GnuPG Assinatura de Chaves

#FiqueEmCasaUseDebian

Thiago Andrade Marques
Campinas - SP, 14 maio 20

SUMÁRIO

SUMÁRIO

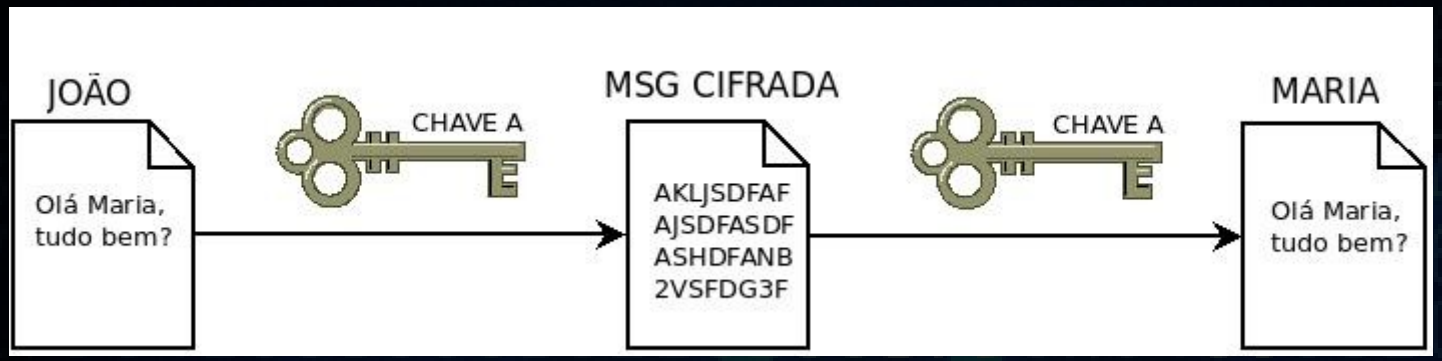
O QUE É O GNUPG

- O GnuPG é uma implementação completa e gratuita do padrão OpenPGP (Pretty Good Privacy), conforme definido pela **RFC4880**.
- **Permite “Criptografia” e assinatura digital.**
- O GnuPG, também conhecido como GPG, é uma ferramenta de linha de comando com diversos recursos.
- **GnuPG é software livre e está em grande parte sob a licença GPL-3+.**

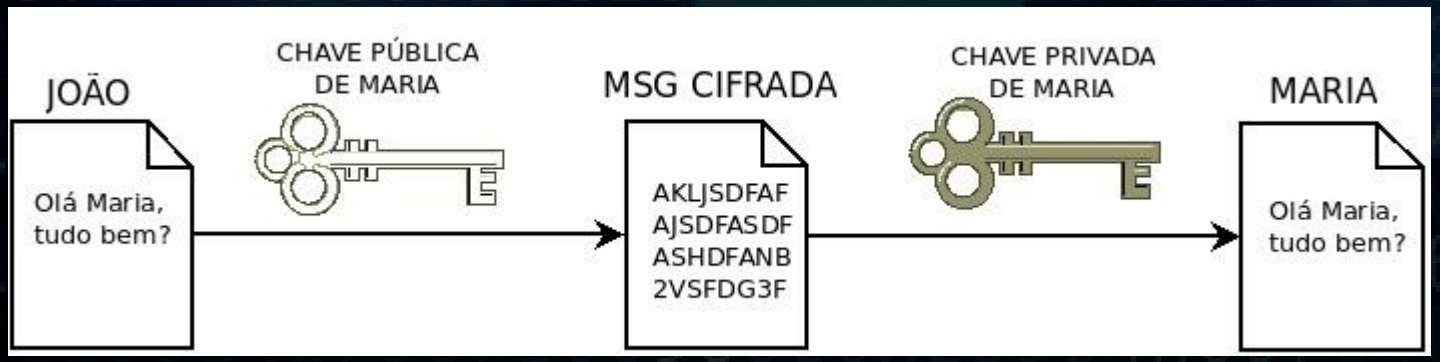
SUMÁRIO

TIPOS DE CRIPTOGRAFIA

- **Simétrica**



- **Assimétrica**



TIPOS DE CRIPTOGRAFIA

- **Simétrica**
  - Simplicidade.
  - Preciso de outro meio para trocar a senha.
  - Não permite assinatura.

- **Assimétrica**
  - Utiliza par de chaves somente, não preciso de várias chaves para assina.
  - Permite assinatura. (autenticidade, não repúdio, integridade).
  - Difícil manipulação, nem todos sabem usar.

SUMÁRIO

FALANDO DE CRIPTOGRAFIA

Componentes Básicos:

- **Autenticidade – certeza da origem.**
- **Não repúdio – o remetente não pode dizer que não foi ele quem envio a msg.**
- **Integridade – certeza de que a msg não foi alterada no meio de comunicação.**
- **Confidencialidade – criptografia,embaralhamento.**

SUMÁRIO

AFINAL, O QUE É ASSINAR UMA CHAVE?

- Assinar uma chave é criptografar com a chave privada.
- **A assinatura de uma chave gera uma relação de confiança mútua.**
- Exemplo:

  - Aluno1 assina a chave do Aluno2: Isso quer dizer que o Aluno1 atesta que aquela chave realmente é do Aluno2.

SUMÁRIO

CUIDADOS AO ASSINAR UMA CHAVE

- **Nunca assine uma chave de uma pessoa que não a tenha encontrado pessoalmente.**
- **Confira através de um documento com foto que aquela pessoa é ela mesma. Pode-se solicitar um meio adicional para verificar se o documento não é falso.**
- **Confira se o nome completo da pessoa é o mesmo que está na Chave GPG.**

SUMÁRIO

PRECISO DE UMA CHAVE GPG NO DEBIAN?

- **SIM.**

- **Para processo de DM(Debian Maintainer) 1 ass DD**
- **Para processo de DD(Debian Developer) 2 ass DD**
- **RSA (>=4)**
- **4096 bits**
- **Chave completa com todos recursos.(Pública e Privada)**

SUMÁRIO

PRÁTICA

- Instalando o GnuPG
apt install gnupg

- Listando as chaves
gpg –list-keys

- Caso esteja em uma jaula
echo "pinentry-mode loopback" >> ~/.gnupg/gpg.conf – permitir que a passphrase seja digitada no console

- Criando a chave
gpg --full-generate-key
RSA and RSA
4096 bits
2y

- Gerando certificado de revogação
gpg --gen-revoke <id da chave> ./revoke.crt
razão 1

- Exportando chave para outra máquina.
gpg -a --export <id da chave> > aluno1.pub
gpg -a --export-secret-keys <id da chave> > aluno1.key

- Importando em outra máquina
gpg --import aluno1.key aluno1.pub

- Enviando chave para keyserver na Internet
keyserver keyserver.2ndquadrant.com no gpg.conf
gpg --send-keys <id da chave>
gpg --keyserver keyring.debian.org --send-keys <id da chave>

PRÁTICA

- Criptografia simétrica
mcedit teste.txt
gpg --symmetric -a teste.txt
gpg -d teste.asc > teste

- Criptografia assimétrica
gpg --search-keys
gpg -e -a teste
gpg -d teste.asc

- Assinando arquivos
gpg --clearsign teste
gpg --verify test.asc

- Assinando chaves
Recebendo chave do servidor
gpg --search-key aluno1.gpg@gmail.com
- ASSINAR A CHAVE DO ALUNO1
importando para o seu chaveiro
gpg --sign-key <id da chave>
gpg --list-sign
gpg -a --export <id da chave> > nome.asc
Enviar por email
O dono da chave deverá importá-la no seu chaveiro
gpg --import <arquivo que contem a chave assinada>
gpg --list-sign

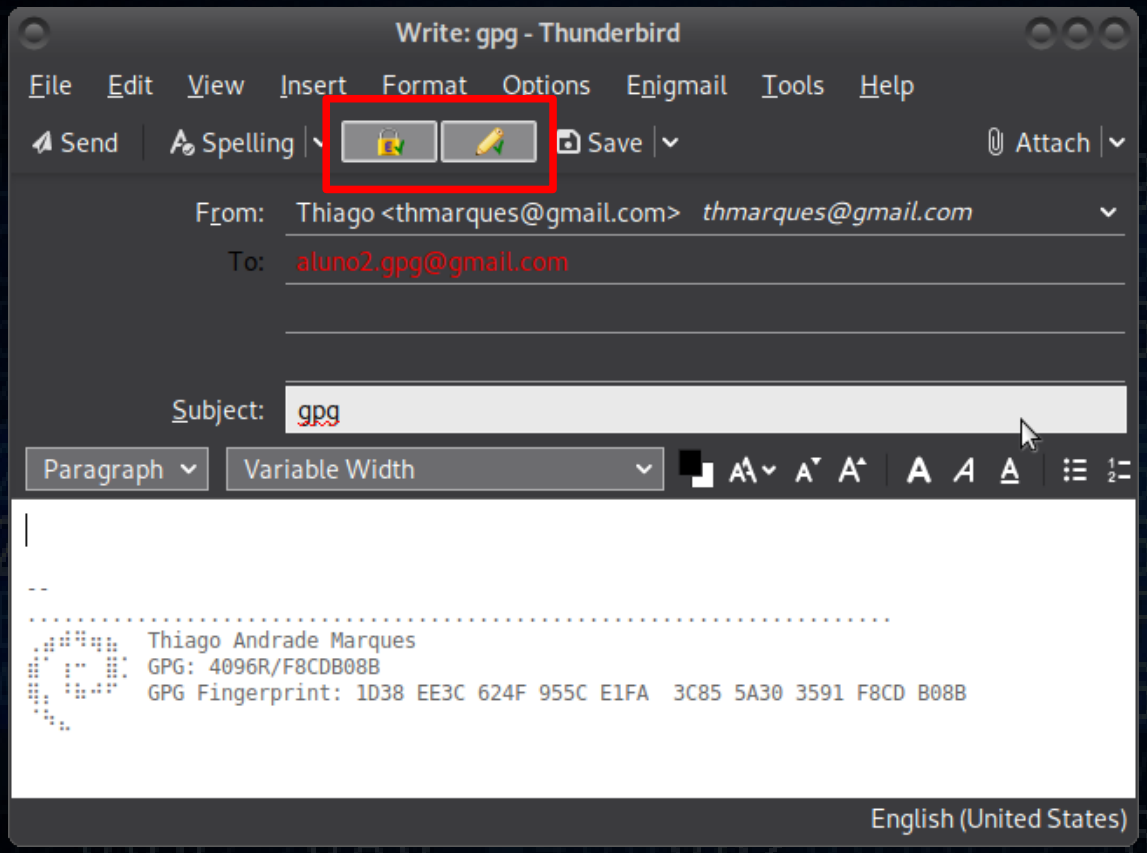
PRÁTICA

Utilizando o EXIM4 + CAFF
 # apt install signing-party exim4
Vamos configurar o GMAIL como MTA para enviar emails.
 # dpkg-reconfigure exim4-config
mail sent by smarthost; no local mail
gmail
deixar 127.0.0.1 ; 0:11
Outros destinos para os quais mensagens devem ser aceitas: deixar em branco
Nome de domínio visível para usuários locais: deixar em branco
smtp.gmail.com::587
Manter o número de pesquisas DNS mínimas (Discagem-sob-Demanda)? Não
Dividir a configuração em pequenos arquivos? Não
 # cat /etc/exim4/update-exim4.conf.conf
 # cat passwd.client
No caso do gmail deve-se permitir aplicativos menos seguros de utilizar sua conta de email
https://myaccount.google.com/security
No arquivo passwd.client
smtp.gmail.com:aluno1.gpg@gmail.com:senhaparaappsmenosseguros
Testar envio de email
 # echo "teste de email" | sendmail aluno2.gpg@gmail.com
Caso algo der errado estará em:
 # cat /var/log/exim4/mainlog
Configurar caff
 # caff
Editar o arquivo criado em ~/.caffrc
$CONFIG{'owner'} = 'Aluno1';
$CONFIG{'email'} = 'aluno1.gpg@gmail.com';
$CONFIG{'keyid'} = [qw{3DD433F9ED097888EF177C87BD1D370F0F7375EE}];

caff 1D38EE3C624F955CE1FA3C855A303591F8CDB08B
gpg> quit
gpg> Y

ADDONS

- **Cliente de e-mail Thunderbird – Enigmail**



SUMÁRIO

CONCLUSÃO

- **GnuPG serve para muito mais que somente criptografia.**
- **Pode-se ser usado livremente na Internet ou em ambiente corporativo.**
- **“Argumentar que você não se importa com o direito à privacidade porque não tem nada a esconder não é diferente de dizer que não se importa com a liberdade de expressão porque não tem nada a dizer.” - Edward Snowden**

REFERÊNCIAS

- **https://eriberto.pro.br/wiki/index.php?title=Usando_o_Caff_%2B_Exim_para_assinar_e_enviar_chaves_GPG**
- **https://eriberto.pro.br/wiki/index.php?title=Usando_o_GnuPG**
- **https://www.debian.org/events/keysigning.pt.html**
- **https://wiki.debian.org/Keysigning**
- **https://keyring.debian.org/creating-key.html**
- **https://wiki.debian.org/caff**
- **https://gnupg.org/**

Thiago Andrade Marques
GPG: 4096R/F8CDB08B
GPG Fingerprint: 1D38 EE3C 624F 955C E1FA 3C85 5A30 3591 F8CD B08B

Palestra disponível em *https://andrade.wiki.br/palestras/*