Seminário - Redes II: GnuPG

Hernane Velozo Rosa Gustavo Valadares Castro João Víctor Martins Medeiros
Matheus Dias Soares Pedro Igor Martins dos Reis

Pontifícia Universidade Católica de Minas Gerais

2 de junho de 2024

PUC Minas

Introdução

- **GnuPG** (*GNU Privacy Guard*) é uma ferramenta gratuita e de código aberto para criptografia e assinatura de dados [2];
- Se propõe a garantir a privacidade e a autenticidade das comunicações digitais [3];
- Desenvolvido como uma alternativa ao PGP (*Pretty Good Privacy*);
- Parte do projeto **GNU**, seguindo os princípios do software livre.

PUC Minas

Instalação e Configuração

```
brew install gnupg                          # MacOS
winget install -h gnupg.Gpg4win             # Windows 10/11
sudo {apt,dnf,pacman,...} install gnupg # Distribuições Linux
```

Listing 1: Comandos para instalação

PUC Minas

Exemplos de uso

```
gpg --gen-key                          # Gerar chave;
gpg --import chave.pub                 # Importar chave;
gpg --export -a "nome" > chave.pub     # Exportar chave;
gpg --list-keys                        # Listar chaves;
gpg -e -r "recipient" arquivo          # Criptografar arquivo;
gpg --sign arquivos                    # Gerar assinatura;
gpg --verify arquivo.assinado          # Verificar assinatura.
```

Listing 2: Parâmetros úteis

PUC Minas

Exemplos de uso

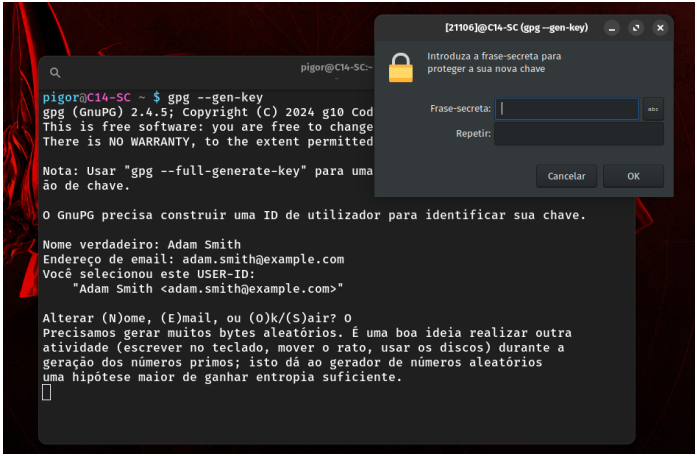


Figura: Comando '–gen-key' em execução.

PUC Minas

```
gpg: pasta '/home/ad-smith/.gnupg/openpgp-revocs.d' criada
gpg: certificado de revogação armazenado como '...F015906A9083E.rev'
chaves pública e privada criadas e assinadas.

pub   ed25519 2024-05-31 [SC] [expira: 2027-05-31]
      CCEBE16CFA1F1958058FB4BC1C8F015906A9083E
uid   Adam Smith <adam.smith@example.com>
sub   cv25519 2024-05-31 [E] [expira: 2027-05-31]
```

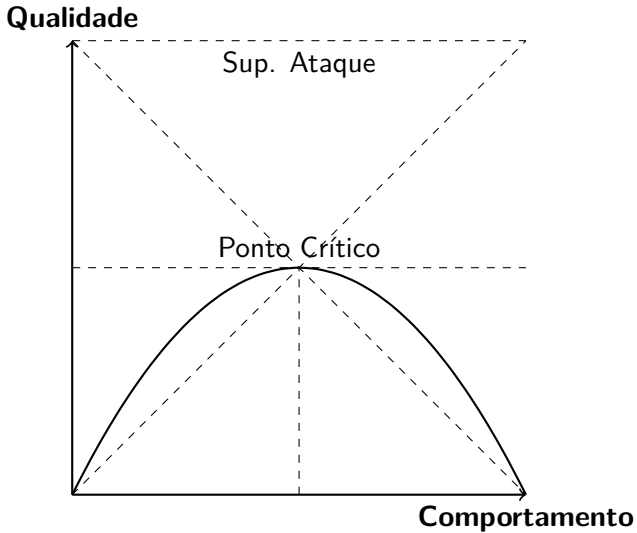
Listing 3: Saída de exemplo

PUC Minas

Funcionalidade

- Criptografa arquivos e mensagens para proteger contra acesso não autorizado;
- Confirma a origem e integridade dos dados recebidos;
- Garante a autenticidade e integridade dos dados;
- E-mails, documentos, arquivos sensíveis;
- Uso em sistemas de controle de versão [1] para assinar *commits* (ex.: Git).

PUC Minas



PUC Minas

Enunciado

O GnuPG (GNU Privacy Guard) é uma ferramenta amplamente utilizada para criptografia e assinatura digital de dados. No entanto, há situações onde o uso do GnuPG pode não ser a escolha mais prática. Em qual dos cenários abaixo o uso do GnuPG provavelmente não seria prático?

- a) Envio de documentos sensíveis por e-mail entre duas empresas que já possuem chaves públicas trocadas e configuradas.
- b) Criptografia de arquivos armazenados em um servidor compartilhado, acessível por vários funcionários que possuem chaves públicas compatíveis.
- c) Troca de mensagens instantâneas em tempo real entre duas pessoas usando um aplicativo de bate-papo.
- d) Assinatura digital de documentos para garantir a autenticidade e integridade ao enviar para clientes que utilizam GnuPG.

PUC Minas

Gabarito

O GnuPG (GNU Privacy Guard) é uma ferramenta amplamente utilizada para criptografia e assinatura digital de dados. No entanto, há situações onde o uso do GnuPG pode não ser a escolha mais prática. Em qual dos cenários abaixo o uso do GnuPG provavelmente não seria prático?

- a) Envio de documentos sensíveis por e-mail entre duas empresas que já possuem chaves públicas trocadas e configuradas.
- b) Criptografia de arquivos armazenados em um servidor compartilhado, acessível por vários funcionários que possuem chaves públicas compatíveis.
- **c) Troca de mensagens instantâneas em tempo real entre duas pessoas usando um aplicativo de bate-papo.**
- d) Assinatura digital de documentos para garantir a autenticidade e integridade ao enviar para clientes que utilizam GnuPG.

PUC Minas

Referências

[1] Michael Lucas. *PGP & GPG: Email for the practical paranoid*. No Starch Press, 2006.

[2] GnuPG Project. *The GNU Privacy Guard*. https://gnupg.org. 2024.

[3] Arch Linux Team. *GnuPG - ArchWick*. https://wiki.archlinux.org/title/GnuPG. 2024.

PUC Minas