# Tutorial para uso do gnupg

De Stoa

## Conteúdo


- 1 Tutorial para uso do GnuPG
  - 1.1 Utilizando o GnuPG:
  - 1.2 Criando um par de chaves:
  - 1.3 Importando uma chave pública de um arquivo:
  - 1.4 Exportando sua chave pública para um arquivo:
  - 1.5 Criptografando um arquivo:
  - 1.6 Assinando um arquivo:
  - 1.7 Checando a assinatura de um arquivo:
  - 1.8 Descriptografando um arquivo:
  - 1.9 EXEMPLO 1: gerando um arquivo criptografado
  - 1.10 EXEMPLO 2: descriptografando um arquivo recebido
  - 1.11 Links:


# Tutorial para uso do GnuPG

### Utilizando o GnuPG:

Para criar um arquivo criptografado você deve:

- Criar um par de chaves.
- Importar a chave pública do seu destinatário.
- Criptografar (com a chave pública do seu destinatário) e assinar (com a sua chave) o arquivo.

Para descriptografar um arquivo você deve:

- Checar a assinatura do arquivo criptografado.
- Descriptografar o arquivo.

---

### Criando um par de chaves:

- Digite no terminal **gpg --gen-key** e escolha:
  - O tipo de criptografia.
  - O tamanho da chave (quanto maior tamanho, maior é a segurança e também o tempo de processamento).
  - A validade da chave.
  - Um userID, email e comentário.
  - IMPORTANTE: escolha uma frase secreta para sua chave, ela será necessária para descriptografar uma mensagem criptografada com a sua chave pública!

**Importando uma chave pública de um arquivo:**

- **gpg --import arquivo**

**Exportando sua chave pública para um arquivo:**

- **gpg -o arquivo --export userID**

**Criptografando um arquivo:**

- **gpg --encrypt arquivo**
  - Digite o userID do seu destinatário.
  - Será gerado um arquivo criptografado arquivo.gpg.

**Assinando um arquivo:**

É importante assinar o arquivo para seu destinatário saber que foi realmente você que o mandou.

- **gpg ---clearsign arquivo**

**Checando a assinatura de um arquivo:**

É importante checar se a assinatura do arquivo descriptografado é mesmo a do seu remetente, ele pode ser um "cavalo de tróia".

- **gpg --verify arquivo**

**Descriptografando um arquivo:**

- **gpg --decrypt arquivo**

**EXEMPLO 1: gerando um arquivo criptografado**

- Depois de exportar a chave pública do seu destinatário criptografe o arquivo:
  - **gpg -u seuUserID -r userIDdestinatário --encrypt file**
- Agora assine o arquivo gerado:
  - **gpg --clearsign file.gpg**

Será gerado o arquivo file.gpg.asc criptografado e assinado.

**EXEMPLO 2: descriptografando um arquivo recebido**

- Verifique a assinatura do arquivo:
  - **gpg --verify file.gpg.asc**
- Descriptografe a assinatura:
  - **gpg -o file.gpg -d file.gpg.asc**
- Descriptografe o arquivo:
  - **gpg -o file -d file.gpg**

Será gerado o arquivo file descriptografado.

**Links:**

Um howto um pouco mais detalhado:
http://www.dewinter.com/gnupg_howto/english/GPGMiniHowto.html

Seahorse, uma interface gráfica para o gnome: http://projects.gnome.org/seahorse/

WinPT, uma versão para para o (ru)Windows: http://winpt.gnupt.de/int/



---