública que tivessem a assinatura da Autoridade de Certificação poderiam ser considerados como realmente pertencentes às pessoas a quem aparentam pertencer. Todos os utilizadores que quisessem participar precisariam de uma cópia boa conhecida apenas da chave pública da Autoridade de Certificação, de uma forma que as assinaturas da Autoridade de Certificação pudessem ser verificadas. Em alguns casos, a Autoridade de Certificação também poderia atuar como um servidor de chaves, permitindo usuários em uma rede procurar por chaves públicas pedindo-as ao servidor de chaves, mas não há razão para um servidor de chaves também precisar certificar chaves.

Uma Autoridade de Certificação confiada e centralizada é especialmente apropriada para grandes corporações impessoais centralmente controladas ou para instituições governamentais. Alguns ambientes institucionais usam hierarquias de Autoridades de Certificação.

Para ambientes mais descentralizados, permitir que todos os usuários atuem como apresentadores confiáveis para seus amigos provavelmente funcionaria melhor que uma autoridade de certificação centralizada.

Um dos recursos atrativos de PGP é que ele opera igualmente bem em um ambiente centralizado com uma Autoridade de Certificação ou em um ambiente mais descentralizado onde os indivíduos trocam chaves pessoais.

Todo esse negócio de proteger chaves públicas de falsificações é o problema único mais difícil em aplicativos práticos de chave pública. É o “calcanhar de Aquiles” da criptografia por chave pública, e um bocado da complexidade do software diz respeito à solução deste problema.

Você deve usar uma chave pública somente depois de ter certeza de que se trata de uma chave boa que não foi falsificada, e que ela realmente pertence à pessoa a quem pretende estar associada. Você pode estar certo disto se você obter este certificado de chave pública diretamente de seu proprietário, ou se ela leva a assinatura de uma outra pessoa que você confia, e de quem você já possui uma chave pública boa. Também, o ID de usuário deveria ter o nome completo do proprietário da chave, não apenas seu primeiro nome.

Não importa o quão tentado você fique, você *nunca* deve deixar a prudência de lado e confiar em uma chave pública que transferiu de uma BBS, a menos que ela esteja assinada por alguém que você confie. Aquela chave pública não certificada poderia ter sido falsificada por qualquer um, talvez até pelo administrador de sistema da BBS.

Se lhe pedirem para assinar o certificado de chave pública de alguém, certifique-se de que ele realmente pertence à pessoa mencionada no ID de usuário daquele certificado. Isto porque sua assinatura neste certificado de chave pública é uma promessa feita por você que esta chave realmente pertence àquela pessoa. Outras pessoas que confiem em você aceitarão a chave pública da pessoa porque ela leva sua assinatura. Não é aconselhável confiar no que outros dizem — não assine a chave pública a menos que tenha conhecimento de primeira mão que esta chave realmente pertence à pessoa. Preferivelmente, você deve assiná-la somente se conseguir diretamente dela.

De forma a assinar uma chave pública, você deve ter muito mais certeza da propriedade da chave do que se meramente a quiser usar para codificar uma mensagem. Para estar convencido da validade de uma chave o suficiente para usá-la, assinaturas de certificação de apresentadores confiáveis devem bastar. Mas, para assinar por si só uma chave, você deve ter um conhecimento próprio de primeira mão sobre quem a possui. Talvez você possa ligar para o proprietário da chave e ler a impressão digital da chave para ele, para confirmar que a chave que você tem é realmente dele — e certificar-se de que está realmente falando com a pessoa certa.

Tenha em mente que sua assinatura num certificado de chave pública não garante a integridade daquela pessoa, mas apenas garante a integridade (a propriedade) da chave pública desta pessoa. Você não está arriscando sua credibilidade quando assina a chave pública de um sociopata, se estiver completamente certo que a chave realmente pertence a ele. Outras pessoas aceitariam a chave como pertencendo a ele porque você a assinou

(assumindo que eles confiam em você), mas eles não confiariam no proprietário da chave. Confiar em uma chave não é a mesma coisa que confiar no proprietário da chave.

Seria uma boa idéia manter sua própria chave pública em mãos com uma coleção de assinaturas de certificação anexas, de uma série de “apresentadores”, na esperança que a maioria das pessoas confiem em pelo menos um dos apresentadores que garantem a validade da sua chave pública. Você poderia colocar sua chave com a coleção anexada de assinaturas de certificação em várias BBSs. Se você assinar a chave pública de alguém, envie-a de volta à pessoa com sua assinatura, de forma que ele possa acrescentar sua assinatura à sua própria coleção de credenciais para sua chave pública.

Certifique-se de que ninguém possa falsificar o seu próprio chaveiro público. A verificação de um certificado de chave pública recém assinado deve definitivamente depender da integridade das chaves públicas confiáveis que já estão em seu próprio chaveiro público. Mantenha controle físico sobre seu chaveiro público, preferencialmente em seu próprio computador pessoal ao invés de em um sistema remoto de compartilhamento de tempo, como você faria com sua chave privada. Isto é para protegê-lo de falsificações, não de exposição. Mantenha uma cópia *backup* confiável de seu chaveiro público e de sua chave privada em uma mídia protegida contra gravação.

Já que sua própria chave pública confiável é usada como autoridade final para direta ou indiretamente certificar todas as outras chaves no seu chaveiro, ela é a chave mais importante a ser protegida contra falsificações. Você pode querer manter uma cópia *backup* dela em um disquete protegido contra gravação.

PGP geralmente assume que você mantém segurança física sobre seu sistema e seus chaveiros, como também à sua própria cópia de PGP. Se um intruso conseguir falsificar seu disco, então em teoria ele poderá falsificar o próprio programa, tornando inúteis as proteções que o programa pode ter para detectar falsificações com chaves.

Uma forma um tanto complicada de proteger todo seu chaveiro de falsificações é assinando-o todo com sua própria chave privada. Você poderia fazer isso fazendo um “certificado de assinatura separada” do seu chaveiro público.

Como PGP mantém registro de quais chaves são válidas?

Antes de ler esta seção, você deveria ler a seção anterior, [“Como proteger chaves públicas de falsificações”](#).

PGP mantém registro de quais chaves no seu chaveiro público estão apropriadamente certificadas com assinaturas de apresentadores que você confia. Tudo o que você tem a fazer é dizer a PGP quais pessoas você confia como apresentadores, e certificar você mesmo as chaves destes com sua chave privada. A partir daí PGP automaticamente validará quaisquer outras chaves que tenham sido assinadas pelos apresentadores que você designou. E é claro que você pode diretamente assinar mais chaves você mesmo.

Há dois critérios completamente diferentes que PGP usa para julgar a utilidade de uma chave pública — não as confunda:

1. A chave realmente pertence a quem ela aparenta pertencer? Em outras palavras, ela foi certificada por uma assinatura confiável?
2. A chave pertence a alguém em quem você pode confiar para certificar outras chaves?

PGP pode calcular a resposta para a primeira questão. Para responder à segunda questão, você deve dizer explicitamente a PGP. Quando você fornece a resposta à questão 2, PGP então calcula a resposta para a questão 1 para outras chaves assinadas pelo apresentador que você designou como sendo confiável.

Chaves que foram certificadas por um apresentador confiável são consideradas válidas por PGP. As chaves que pertençam a apresentadores confiáveis devem ser elas próprias serem certificadas ou por você ou por outros apresentadores confiáveis.

PGP também permite a possibilidade de você ter vários níveis de confiança para as pessoas que atuam como apresentadores. Sua confiança para um proprietário de uma chave atuar como um apresentador não simplesmente reflete sua estima em sua integridade pessoal — ela também deve refletir quão competente você pensa que eles são em entender o gerenciamento de chaves e usar um bom julgamento quando assinam chaves. Você pode designar uma pessoa como não confiável, marginalmente confiável, ou totalmente confiável para certificar outras chaves públicas. Esta informação sobre confiança é armazenada em seu chaveiro com as chaves destes, mas quando você diz a PGP para copiar uma chave que não está em seu chaveiro, PGP não copia a informação sobre confiança juntamente com a chave, porque suas opiniões pessoais sobre confiança são consideradas confidenciais.

Quando PGP está calculando a validade de uma chave pública, ele examina o nível de confiança de todas as assinaturas de certificação anexadas a ela. Ele computa uma nota média de validade — por exemplo, duas assinaturas marginalmente confiáveis são consideradas tão dignas de crédito quanto uma assinatura de confiança completa. O ceticismo do programa é ajustável — por exemplo, você pode regular PGP para requerer duas assinaturas de total confiança ou três de confiança marginal para julgar uma chave como válida.

Sua própria chave é “axiomaticamente” válida para PGP, não necessitando de nenhuma assinatura de apresentadores para provar sua validade. PGP sabe quais são suas chaves públicas, procurando pelas chaves privadas correspondentes no chaveiro privado. PGP também assume que você confia completamente em você mesmo para certificar outras chaves.

À medida que o tempo passa, você acumulará chaves de outras pessoas que talvez possa querer designar como apresentadores confiáveis. Todos os outros escolherão seus próprios apresentadores confiáveis. E todo mundo irá gradualmente acumular e distribuir com suas chaves uma coleção de assinaturas de certificação de outras pessoas, com a esperança de que alguém que a receba irá confiar em pelo menos uma ou duas das assinaturas. Isto

causará a emergência de uma rede de confiança descentralizada e tolerante a erros para todas as chaves públicas.

Esta atitude popular única contrasta fortemente com os esquemas padrão de gestão de chaves desenvolvido pelo governo e outras instituições monolíticas, como o Internet Privacy Enhanced Mail (PEM), que são baseados num controle centralizado e num sistema de confiança centralizado mandatório. Os esquemas padrões baseiam-se numa hierarquia de Autoridades de Certificação que ditam em quem você deve confiar. O método descentralizado probabilístico do programa para determinar a legitimidade de chaves públicas é o ponto chave da sua arquitetura do gerenciamento de chaves. PGP permite que você apenas decida em quem confiar, colocando você no topo de sua própria pirâmide de certificação privada. PGP é para as pessoas que preferem elas mesmas embalam seus próprios pára-quadras.

Note que enquanto essa atitude descentralizada e popular é enfatizada aqui, isto não significa que PGP não funcione igualmente bem em esquemas de gerenciamento de chaves públicas mais hierárquicos e centralizados. Usuários de grandes corporações, por exemplo, vão provavelmente querer uma figura ou pessoa central que assine todas as chaves de seus funcionários. PGP manipula este cenário centralizado como um caso especialmente degenerado do modelo de confiança mais generalizado de PGP.

Como proteger suas chaves privadas de serem descobertas

Proteja sua própria chave pública e sua frase-senha com muito cuidado. Se a sua chave privada for comprometida, é melhor que você avise o mais rápido possível todas as partes interessadas antes que alguém a use para fazer assinaturas em seu nome. Por exemplo, alguém poderia utilizá-la para assinar certificados de chave pública falsos, o que poderia criar problemas para muitas pessoas, especialmente se a sua assinatura é largamente confiada. E é claro, o comprometimento de sua própria chave pública poderia revelar todas as mensagens que lhe foram enviadas.

Para proteger a sua chave secreta, você pode começar por manter sempre um controle físico sobre ela. Guardá-la em seu computador pessoal em casa está OK, ou mantê-la em seu computador “notebook” que transporta consigo. Se você precisar usar um computador num escritório no qual você não tem sempre um controle físico, guarde suas chaves públicas e privadas em um disquete removível protegido contra gravação, e não o deixe para trás quando deixar o escritório. Não seria boa idéia deixar sua chave privada residir em um computador remoto com compartilhamento de tempo, como um sistema remoto UNIX por discagem. Alguém poderia espionar sua linha do modem e capturar sua frase-senha, e então obter sua chave privada a partir do sistema remoto. Você deve usar sua chave privada apenas em uma máquina que está sob seu controle físico.

Não armazene sua frase-senha em qualquer lugar no computador que tem o arquivo de sua chave privada. Armazenar tanto a chave privada e a frase-senha no mesmo computador é tão perigoso quanto guardar seu código pessoal na mesma carteira onde está seu cartão de crédito. Você não irá querer que alguém ponha suas mãos no seu disco que contém tanto a sua frase-senha e o arquivo da chave privada. Seria mais seguro se você simplesmente

memorizasse sua frase-senha e a guardasse somente no seu cérebro. Se você acha que deve escrever sua frase-senha, guarde-a bem protegida, talvez ainda mais bem protegida que o arquivo com sua chave privada.

Guarde cópias *backup* de sua chave privada — lembre-se, você possui a única cópia de sua chave privada, e perdê-la tornará inutilizável todas as cópias de sua chave pública que você espalhou pelo mundo.

A maneira descentralizada e não-institucional que PGP suporta para gerenciamento de chaves públicas tem seus benefícios, mas infelizmente isso também quer dizer que você não pode contar com uma única lista centralizada de quais chaves foram comprometidas. Isto torna um pouco mais difícil conter os danos do comprometimento de uma chave privada. Você simplesmente deve espalhar a notícia e esperar que todos a ouçam.

Se o pior caso acontecer — sua chave privada e sua frase-senha estarem comprometidas (esperando que você descobriu isso de alguma forma) — você precisará emitir um certificado de “revogação de chave”. Este tipo de certificado é utilizado para avisar às outras pessoas que parem de utilizar sua chave pública. Você pode usar PGP para criar tal certificado, usando o comando “Revoke” (Revogar) do menu de PGPkeys ou pedindo seu “Revogador Designado” para fazê-lo por você. Então você deve enviar este certificado para um servidor de certificados, de forma que outros possam achá-lo. O próprio PGP destas pessoas instala este certificado de chave revogada em seus chaveiros públicos, e automaticamente evita que eles acidentalmente utilizem sua chave pública novamente. Você pode então gerar um novo par de chaves privada/pública e publicar sua nova chave pública. Você poderia enviar um “pacote” contendo tanto sua nova chave pública quanto seu certificado de revogação de chave para sua chave antiga.

E se você perder sua chave privada?

Normalmente, se você quisesse revogar sua própria chave privada, você poderia usar o comando “Revoke” (Revogar) no menu de PGPkeys para emitir um certificado de revogação, assinado com sua própria chave privada.

Mas o que aconteceria se você perdesse sua chave privada, ou sua chave privada fosse destruída? Você não pode revogá-la você mesmo, porque você deve usar sua própria chave privada para revogá-la, e você não a tem mais. Se você não possui um revogador designado para sua chave, alguém especificado em PGP que pode revogar sua chave sob seu nome, você deverá pedir a cada pessoa que assinou sua chave para retirar sua certificação. Então qualquer um que tente usar sua chave baseado na confiança de um de seus apresentadores saberá que não deve confiar em sua chave pública.

Para maiores informações sobre revogadores designados, veja a seção [“Para apontar um revogador designado”](#) no [Capítulo 6](#).

Cuidado com veneno de cobra

Quando se examina um pacote de software criptográfico, fica sempre a dúvida, por que você deveria confiar neste produto? Mesmo que você examinasse o código fonte você mesmo, nem todo mundo tem experiência criptográfica para julgar a segurança. Mesmo se você for um criptógrafo experiente, falhas imperceptíveis nos algoritmos ainda poderiam enganá-lo.

Quando eu estava na faculdade no início dos anos 70, eu planejei o que acreditava ser um brilhante esquema de codificação. Uma simples cadeia de números pseudo-aleatórios era acrescentada a uma cadeia de texto puro para criar um texto cifrado. Isto aparentemente impediria qualquer análise de frequência do texto cifrado, e seria inquebrável até mesmo para as melhores agências de inteligência do governo. Senti-me muito satisfeito com minha façanha.

Anos mais tarde, descobri este mesmo esquema em diversos textos introdutórios de criptografia e trabalhos educacionais. Que legal. Outros criptógrafos pensaram no mesmo esquema. Infelizmente, o esquema era apresentado como uma simples atribuição de dever de casa sobre como usar técnicas criptoanalíticas elementares para trivialmente quebrá-la. Tão pouco para meu esquema brilhante.

Desta humilde experiência aprendi como é fácil cair num falso senso de segurança quando se planeja um algoritmo de codificação. A maioria das pessoas não percebe como é terrivelmente complicado planejar um algoritmo de codificação que consiga resistir a um ataque prolongado e determinado de um oponente com recursos. Muitos engenheiros de software conceituados desenvolvem esquemas igualmente simples de codificação (muitas vezes até os mesmos esquemas de codificação) e alguns destes foram incorporados a pacotes comerciais de software de codificação e vendidos por um bom dinheiro para milhares de usuários inocentes.

Isto é como vender cinto de segurança para automóveis que parecem bons e ajustam-se bem, mas abrem com um estalo no mais lento teste de colisão. Dependendo dele pode ser pior que não usar nenhum cinto. Ninguém suspeita que são ruins até acontecer uma batida real. E depender de softwares de criptografia fraca pode fazer você colocar em risco informações confidenciais sem saber, o que por outro lado poderia até não acontecer se você não tivesse um software criptográfico. Talvez você nunca nem descobriria que seus dados foram comprometidos.

Algumas vezes pacotes comerciais utilizam o “Federal Data Encryption Standard” (DES, ou Padrão Federal de Criptografia de Dados), que é um bom algoritmo convencional recomendado pelo governo para uso comercial (mas não para informações confidenciais, por estranho que pareça — Hmmm). Existe vários “modos de operação” que DES pode utilizar, alguns deles melhores do que outros. O governo especificamente recomenda não usar o modo mais fraco e simples nas mensagens, o modo “Eletronic Codebook” (ECB). Mas recomendam os modos mais fortes e mais complexos, tais como “Cipher Feedback” (CFB) e “Cipher Block Chaining” (CBC).

Infelizmente, a maioria dos pacotes comerciais de codificação que observei usam o modo ECB. Quando conversei com os autores de algumas dessas implementações, eles disseram que nunca tinham ouvido falar dos modos CBC ou CFB, e não sabiam de nada sobre as fraquezas do modo ECB. O fato de que eles não sequer aprenderam criptografia o suficiente para conhecer estes conceitos elementares não é tranquilizador. E eles às vezes gerenciam suas chaves DES de forma inapropriada ou insegura. Também, estes mesmos pacotes de software muitas vezes incluem um segundo algoritmo de criptografia, mais rápido, para ser usado no lugar do lento DES. O autor do pacote geralmente acha que seu algoritmo proprietário mais rápido é tão seguro quanto DES, mas depois de questioná-lo geralmente descubro que é apenas uma variação do meu próprio esquema brilhante da época da faculdade. Ou talvez ele até não revelaria como seu esquema de criptografia proprietário funciona, mas me asseguram que é um esquema brilhante e que eu deveria acreditar nele. Eu tenho certeza de que ele acredita que seu algoritmo é brilhante, mas como posso saber disto sem vê-lo?

Honestamente, devo destacar que na maioria dos casos estes produtos terrivelmente fracos não vêm de companhias que se especializam na tecnologia criptográfica.

Mesmo os pacotes de software realmente bons, que utilizam DES nos modos corretos de operação, ainda possuem problemas. DES padrão usa uma chave de 56 bits, que é muito pequena para os padrões de hoje, e já podem ser facilmente quebradas através de procuras exaustivas de chaves em máquinas especiais de alta velocidade. O DES chegou ao fim de sua vida útil, como também qualquer pacote de software que se baseie nele.

Existe uma companhia chamada AccessData (<http://www.accessdata.com>) que vende um pacote de preço muito baixo que quebra os esquemas internos de criptografia usados pelo WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word e PKZIP. Ele não faz simples adivinhações de senhas — faz verdadeiras criptoanálises. Algumas pessoas o compram quando se esquecem de suas senhas para seus próprios arquivos. Agências para cumprimento da lei também o compram, assim podem ler os arquivos que conseguirem capturar. Conversei com Eric Thompson, o autor, e ele disse que seu programa leva apenas uma fração de segundo para quebrá-las, mas ele inseriu alguns “loops” de espera para torná-lo mais lento de modo que não pareça tão fácil para o cliente.

Na arena da telefonia segura, suas chances parecem desanimadoras. O concorrente líder é o STU-III (de “Secure Telephone Unit”, ou Unidade de Telefone Seguro), feito pela Motorola e AT&T por US\$2,000 a US\$3,000, e usado pelo governo para aplicações confidenciais. Ele possui criptografia forte, mas requer algum tipo de licença especial do governo para comprar a versão forte. Uma versão comercial do STU-III está disponível, mas enfraquecida para conveniência da NSA, e uma versão para exportação está disponível mas ainda mais severamente enfraquecida. Então houve o AT&T Surity 3600, de US\$1,200, que usa o famoso chip “Clipper” do governo para codificação, com as chaves em juízo para o governo para conveniência dos monitores de chamadas. Então, é claro, houve os misturadores de vozes analógicos (não digitais), que você pode comprar em catálogos de “futuros espões”, que são brinquedos realmente inúteis ao tanto quanto a criptografia está envolvida, mas são vendidas como produtos “seguros” de comunicação para consumidores que não conhecem nada melhor.

De certa forma, criptografia é como farmacêutica. Sua integridade pode ser absolutamente crucial. Penicilina ruim se parece como penicilina boa. Você pode dizer se seu software de planilha estiver errado, mas como dizer se seu pacote de criptografia é fraco? O texto cifrado produzido por um algoritmo fraco de criptografia parece tão bom quanto o texto cifrado produzido por um forte algoritmo de criptografia. Há um bocado de veneno de cobra lá fora. Um bocado de curandeiros. Diferentemente dos vendedores ambulantes de remédios do passado, estes implementadores de software geralmente nem sabem que suas coisas são veneno de cobra. Podem ser bons engenheiros de software, mas geralmente nunca leram nada da literatura acadêmica sobre criptografia. Mas acham que podem escrever bons softwares criptográficos. E por que não? No fim das contas, parece intuitivamente fácil escrever um. E seus softwares parecem funcionar bem.

Qualquer um que pensa que planejou um esquema de codificação inquebrável ou é um gênio incredivelmente raro ou é ingênuo e inexperiente. Infelizmente, eu às vezes tenho que lidar com “aprendizes de criptógrafos” que gostariam de fazer “melhorias” em PGP adicionando algoritmos de codificação que eles próprios projetaram.

Lembro-me de uma conversa com Brian Snow, um criptógrafo veterano com influência na NSA. Ele disse que nunca confiaria num algoritmo de codificação planejado por alguém que não tivesse “ganhado seus ossos” primeiramente gastando muito tempo quebrando códigos. Isto fez muito sentido. Observei que praticamente ninguém no mundo comercial de criptografia se qualificava sob este critério. “Sim”, ele disse com um sorriso confiante, “e isto torna nosso trabalho na NSA bem mais fácil”. Um pensamento desanimador. Eu também não me qualificaria.

O governo também vendeu veneno de cobra. Depois da Segunda Guerra Mundial, os Estados Unidos venderam máquinas alemãs de codificação “Enigma” para governos do terceiro mundo. Mas não disseram que os aliados quebraram o código Enigma durante a guerra, um fato que permaneceu confidencial por muitos anos. Mesmo hoje muitos sistemas UNIX em todo o mundo usam a cifra Enigma para codificação de arquivos, em parte porque o governo criou obstáculos legais contra o uso de algoritmos melhores. Eles até tentaram proibir a publicação inicial do algoritmo RSA em 1977. E eles por muitos anos esmagaram essencialmente todos os esforços comerciais para desenvolver telefones efetivamente seguros para o público em geral.

O principal trabalho da agência de segurança nacional (“National Security Agency”, NSA) do governo americano é agrupar inteligência, principalmente grampeando as comunicações particulares das pessoas (veja o livro de James Bamford, “The Puzzle Palace”). A NSA acumulou considerável habilidade e recursos na quebra de códigos. Quando as pessoas não possuem uma boa criptografia para se protegerem, isto torna o trabalho da NSA bem mais fácil. NSA também tem a responsabilidade de aprovar e recomendar algoritmos de codificação. Alguns críticos afirmam que isto é um conflito de interesses, como colocar a raposa para tomar conta do galinheiro. Nos anos 80, NSA colocou no mercado um algoritmo de criptografia convencional que planejou (o COMSEC Endorsement Program) e nunca revelou a ninguém como funciona porque é considerado confidencial. Ela queria que outros confiassem nele e o usassem. Mas qualquer criptógrafo pode lhe dizer que um algoritmo de criptografia bem planejado não precisa ser confidencial para permanecer seguro. Somente as chaves precisariam de proteção. Como alguém poderia realmente saber se o algoritmo confidencial da RSA é seguro? Não é tão

difícil para a NSA projetar um algoritmo de criptografia que somente eles poderiam quebrar, se ninguém mais pode revisar o algoritmo.

Há três fatores principais que têm minado a qualidade do software comercial de criptografia nos Estados Unidos.

- O primeiro é a virtualmente universal falta de competência dos implementadores de software comerciais de codificação (apesar disto estar começando a mudar desde a publicação de PGP). Cada engenheiro de software imagina-se um criptógrafo, o que causou a proliferação de softwares de criptografia realmente ruins.
- O segundo é a NSA deliberadamente e sistematicamente suprimir toda a boa tecnologia comercial de criptografia, através de intimidação legal e pressão econômica. Parte desta pressão é sustentada por rigorosos controles de exportação em softwares de codificação que, pela economia do mercado de software, possui o efeito colateral de suprimir softwares domésticos de codificação.
- O terceiro método principal de supressão vem de garantir todas as patentes de software para todos os algoritmos de codificação por chave pública para uma única companhia, proporcionando um único ponto de estrangulamento para suprimir a difusão desta tecnologia (apesar do cartel de patentes de criptografia ter sido quebrado no outono de 1995).

O efeito colateral de tudo isso é que antes de PGP ser publicado, não havia praticamente nenhum software de codificação de alta segurança para propósitos gerais disponível nos Estados Unidos.

Não estou tão certo da segurança do PGP como certa vez estive com meu brilhante software de criptografia da faculdade. Se estivesse, seria um mau sinal. Mas eu não acho que PGP contenha alguma fraqueza evidente (apesar de estar bem certo de que ele contém *bugs*). Eu selecionei os melhores algoritmos da literatura publicada da academia criptográfica civil. Na maior parte, estes algoritmos foram individualmente submetidos à extensas revisões. Conheço muitos dos melhores criptógrafos do mundo, e tenho discutido com alguns deles vários dos protocolos e algoritmos de criptografia usados em PGP. Ele está bem pesquisado, e levou anos para ser feito. E eu não trabalho para a NSA. Mas você não precisa acreditar na minha palavra sobre a integridade criptográfica de PGP, porque o código fonte está disponível para facilitar revisões.

Mais um ponto sobre meu compromisso com a qualidade criptográfica em PGP: desde que comecei a desenvolver e lancei PGP gratuitamente em 1991, eu fiquei três anos sob investigação criminal pelas Alfândegas dos EUA devido à difusão de PGP pelo mundo, com risco de acusação criminal e anos de prisão. Por falar nisso, você não viu o governo se preocupar com outros softwares criptográficos — é PGP que eles atacam. O que isto diz a você sobre a força de PGP? Eu ganhei minha reputação de integridade com a integridade criptográfica de meus produtos. Eu não vou trair meu compromisso com nosso direito de privacidade, pelo qual eu arrisquei minha liberdade. Eu não vou permitir que um produto que leve meu nome possua quaisquer “backdoors” secretos.

Vulnerabilidades

“Se todos os computadores pessoais no mundo — 260 milhões — fossem colocados para trabalhar em uma única mensagem codificada por PGP, ainda levaria um tempo estimado de 12 milhões de vezes a idade do universo, em média, para quebrar uma única mensagem”.

— William Crowell, Diretor Adjunto, Agência de Segurança Nacional (“National Security Agency”, NSA), 20 de março de 1997.

Nenhum sistema de segurança é impenetrável. PGP pode ser enganado de várias formas diferentes. Em qualquer sistema de segurança, você precisa se perguntar se a informação que tenta proteger é mais valiosa para o atacante que o custo do ataque. Isto deveria levá-lo a se proteger de ataques de baixo custo, sem se preocupar com ataques mais caros.

Um pouco da discussão que segue pode parecer um tanto ou quanto paranóica, mas tal atitude é apropriada para uma discussão razoável sobre quesitos de vulnerabilidade.

Comprometimento da frase-senha e chave privada

Provavelmente a forma mais simples de ataque é feita se você deixar a frase-senha para sua chave privada escrita em algum lugar. Se alguém a achar e também conseguir seu arquivo de chave privada, ele pode ler suas mensagens e fazer assinaturas em seu nome.

Aqui estão algumas recomendações para proteger sua frase-senha:

1. Não use frases-senhais óbvias que possam ser facilmente descobertas, como os nomes de seus filhos ou esposa(o).
2. Use espaços e uma combinação de números e letras em sua frase-senha. Se você fizer de sua frase-senha uma única palavra, ela poderá ser descoberta fazendo um computador tentar todas as palavras do dicionário até encontrar sua senha. É por isso que uma frase-senha é melhor do que uma senha simples. Um atacante mais sofisticado poderia fazer seu computador pesquisar um livro com frases famosas para tentar achar sua frase-senha.
3. Seja criativo. Use uma frase-senha fácil de lembrar e difícil de se descobrir; você poderia facilmente construir uma usando alguns dizeres criativos sem sentido ou citações literárias obscuras.

Falsificação da chave pública

Uma maior vulnerabilidade existe se chaves públicas são falsificadas. Esta deve ser a vulnerabilidade mais crucialmente importante em um criptosistema de chave pública, em parte porque a maioria dos novatos não a percebem imediatamente.

Para resumir: quando você usar a chave pública de alguém, esteja certo de que não foi falsificada. Uma nova chave pública de alguém deve ser confiada apenas se você a obtiver diretamente de seu proprietário, ou se ela foi assinada por alguém em quem você confia. Certifique-se de que ninguém irá falsificar sua própria chave pública. Mantenha controle físico de seu chaveiro público e sua chave privada, preferivelmente em seu computador pessoal ao invés de um sistema remoto de compartilhamento de tempo. Tenha sempre uma cópia *backup* de ambos os chaveiros.

Arquivos não apagados completamente do disco

Outro problema potencial é causado pelo modo que a maioria dos sistemas operacionais apaga arquivos. Quando você codifica um arquivo e apaga o texto puro original, na verdade o sistema operacional não apaga fisicamente os dados. Ele simplesmente marca aqueles blocos de disco como apagados, permitindo que o espaço seja reutilizado posteriormente. É como jogar documentos sensíveis em papel para uma lixeira reciclável ao invés de um destruidor de papéis. Os blocos do disco ainda contêm o texto original sensível que você queria destruir, e serão provavelmente sobrescritos por novos dados em algum ponto no futuro. Se o atacante ler estes blocos de disco apagados logo que eles forem desalojados, ele poderia recuperar seu texto original.

De fato isto poderia até acontecer acidentalmente, se algo der errado com o disco e alguns arquivos foram acidentalmente apagados ou corrompidos. Um programa de recuperação de discos pode ser utilizado para recuperar os arquivos danificados, mas isto geralmente significa que alguns arquivos apagados sejam ressuscitados juntos com tudo mais. Seus arquivos confidenciais que você pensou terem sumido para sempre poderiam então reaparecer e serem inspecionados por qualquer um que estiver tentando recuperar seu disco danificado. Mesmo enquanto você está criando a mensagem original com um processador ou editor de textos, o editor pode estar criando várias cópias temporárias do seu texto no disco, simplesmente por causa de seus trabalhos internos. Estas cópias temporárias de seu texto são apagadas pelo processador de textos quando ele tiver terminado, mas estes fragmentos sensíveis ainda estarão em seu disco em algum lugar.

A única forma de se prevenir que o texto puro de reaparecer é de alguma forma fazer com que os arquivos de texto puro apagados sejam sobrescritos. A não ser que você tenha certeza de que todos os blocos apagados do disco serão brevemente reutilizados, você deve tomar providências para sobrescrever o arquivo, e também quaisquer fragmentos dele no disco deixado por seu processador de textos. Você pode cuidar de quaisquer fragmentos do texto deixado no disco usando os recursos de Eliminação Segura (“Secure Wipe”) e Eliminação de Espaço Livre (“Freespace Wipe”) de PGP.

Viroses e Cavalos de Tróia

Outro ataque poderia envolver um vírus ou “verme” hostil para computadores especialmente criado que poderia infectar PGP ou seu sistema operacional. Este vírus hipotético poderia ser projetado para capturar sua frase-senha ou chave privada ou decifrar mensagens e para invisivelmente escrever as informações capturadas em um arquivo ou enviá-los através de uma rede para o dono do vírus. Ou ele poderia alterar o comportamento de PGP de forma que as assinaturas não sejam checadas corretamente, por exemplo. Este ataque é mais barato que ataques criptoanalíticos.

A defesa para este tipo de ataque cai na categoria de defesa contra infecções de viroses em geral. Há alguns produtos antivírus moderadamente capazes comercialmente disponíveis, e há procedimentos higiênicos a serem seguidos que podem grandemente reduzir as chances de uma infecção viral. Um tratamento completo de contramedidas antivírus e antivermes está além do escopo deste documento. PGP não tem defesas contra vírus, e assume que seu próprio computador pessoal é um ambiente confiável de execução. Se tal tipo de vírus ou verme realmente aparecer, espera-se que todos logo tomemos conhecimento.

Um ataque similar envolve alguém criando uma inteligente imitação de PGP que se comporta como PGP na maioria dos aspectos, mas não funcionando da forma esperada. Por exemplo, ele poderia ser deliberadamente avariado para não verificar assinaturas corretamente, permitindo que certificados de chaves falsas fossem aceitas. Esta versão cavalo de tróia de PGP não é difícil de ser criada por um atacante, porque o código fonte de PGP está amplamente disponível, portanto qualquer um poderia modificar o código fonte e produzir uma imitação lobotomizada zumbi de PGP que pareceria real, mas faz os desejos de seu mestre diabólico. Esta versão cavalo de tróia de PGP poderia então ser amplamente distribuída, dizendo-se ser de uma fonte legítima. Que traiçoeiro.

Você deve fazer um esforço para obter sua cópia de PGP diretamente da Network Associates, Inc.

Há outras formas de checar PGP por falsificações, usando assinaturas digitais. Você poderia usar outra versão confiável de PGP para checar a assinatura de uma versão suspeita de PGP. Mas isto não ajudaria se seu sistema operacional estiver infectado, já que não detectaria se sua cópia original de `pgp.exe` foi maliciosamente alterada de tal forma a comprometer sua própria habilidade de checar assinaturas. Este teste também assume que você possui uma boa cópia confiável da chave pública que você usa para checar a assinatura no executável de PGP.

Arquivos de troca ou memória virtual

PGP foi originalmente desenvolvido para MS-DOS, um sistema operacional primitivo para os padrões de hoje. Mas quando foi portado para outros sistemas operacionais mais complexos, como Microsoft Windows e Macintosh OS, uma nova vulnerabilidade emergiu. Esta vulnerabilidade provém do fato de que estes sistemas operacionais modernos usam uma técnica chamada *memória virtual*.

Memória virtual permite que você execute programas enormes em seu computador que são maiores que o espaço disponível nos chips de memória de semicondutores em seu computador. Isto é útil porque software tem se tornado mais e mais “gordo” desde que interfaces gráficas com o usuário tornaram-se norma e usuários começaram a executar diversos programas grandes ao mesmo tempo. O sistema operacional usa o disco rígido para armazenar porções de seu software que não estão sendo usadas em determinado momento. Isto significa que o sistema operacional pode, sem seu conhecimento, escrever no disco algumas coisas que você pensou que eram mantidas apenas na memória principal — coisas como chaves, frases-senhas, e textos decifrados. PGP não mantém este tipo de dados sensíveis em algum lugar na memória além do necessário, mas há alguma chance de que o sistema operacional poderia escrevê-los em disco de qualquer forma.

Os dados são escritos em uma área de “notas” no disco, conhecido como um *arquivo de troca*. Dados são lidos de volta a partir do arquivo de troca quando necessário, de forma que apenas parte de seu programa ou dados estarão na memória física por vez. Toda esta atividade é invisível para o usuário, que simplesmente vê o disco trepidando. Microsoft Windows faz trocas de pedaços de memória, chamadas “páginas”, usando um algoritmo de troca de páginas do tipo Último Recentemente Usado, ou “Least Recently Used” (LRU). Isto significa que páginas que não foram acessadas pelos períodos de tempo mais longos são as primeiras a serem colocadas no disco. Este caminho sugere que na maioria dos casos o risco é bem baixo que dados sensíveis serão colocados no disco, já que PGP não os deixa na memória por muito tempo. Mas não damos nenhuma garantia.

Este arquivo de troca pode ser acessado por qualquer um que tiver acesso físico à seu computador. Se você estiver preocupado com este problema, você talvez possa resolvê-lo obtendo algum software especial que sobrescreva seu arquivo de troca. Outra cura possível é desligar o recurso de memória virtual de seu sistema operacional. Microsoft Windows permite isto, e também Mac OS. Desligar a memória virtual pode significar que você precisará ter mais chips físicos de memória RAM instalados de forma a fazer com que tudo caiba na RAM.

Falha de segurança física

Uma falha de segurança física poderia permitir a alguém fisicamente obter seus arquivos de texto ou mensagens impressas. Um oponente determinado poderia obter isto através de roubo, vasculhando lixo, procura e captura sem motivo, ou suborno, chantagem ou infiltração entre seu quadro de funcionários. Alguns desses ataques podem ser especialmente praticáveis contra organizações políticas populares que dependem de um quadro de funcionários largamente formado por voluntários.

Não se iluda em uma falsa sensação de segurança só porque você tem uma ferramenta de criptografia. Técnicas criptográficas protegem dados apenas quando elas estão codificadas — violações diretas de segurança física ainda podem comprometer dados em textos ou informações escritas ou faladas.

Este tipo de ataque é mais barato que ataques criptoanalíticos em PGP.

Ataques “Tempest”

Outro tipo de ataque que tem sido utilizado por oponentes bem equipados envolve a detecção remota dos sinais eletromagnéticos vindos de seu computador. Este ataque caro e um tanto trabalhoso é provavelmente ainda mais barato que ataques criptoanalíticos diretos. Um caminhão ou van apropriadamente suprido das máquinas necessárias pode estacionar próximo ao seu escritório e remotamente capturar todos os seus toques no teclado e mensagens mostradas na tela de vídeo de seu computador. Isto iria comprometer todas as suas senhas, mensagens etc. Este ataque poderia ser evitado através de blindagens apropriadas em todos os seus equipamentos para computador e cabos de rede, de forma a não emitir estes sinais. Esta tecnologia de blindagem, conhecida como “Tempest”, é usado por algumas agências governamentais e fornecedores de defesas. Há fabricantes de hardware que fornecem blindagens Tempest comercialmente.

Algumas novas versões de PGP (após a versão 6.0) podem exibir textos decifrados usando uma fonte especialmente projetada que pode possuir níveis reduzidos de emissão de frequências de rádio a partir da tela de vídeo de seu computador. Isto pode tornar mais difícil que sinais sejam remotamente detectados. Esta fonte especial está disponível em algumas versões de PGP que suportam o recurso Visualizador Seguro (“Secure Viewer”).

Protegendo-se contra marcas de hora falsas

Uma vulnerabilidade um tanto obscura de PGP envolve usuários desonestos criarem marcas de horas (“timestamps”) falsas em seus certificados e assinaturas de chaves públicas. Você pode saltar esta seção se é um usuário casual e não quer se aprofundar em obscuros protocolos de chaves públicas.

Não há nada que impeça um usuário desonesto de alterar a configuração de data e hora do relógio de seu próprio sistema, e gerar seus próprios certificados de chave pública e assinaturas que parecem ter sido criadas em uma hora diferente. Ele pode fazer parecer que ele assinou algo mais cedo ou tarde do que realmente fez, ou que seu par de chaves público/privado foi criado mais cedo ou mais tarde. Isto pode dar algum benefício legal ou financeiro a ele, por exemplo, criando algum tipo de evasiva que poderia permitir que ele rejeitasse uma assinatura.

Creio que este problema de marcas de hora falsificadas em assinaturas digitais não é pior do que já é em assinaturas feitas à mão. Qualquer um pode escrever qualquer data perto de sua assinatura escrita em um contrato, mas ninguém parece estar alarmado sobre este acontecimento. Em alguns casos, uma data “incorreta” em uma assinatura feita à mão pode não estar associada com fraudes reais. A marca de hora também pode ser quando o assinante afirma que ele assinou um documento, ou talvez quando ele deseja que sua assinatura entre em efeito.

Em situações onde é crítico confiar em uma assinatura com a data atual correta, as pessoas podem simplesmente usar tabeliãs para testemunhar e datar uma assinatura feita à mão. O análogo a isto em assinaturas digitais é obter uma terceira pessoa confiável para assinar um certificado de assinatura, aplicando uma marca de hora confiável. Nenhum protocolo

exótico ou muito formal é necessário para isso. Assinaturas testemunhadas têm sido por muito tempo reconhecidas como uma forma legítima de determinar quando um documento foi assinado.

Uma Autoridade de Certificação digna de confiança ou tabelião poderia criar assinaturas autenticadas com uma marca de hora digna de confiança. Isto não necessariamente iria requerer uma autoridade centralizada. Talvez qualquer apresentador confiável ou parte desinteressada poderia exercer esta função, da mesma forma que tabeliães públicos reais fazem hoje. Quando um tabelião assina a assinatura de outras pessoas, ele cria um certificado de assinatura de um certificado de assinatura. Isto serviria como um testemunho para a assinatura da mesma forma que tabeliães reais hoje testemunham assinaturas feitas à mão. O tabelião poderia inserir o certificado de assinatura separado (sem todo o documento que foi assinado) em um registro especial controlado pelo tabelião. Qualquer um poderia ler este registro. A assinatura do tabelião teria uma marca de hora confiável, que poderia ter maior credibilidade ou significado legal maior que a marca de hora na assinatura original.

Há um bom tratamento sobre este tópico no artigo de Denning feito em 1983 para a “IEEE Computer”. Futuras melhorias em PGP poderiam ter recursos para facilmente gerenciar assinaturas reconhecidas de assinaturas, com marcas de hora confiáveis.

Exposição em sistemas multiusuário

PGP foi originalmente projetado para um PC monousuário sob seu controle físico direto. Se você executa PGP em casa ou em seu próprio PC, seus arquivos codificados geralmente estão seguros, a não ser que alguém invada sua casa, roube seu PC e o convença a lhes dar sua frase-senha (ou sua frase-senha é simples o suficiente para ser descoberta).

PGP não foi projetado para proteger seus dados enquanto eles estão em formato de texto em um sistema comprometido. Nem pode prevenir que um invasor use medidas sofisticadas para ler sua chave privada enquanto ela está sendo usada. Você simplesmente deverá reconhecer estes riscos em sistemas multiusuários, e ajustar suas expectativas e comportamento de acordo. Talvez sua situação seja tal que você deve considerar executar PGP apenas em um sistema isolado e monousuário sob seu controle físico direto.

Análise de tráfico

Mesmo se um atacante não puder ler o conteúdo de suas mensagens codificadas, ele poderia deduzir ao menos algumas informações úteis observando de onde as mensagens vêm e para onde elas vão, o tamanho das mensagens, e a hora do dia que são enviadas. Isto é análogo ao atacante olhar para sua conta telefônica de longa distância para ver para quem você ligou e quando e por quanto tempo, mesmo que o conteúdo atual de suas conversas seja desconhecido para o atacante. Isto é chamado de análise de tráfico. PGP por si só não protege contra análise de tráfico. A solução deste tipo de problema requer protocolos de comunicação especializados, projetados para reduzir a exposição à análise

de tráfico em seu ambiente de comunicação, possivelmente com alguma assistência criptográfica.

Criptoanálise

Um ataque criptoanalítico caro e formidável poderia possivelmente ser montado por alguém com vastos recursos de supercomputadores, como uma agência governamental de inteligência. Eles poderiam quebrar sua chave pública usando algum novo método secreto de quebra de defesas. Mas a academia civil tem intensivamente atacado a criptografia por chave pública sem sucesso desde 1978.

Talvez o governo possua algum método confidencial para quebrar os algoritmos de criptografia convencional utilizados em PGP. Isto é o pior pesadelo de qualquer criptógrafo. Não pode haver nenhuma garantia absoluta de segurança em implementações criptográficas práticas.

Entretanto, algum otimismo parece justificável. Os algoritmos de chave pública, algoritmos de sumário da mensagem, e cifras de bloco usados em PGP foram projetados por alguns dos melhores criptógrafos no mundo. Os algoritmos de PGP têm sido extensivamente analisados quanto à segurança e revisados por alguns dos melhores criptoanalistas no mundo.

Além disso, mesmo se as cifras de blocos usadas em PGP possuírem alguma pequena fraqueza desconhecida, PGP comprime o texto puro antes de codificá-lo, o que deve grandemente reduzir essas fraquezas. O gasto computacional para quebrá-lo seria provavelmente muito mais caro que o valor da mensagem.

Se sua situação justificar a preocupação com ataques muito formidáveis deste calibre, então talvez você deveria contactar uma consultoria de segurança de dados para algumas direções sob medida para segurança de dados, específicas para suas necessidades em particular.

Em resumo, sem boa proteção criptográfica de sua comunicação de dados, pode ser praticamente sem esforço e talvez mesmo rotineiro para um oponente interceptar suas mensagens, especialmente aquelas enviadas através de um modem ou sistema de email. Se você usa PGP e segue precauções razoáveis, o atacante terá que gastar muito mais esforços e dinheiro para violar sua privacidade.

Se você se proteger contra os ataques mais simples, e se sente seguro de que sua privacidade não será violada por um atacante determinado e com muitos recursos, então você provavelmente estará seguro usando PGP. PGP lhe dá uma privacidade muito boa (no original, “PGP gives you Pretty Good Privacy”).

Glossário

apresentador	Uma pessoa ou organização a quem é permitido certificar a autenticidade da chave pública de alguém. Você designa um apresentador assinado a chave pública deste.
apresentador confiável	Alguém que você confia para lhe prover com chaves que são válidas. Quando um apresentador confiável assina a chave de outra pessoa, você acredita que as chaves dela são válidas, e você não precisa verificar suas chaves antes de usá-las.
assinar	Aplicar uma assinatura.
assinatura	Um código digital criado com uma chave privada. Assinaturas permitem autenticação das informações pelo processo de verificação de assinatura. Quando você assina uma mensagem ou arquivo, o programa PGP usa sua chave privada para criar um código digital que é único tanto para o conteúdo da mensagem quanto para sua chave privada. Qualquer um pode usar sua chave pública para verificar sua assinatura.
assinatura digital	veja “Assinatura”.
autenticação	A determinação da origem da informação codificada através da verificação da assinatura digital de alguém ou da chave pública de alguém, checando sua “impressão digital” única.
autoridade de certificação	Uma ou mais pessoas a quem é/são atribuída(s) a responsabilidade de certificar a origem de chaves e

adicioná-las a um banco de dados comum.

certificar

Assinar a chave pública de outra pessoa.

chave

Um código digital usado para codificar e assinar e decifrar e verificar mensagens e arquivos. Chaves vêm em pares de chave e são armazenadas em chaveiros.

chave privada

A parte secreta de um par de chaves, usada para assinar e decifrar informações. A chave privada de um usuário deve ser mantida secreta, conhecida apenas pelo usuário.

chave pública

Uma das duas chaves em um par de chaves, usada para codificar informações e verificar assinaturas. A chave pública de um usuário pode ser amplamente disseminada para colegas ou estranhos. Conhecer a chave pública de uma pessoa não ajuda ninguém a descobrir a chave privada correspondente.

chaveiro

Um conjunto de chaves. Cada usuário possui dois tipos de chaveiros: um chaveiro privado e um chaveiro público.

chaveiro privado

Um conjunto de uma ou mais chaves privadas, todas elas pertencendo ao proprietário do chaveiro privado.

chaveiro público

Um conjunto de chaves públicas. Seu chaveiro público inclui suas próprias chaves públicas.

codificação

Um método de misturar informação para torná-la ilegível para qualquer um exceto o destinatário intencionado, que deve decifrá-la para lê-la.

codificação convencional

Codificação que se baseia em uma frase-senha comum ao invés de criptografia por chave pública. O arquivo é

usando uma frase-senha que você deve escolher.

**Compartilhamento
Secreto**

Veja “Divisão de Chaves”.

confiável

Uma chave pública é dita confiável por você se ela foi certificada por você ou por alguém que você designou como um apresentador.

**criptografia por chave
pública**

Criptografia aonde um par de chaves público e privado é usado, e nenhuma segurança é necessária no canal em si.

decifração

Um método de reajuntar informação codificada de forma a torná-la legível novamente. A chave privada do destinatário é usada para decifração.

**Divisão de chaves ou
“compartilhamento
secreto”**

O processo de dividir uma chave privada em várias partes, e compartilhar estas partes entre um grupo de pessoas. Um número designado de pessoas deve trazer suas partes da chave e juntá-las para usar a chave.

frase-senha

Uma série de teclas pressionadas que permitem acesso exclusivo à sua chave privada, que você usa para assinar e decifrar mensagens de email e anexos de arquivo.

ID de chave

Um código legível que identifica unicamente um par de chaves. Dois pares de chave podem possuir o mesmo ID de usuário, mas terão diferentes IDs de chave.

ID de usuário

Uma frase de texto que identifica um par de chaves. Por exemplo, um formato comum para o ID de usuário é o nome do proprietário e seu endereço de email. O ID de usuário ajuda os usuários (tanto o dono quanto colegas) a identificar o proprietário do par de chaves.

impressão digital	Uma cadeia única de números e caracteres usada para autenticar chaves públicas. Esta é a forma primária de checar pela autenticidade de uma chave. Veja “impressão digital de uma chave”.
impressão digital de uma chave	Uma cadeia única de números e caracteres usados para autenticar chaves públicas. Por exemplo, você poderia telefonar para o proprietário de uma chave pública e pedir que ele ou ela lesse a impressão digital associada com sua chave, de forma que você pudesse compará-la com a impressão digital na sua cópia da chave pública dele para ver se ambos são iguais. Se a impressão digital não for igual, então você sabe que possui uma chave falsa.
juízo de chave	Uma prática onde um usuário de um sistema de criptografia por chave pública entrega sua chave privada à uma terceira pessoa, assim permitindo a ela monitorar comunicações codificadas.
meta-apresentador	Um apresentador confiável de apresentadores confiáveis.
par de chaves	Uma chave pública e sua chave privada complementar. Em sistemas de criptografia por chave pública, como o programa PGP, cada usuário possui ao menos um par de chaves.
rede de confiança	Um modelo de confiança distribuído usado por PGP para validar a propriedade de uma chave pública onde o nível de confiança é cumulativo, baseado no conhecimento dos indivíduos dos apresentadores.
subchave	Uma subchave é uma chave de codificação Diffie-Hellman que é adicionada como um subconjunto de sua chave mestra. Uma vez que uma subchave é criada, você pode expirar ou revogá-la sem afetar sua chave mestra ou as assinaturas colecionadas nela.

sumário da mensagem (“message digest”)	Um “destilado” compacto de sua mensagem ou checksum (método de checagem de erros) de um arquivo. Ele representa sua mensagem, onde se a mensagem for alterada de qualquer forma, um sumário da mensagem diferente seria computado dela.
texto	Um texto ASCII de 7 bits padrão, imprimível.
Texto ASCII-blindado (ASCII-armored text)	Informação binária que foi codificada usando um conjunto de caracteres ASCII de 7 bits, padrão, e imprimível, para conveniência em transportar a informação através de sistemas de comunicação. No programa PGP, arquivos texto ASCII-blindado possuem a extensão padrão de nome de arquivos, e são codificados e decodificados usando um formato ASCII radix-64.
texto cifrado (cyphertext)	Texto puro convertido em um formato secreto através do uso de um algoritmo de codificação. Uma chave de codificação pode destravar o texto puro a partir do texto cifrado.
texto puro	Texto normal, legível, não codificado e não assinado.
verificação	O ato de comparar uma assinatura criada com uma chave privada com sua chave pública. A verificação prova que a informação foi realmente enviada pelo assinante, e que a mensagem não foi posteriormente alterada por ninguém.