

# Seminário - Redes II: GnuPG

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

Pontifícia Universidade Católica de Minas Gerais

4 de junho de 2024

- **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.

```
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

```
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

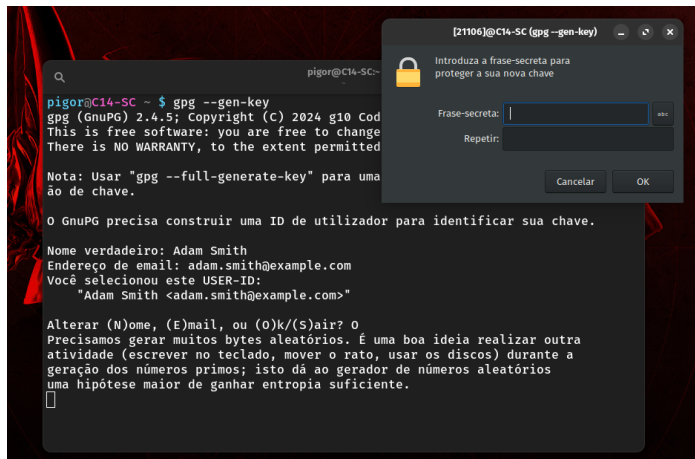


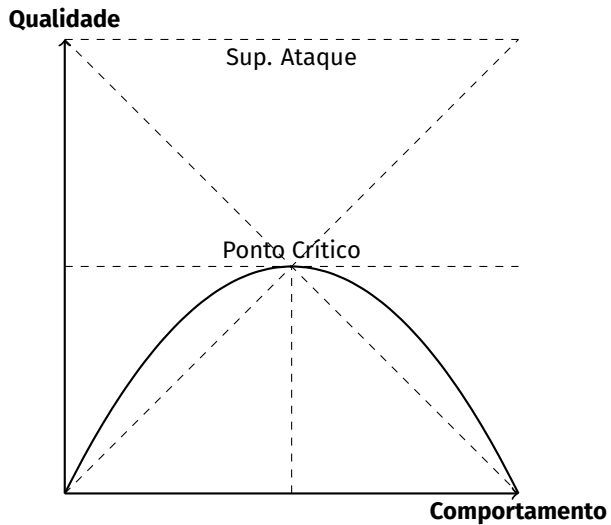
Figura: Comando '–gen-key' em execução.

```
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

- 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).





**Considere as afirmativas abaixo e, em seguida, escolha a alternativa correta.**

”Utilizar o GnuPG para criptografar um arquivo garante que somente o destinatário pretendido possa ler seu conteúdo, desde que este possua a chave privada correspondente.”

- I. A criptografia de dados utilizando GnuPG utiliza um par de chaves: uma chave pública para criptografar e uma chave privada para descriptografar.
- II. Somente o possuidor da chave pública pode acessar o conteúdo criptografado.
- III. A chave pública é distribuída ao destinatário para que ele possa descriptografar o arquivo.
- IV. A segurança do sistema depende da integridade e segurança da chave privada do destinatário.
- V. A criptografia com GnuPG pode ser revertida por qualquer pessoa que possua a chave privada correspondente.

- A) Apenas a afirmativa I está correta.
- B) As afirmativas I e IV estão corretas.
- C) As afirmativas I, II e V estão corretas.
- D) As afirmativas I, IV e V estão corretas.
- E) As afirmativas I, III e IV estão corretas.

- A) Apenas a afirmativa I está correta.
- B) As afirmativas I e IV estão corretas.
- C) As afirmativas I, II e V estão corretas.
- D) As afirmativas I, IV e V estão corretas.
- E) As afirmativas I, III e IV estão corretas.

- [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.