Como usar GPG

O software GPG (GNU's Privacy Guard) é, entre outras coisas, uma implementação do PGP (Pretty Good Privacy), que é um conjunto de especificações para comunicação encriptografada.

Instalando o GPGP

Se você está usando alguma distribuição Linux, BSD, Plan9, ou qualquer outro sistema operacional minimamente decente, é bem provável que o pacote `gnupg` está disponível no repositório de pacotes da sua distribuição. Portanto, basta instalar esse pacote usando seu gerenciador de pacotes. Caso você esteja usando aquelas distribuições sem gerenciadores de pacotes em que tudo deve ser instalado manualmente, então, você pode compilar o `gnupg` pelo código fonte.

Comandos básicos GPGP

Listar chaves disponíveis

Use o seguitne comando para listar as chaves disponíveis no seu computador

```
gpg --list-keys
```

Listar chaves segundo um padrão

Use o seguitne comando para para listar as chaves no seu computador segundo um padrão:

```
gpg --list-keys <pattern>
```

Por exemplo, para listar as chaves (armazenadas no computador) cujo nome do proprietário da chave ou email do proprietário contém o padrão Artix

```
gpg --list-keys Artix
```

Produz (no meu computador) a saída:

```
```

```
pub   rsa4096 2020-04-19 [SC] [expires: 2025-04-18]
      A574A1915CEDE31A3BFF5A68606520ACB886B428
uid           [ unknown] Christos Nouskas <nous@artixlinux.org>
```

Exportar sua chave pública para um arquivo

Use o seguinte comando para exportar sua chave pública para um arquivo:

```
gpg --export '<key>' > pubkey.gpg
```

Substitua `<key>` com o `id` da sua chave (pode ser o `Real name` associado com a chave, ou o `email` associado com a chave, ou o `id` da chave). Por exemplo:

```
gpg --export 'bruce@brucelee.com' > pubkey
```

Você pode querer exportar sua chave pública se você está distribuindo algum software (sua chave pode ser usada para verificar integridade e autenticidade do software) ou simplesmente para compartilhá-la com seus amigos para eles te enviarem mensagem encriptografadas.

Importar uma chave pública vinda de um arquivo

Use o seguinte comando para importar uma chave pública vinda de um arquivo:

```
gpg --import pubkey.gpg
```

Você pode querer importar a chave pública para verificar legitimidade de um software, ou importar a chave de seus amigos para enviar mensagem encriptografadas para eles.

Encriptografar um arquivo usando uma chave pública

Use um dos seguintes comandos (ambos são equivalentes) para encriptografar um arquivo usando uma chave pública:

```

```

```
gpg --encrypted --recipient '<key>' <file_path>
```

```
gpg -e -r '<key>' <file_path>
```

Por exemplo, para encriptografar um convite de festa que você enviará para o homem-aranha, use o comando:

```
gpg -e -r 'peterpark@spiderman.com' ~/documents/party-invitation.txt
```

Irá produzir o arquivo criptografado `party-invitation.txt.gpg`, que somente poderá ser decriptografado por quem deter a chave privada do homem-aranha.

Assinar um arquivo digitalmente

Use o seguinte comando para assinar um arquivo digitalmente:

```
gpg -b <file_path>
```

Isso irá gerar uma assinatura não-anexada, o que significa que o arquivo da assinatura está separado do arquivo original (a assinatura é um arquivo diferente).

Por padrão, o nome do arquivo da assinatura gerada será o nome do arquivo original concatenado com a string `.sig`.

Exemplo: Se o arquivo é `~/documents/letter.pdf`, a assinatura produzida estará localizada em `~/documents/letter.pdf.sig`.

É possível especificar o nome do arquivo gerado usando a flag `-o`, da seguinte forma:

```
gpg -b -o <output_file_path> <file_path>
```

Verificar a assinatura digital de um arquivo

Use o seguinte comando para verificar a assinatura digital de um arquivo:

```
gpg --verify <signature_file_path> <file_path>
```

Para isso funcionar, é necessário que você tenha, no seu computador, a chave pública usada para assinar o arquivo. Do contrário, não será possível verificar a assiantura digital.

A assiantura digital pode ser usada para verificar que um arquivo é legítimo, não foi corrompido, não foi alterado, e foi de fato assinado pelo dono da chave.

Exemplo: verificar a assinatura de um arquivo ISO:

```
gpg --verify manjaro-xfce-21.0.7-minimal-210614-linux510.iso.sig manjaro-xfce-21.0.7-minimal-210614-linux510.iso
```

Decriptografar um arquivo usando a chave privada

Somente é possível decriptografar um arquivo que foi encriptografado com a chave pública se você detiver a chave privada correspondente.

Use o seguinte comando para decriptografar um arquivo usando a chave privada:

```
gpg -d <file_path>
```

O conteúdo do arquivo será enviado para a saída padrão. Se você não deseja isso, redirecione a saída padrão para algum outro arquivo. Exemplo:

```
gpg -d mensagem.txt.gpg > mensagem.txt
```

Encriptografar um arquivo usando uma senha

Você pode encriptografar um arquivo usando uma senha, o que significa que você não precisa usar chave pública.

Use o seguinte comando para encriptografar um arquivo usando uma senha:

```
gpg -c <file_path>
```

Em seguida, você será perguntado para fornecer uma senha. Digite a senha e a confirmação da senha.

Decriptografar um arquivo usando uma senha

Use o seguinte comando para decriptografar um arquivo usando uma senha:

```
gpg -d <file_path>
```

Em seguida, você será perguntado para fornecer a senha. Digite a senha.

O conteúdo do arquivo será enviado para a saída padrão. Se você não deseja isso, redirecione a saída padrão para algum outro arquivo. Exemplo:

```
gpg -d mensagem.txt.gpg > mensagem.txt
```

Revision #5

Created Sun, Aug 29, 2021 2:20 PM by bushell

Updated Tue, Sep 14, 2021 3:16 PM by bushell