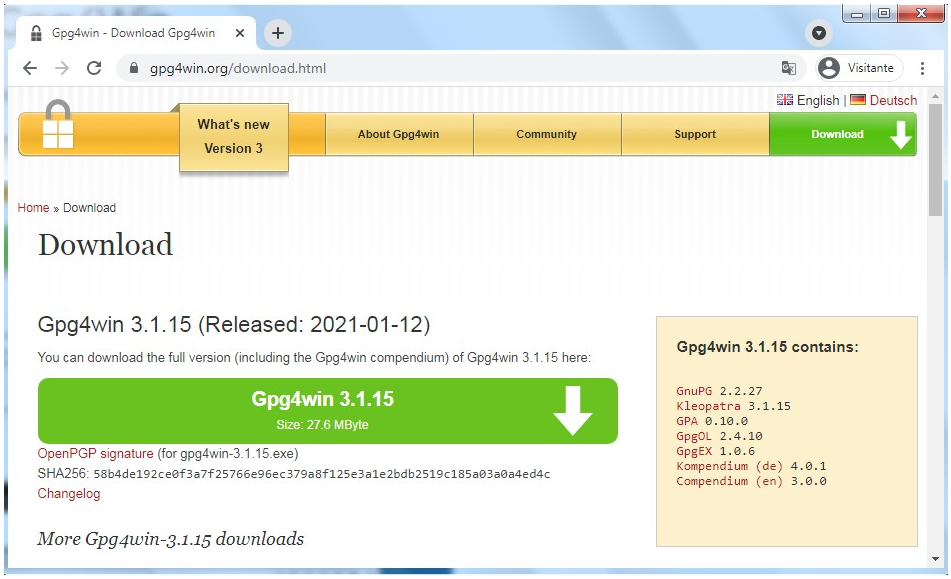
Tutorial para criar um par de chaves PGP

GnuPG para Windows - Utilize o link abaixo para fazer o download:

https://gpg4win.org/download.html

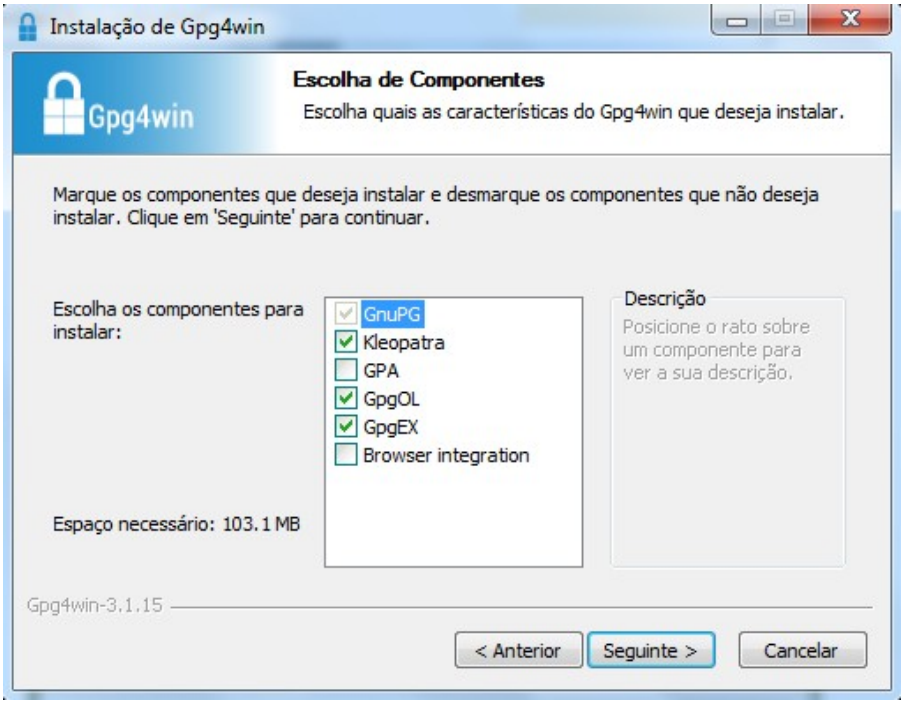
Gpg4win é um pacote de instalação para qualquer versão do Windows, que inclui o software de criptografia GnuPG. Siga abaixo as instruções detalhadas de como gerar um par de chaves PGP (privacidade muito boa, da sigla em inglês).

1. Faça o download do Gpg4win.



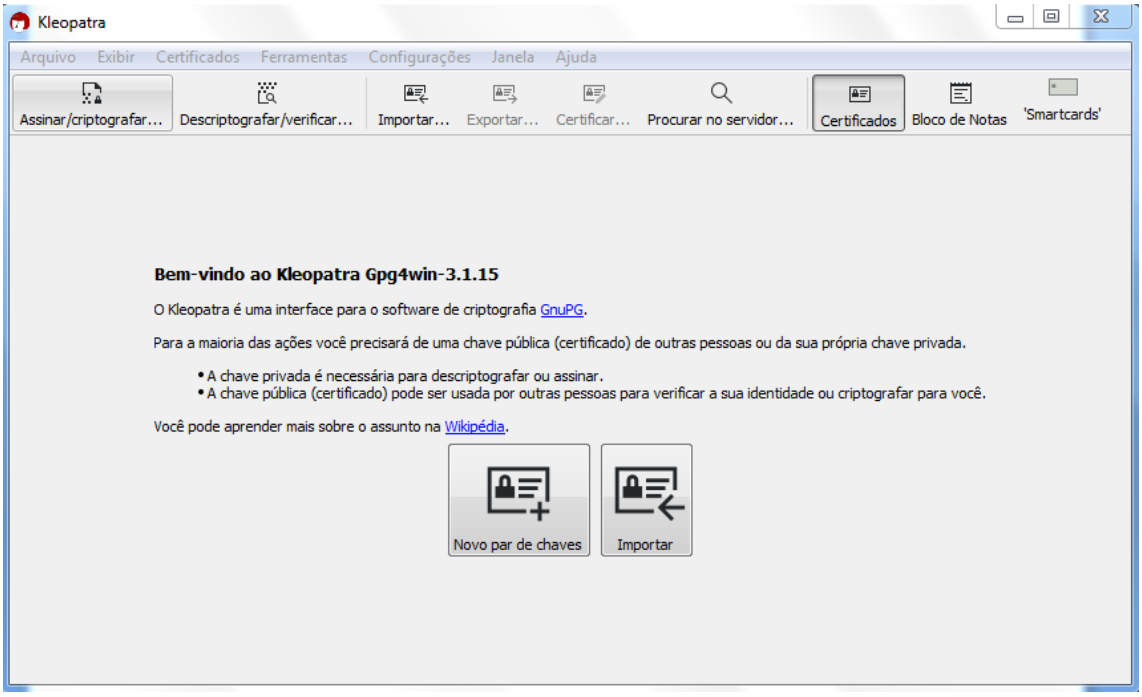
2. Instale o aplicativo

3. Deixe os seguintes componentes marcados:

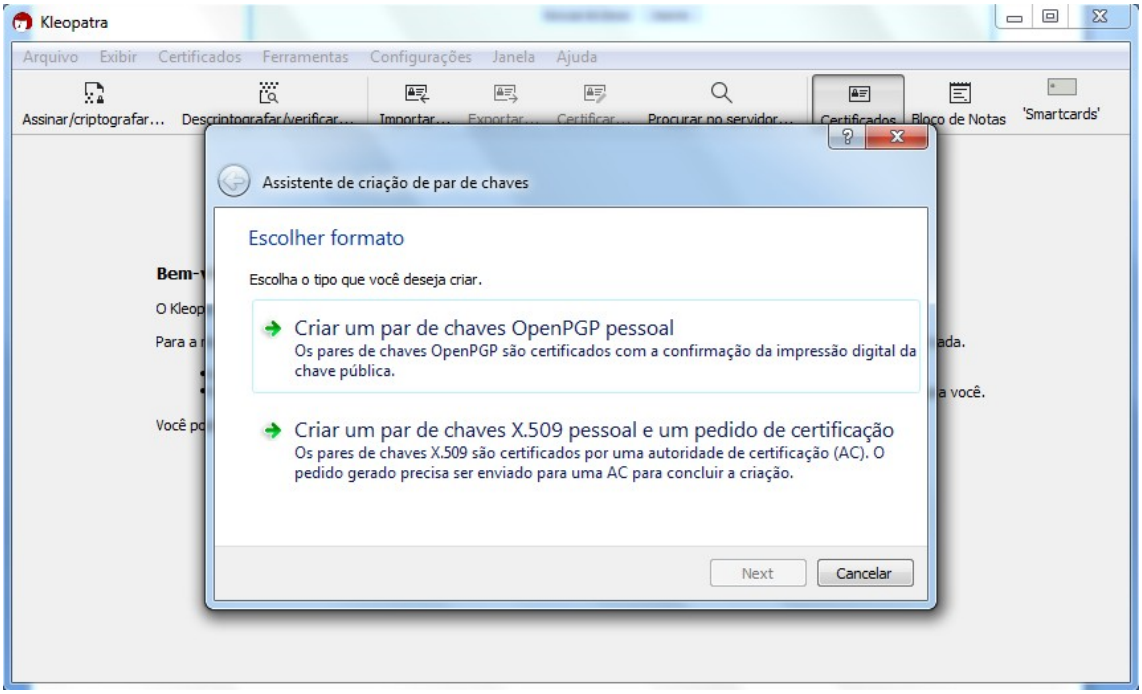


4. Termine a instalação e execute o Kleopatra para poder criar o par de chaves.

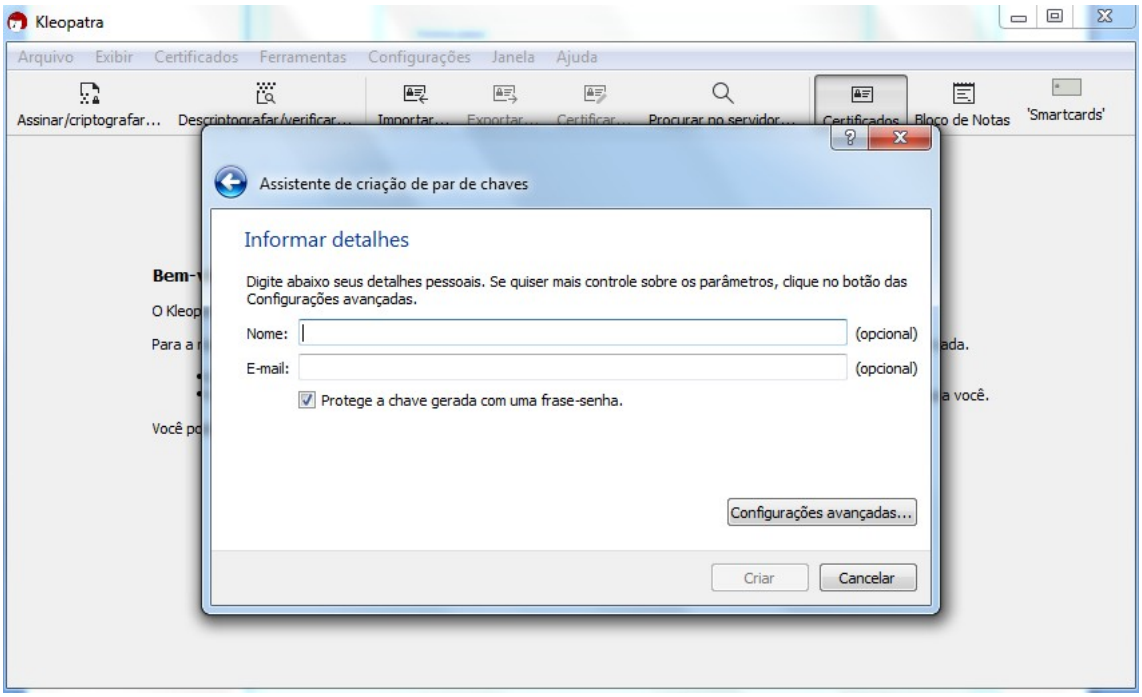
- Kleopatra é uma ferramenta do KDE para gerenciamento de certificados X.509, chaves PGP e também para gerenciamento de certificados de servidores. A janela principal deverá se parecer com a seguinte:



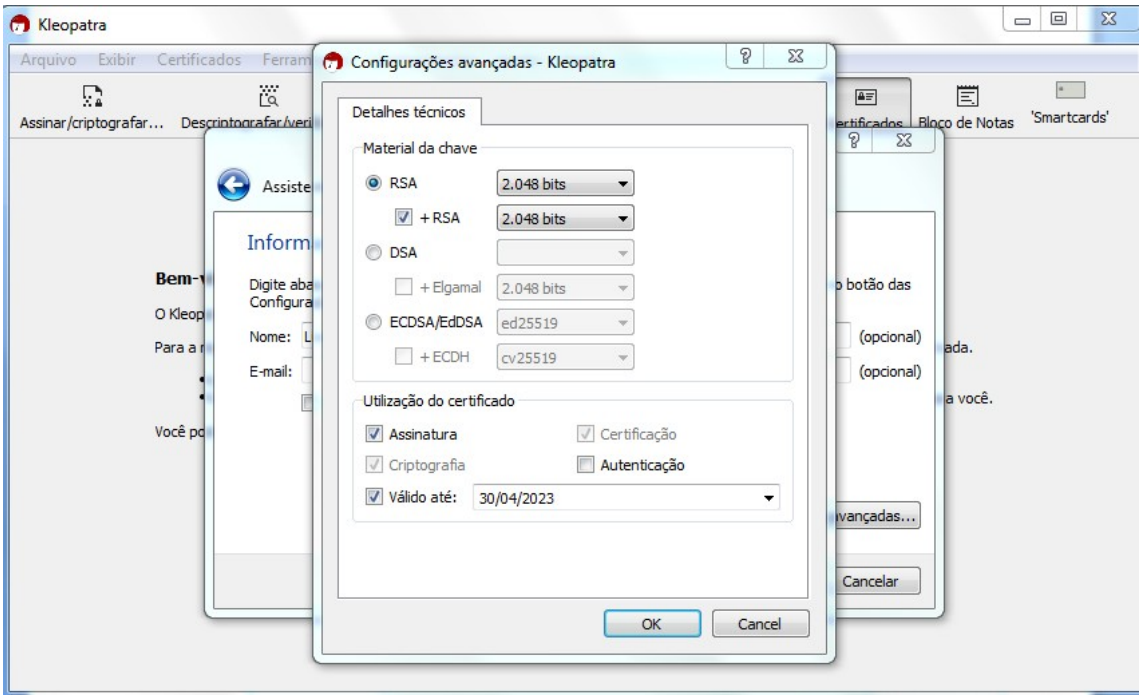
- Criando novos pares de chave:
  No item do Menu Arquivo → Novo Par de chaves... selecione Criar um par de chaves OpenPGP pessoal



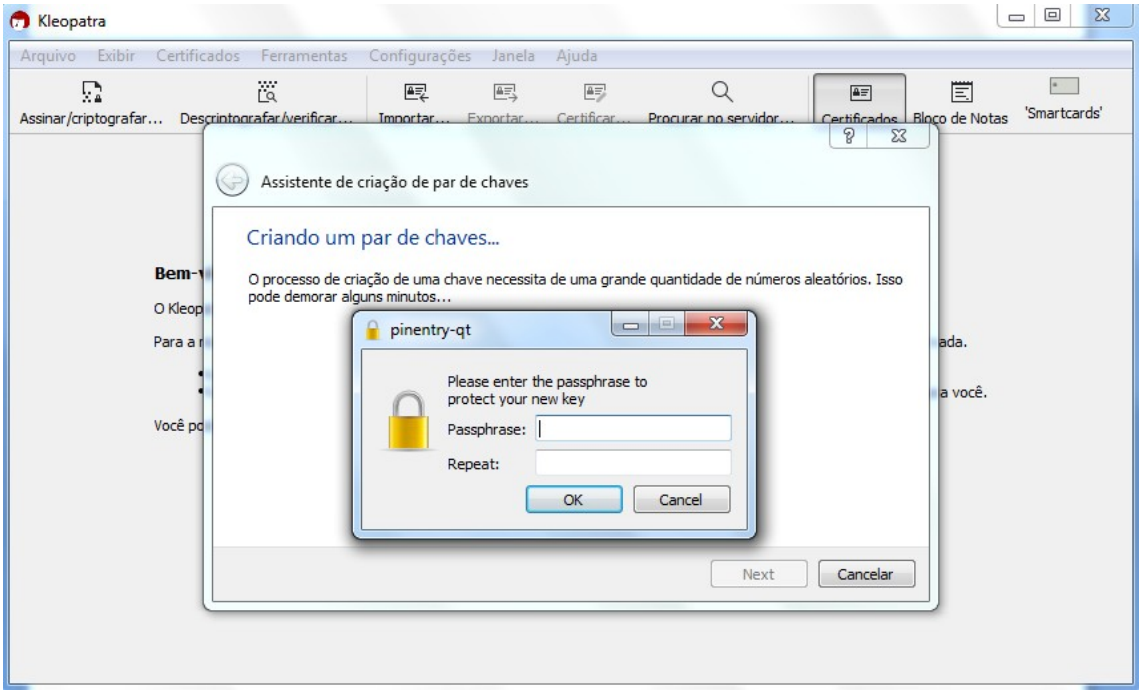
Informe os detalhes Nome: E-mail: Marque a opção para proteger a chave com senha e clique em Configurações avançadas...



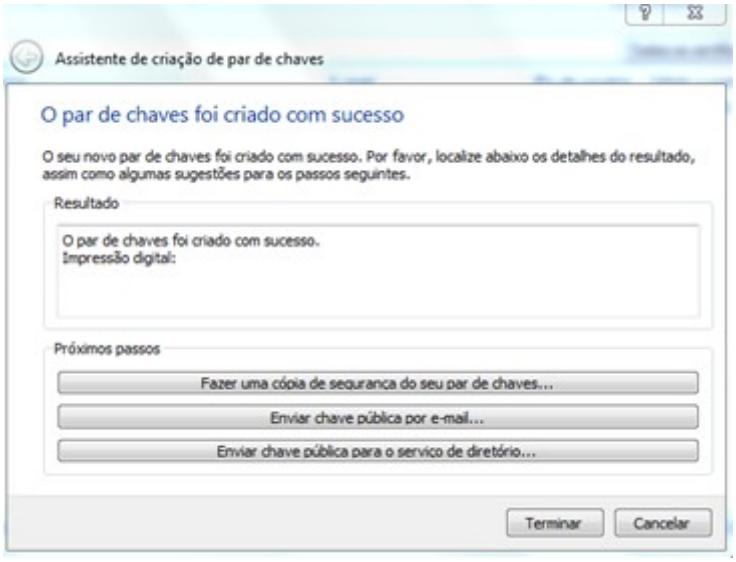
Marque as seguintes opções para tamanho das chaves e defina uma data de validade para o par de chaves. Esta data pode ser alterada depois.



Escolha a sua senha. Obs.: O ideal é colocar uma senha forte.
A senha deve conter pelo menos 8 caracteres, 1 digito ou caractere especial

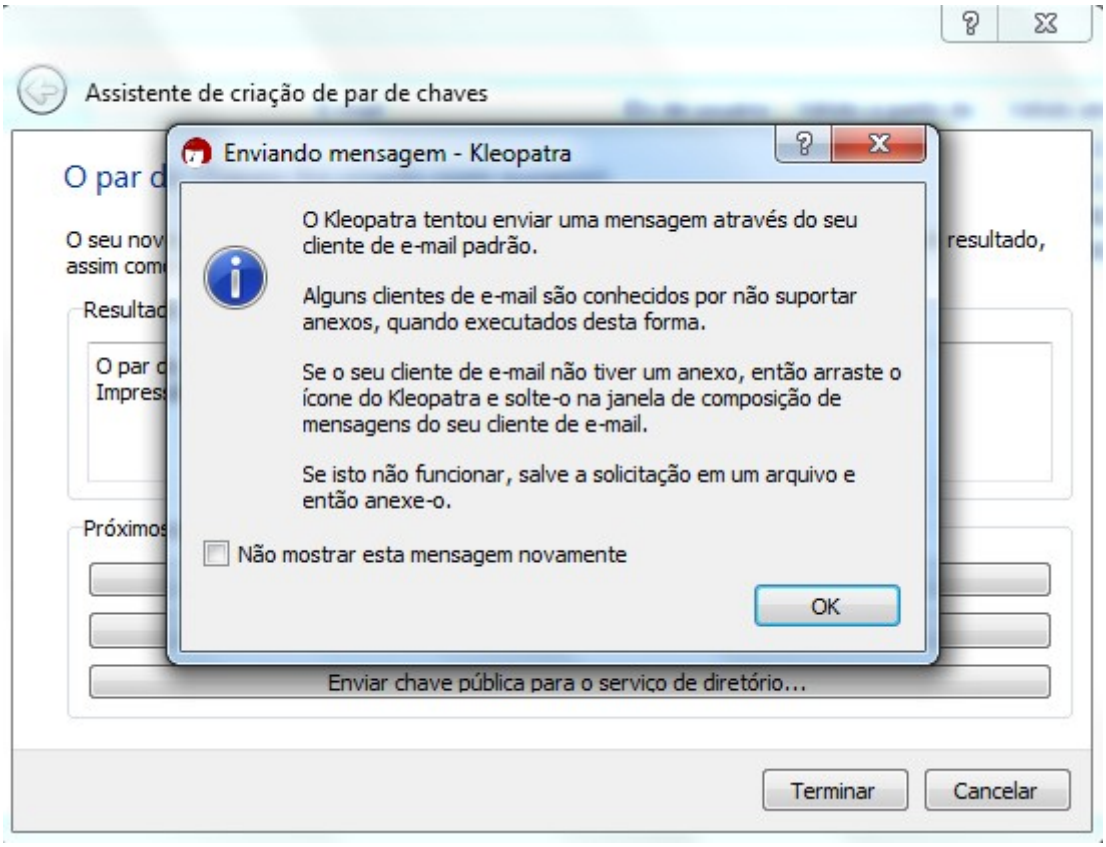


E pronto! O seu par de chaves foi criado.

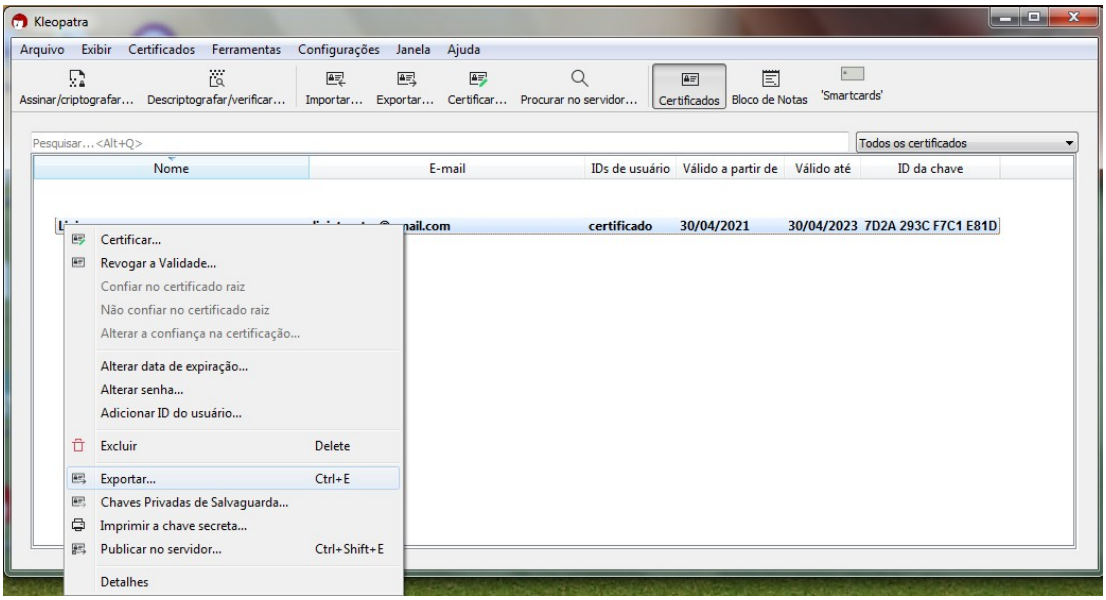


Neste ponto você pode enviar sua chave pública por email clicando em Enviar chave pública por e-mail... ou pode clicar em Terminar e exportar a sua chave pública para enviá-la por email posteriormente. Os passos das duas opções são explicados mais adiante.

Ao clicar em Enviar chave pública por e-mail... é mostrada a mensagem abaixo que irá orientá-lo para envio utilizando o seu cliente de email padrão.



Para exportar sua chave pública e enviá-la em anexo ao seu email, clique com botão direito na sua chave depois em Exportar... conforme demonstrado na tela abaixo:



Escolha o local e salve o arquivo.

GnuPG para Linux

Deixamos os comentários sobre a instalação do GnuPG de lado, pois praticamente todas as distribuições do Linux o trazem instalado. A distribuição do Linux utilizada neste tutorial foi Mint 20.1 Cinnamon e a versão do GnuPG utilizada neste tutorial foi 2.2.19.

1. Criando um par de chaves pública e privada

Abaixo temos um exemplo de criação de par de chaves (pública e privada) em nome do utilizador 'Fulano de Tal'. Abra o terminal e execute o comando abaixo para criar o par de chaves. Se não forem especificados os parâmetros adicionais, o tipo e o tamanho da chave serão RSA e 3072 bits, respectivamente. Será perguntado uma frase para a senha (**frase secreta, memorize-a**), basta responder de acordo com o que será pedido.

```
$ gpg --gen-key
```

```
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
gpg: directory '/home/user/.gnupg' created
gpg: keybox '/home/user/.gnupg/pubring.kbx' created
Note: Use "gpg --full-generate-key" for a
full featured key generation dialog.

O GnuPG precisa construir uma ID de usuário para identificar sua
chave.

Nome completo: Fulano de Tal
Endereço de correio eletrônico: fulanodetal@email.com
Você selecionou este identificador de usuário:
"Fulano de Tal <fulanodetal@email.com>"
Change (N)ame, (E)mail, or (O)kay/(Q)uit? O

Precisamos gerar muitos bytes aleatórios. É uma boa ideia realizar
outra atividade (digitar no teclado, mover o mouse, usar os discos)
durante a geração dos números primos; isso dá ao gerador de números
aleatórios uma chance melhor de conseguir entropia suficiente.

gpg: /home/user/.gnupg/trustdb.gpg: banco de dados de confiabilidade
criado
gpg: chave D5882F501CC722AA marcada como plenamente confiável
gpg: directory '/home/user/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-
revocs.d/269C3D6B65B150A9B349170D5882F501CC722AA.rev'

Chaves pública e privada criadas e assinadas.

pub rsa3072 2021-04-30 [SC] [expira: 2023-04-30]
269C3D6B65B150A9B349170D5882F501CC722AA
uid Fulano de Tal <fulanodetal@email.com>
sub rsa3072 2021-04-30 [E] [expira: 2023-04-30]
```

2. Exportando a minha chave pública

Caso alguém queira te enviar um documento ou um e-mail cifrado com sua chave, é necessário que a pessoa tenha a sua chave pública. Existem algumas maneiras da pessoa conseguir a chave: fazendo uma cópia da chave de algum servidor PGP (pgp.mit.edu) ou pedindo diretamente ao proprietário da chave. Partindo do ponto que a pessoa fez um pedido da sua chave pública, então é necessário criar um arquivo com a chave e passar o arquivo para o solicitante (por exemplo, podemos passar pelo e-mail). Execute o comando abaixo no terminal do Linux para exportar a sua chave para o arquivo **MinhaChave.asc**.

```
$gpg --export 269C3D6B65B150A9B449170D5882F501CC722AA> MinhaChave.asc
```

Onde "269C3D6B65B150A9B349170D5882F501CC722AA" é o ID da chave (da chave que criamos aqui no exemplo, **substitua pelo seu ID**) e **MinhaChave.asc** é o nome do arquivo onde será gravada a chave (**pode ser outro nome**).

3. Enviando a chave por e-mail

Agora basta enviar o arquivo com a chave pública para a pessoa e então ela poderá criptografar um e-mail ou um documento com a sua chave pública. Se foi criptografado com a sua chave pública, somente a sua chave privada será capaz de decodificar o documento (e a **frase secreta** de sua chave será requisitada).

4. Criptografando um documento

Para encriptar um documento com a chave pública de 'Fulano de Tal' basta seguir os passos abaixo, substituindo **NomeArquivo** pelo nome do arquivo a ser criptografado. Um arquivo com nome **NomeArquivo.gpg** será criado na pasta atual. Este arquivo com dados criptografados só poderá ser decifrado pela chave privada de 'Fulano de Tal'.

```
$ gpg -e NomeArquivo
```

```
Você não especificou um ID de usuário. (pode-se usar "-r")
Recipientes atuais:
Entre com o ID do usuário. Final com uma linha vazia: Fulano de Tal
Recipientes atuais:
rsa3072/4628820328759F85 2021-04-30 "Fulano de
Tal <fulanodetal@email.com>"
Entre com o ID do usuário. Final com uma linha vazia: <Enter>
```

5. Decifrando um documento

Para decifrar um documento que foi criptografado por Fulano de Tal basta seguir os passos abaixo, substituindo **NomeArquivo.gpg** pelo nome do arquivo cifrado. Será solicitada a frase secreta da chave privada de Fulano de tal, basta inseri-la. Um arquivo com nome **ArquivoTextoClaro** será criado na mesma pasta. Este arquivo contém os dados decifrados.

```
$ gpg -d NomeArquivo.gpg > ArquivoTextoClaro
gpg: criptografado com 3072-bit RSA chave, ID 4628820328759F85, criado
2021-04-24
"Fulano de Tal <fulanodetal@email.com>"
```