



Adm. e Segurança de Redes de Computadores

C.T. Informática
Prof. Vinícius Alves Hax




Antes

- DHCP: Uso e configuração no Linux



Hoje

- SSH: Teoria e configuração



Acesso remoto é o nome que se dá ao ato de acessar um computador que está disponível pela rede

Tipos de acesso remoto

- Modo gráfico:
 - + Fácil de usar
 - Exige que o computador remoto tenha uma interface gráfica
- Modo texto
 - Menos amigável
 - + Não requer interface gráfica

Tipos de acesso remoto

- Modo gráfico
 - VNC (Virtual Network Computing)
 - RDP (Remote Desktop Protocol): muito utilizado para conectar em sistemas Windows
 - TeamViewer
- Modo texto
 - Telnet
 - SSH (Secure Shell)

Telnet x SSH

- Telnet
 - Vem pré-instalado em sistemas Windows
 - Muito antigo: sujeito à bugs e falhas de segurança porém compatível com sistemas antigos
 - Não possui autenticação e criptografia
- SSH
 - Precisa ser instalado no Windows
 - Atualizado e mais seguro
 - Não compatível com todos modelos de equipamentos de rede



SSH

- Além de execução de comandos permite:
 - Executar programas gráficos remotamente (tela é 'montada' no destino mas 'replicada' na origem)
 - Cópia de arquivos

Instalando o servidor SSH

- A principal implementação do protocolo SSH é o OpenSSH
- No Linux o seu pacote é o openssh-server
 - \$ sudo apt update
 - \$ sudo apt install openssh-server
- Por padrão roda na porta 22 (TCP)

Utilização básica

- No Windows pode ser usado o software Putty
- No Linux o cliente já vem instalado
- Para conectar em HOST usando o usuário USERNAME

```
$ ssh USERNAME@HOST
```

- Se o usuário for omitido será usado o usuário do próprio sistema
- HOST pode ser um hostname ou um IP

```
Ex: $ ssh vinicius@192.168.0.10
```

Cópia de arquivos

- Destino remoto

```
$ scp FILE USERNAME@HOST:FOLDER
```

- Ex (copia arquivo.txt para a pasta ~ do servidor):

```
$ scp arquivo.txt aluno@ifsul.edu.br:~
```

- Destino local

```
$ scp USERNAME@HOST:FOLDER FILE
```

- Ex:

```
$ scp aluno@server:/home/vinicius/teste.doc
```



Mas é chato digitar a senha toda vez. É possível configurar a autenticação sem senha?



Mas é chato digitar a senha toda vez. É possível configurar a autenticação sem senha?

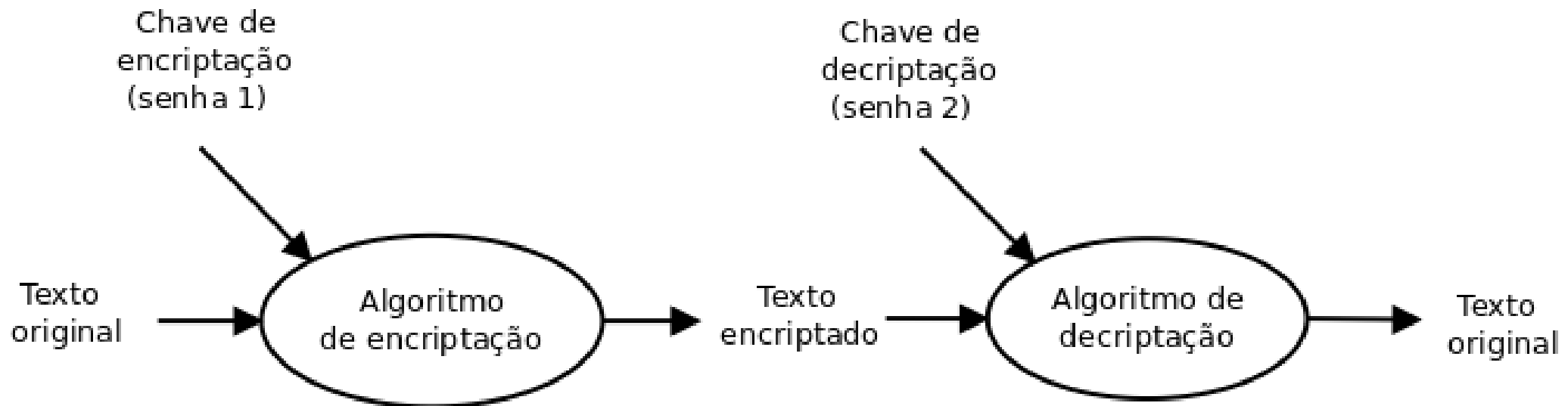
R: Sim, mas para isso precisamos conhecer/relembrar o conceito de chave pública



Criptografia

- “[...] área que estuda e pratica princípios e técnicas para comunicação segura na presença de terceiros [...]”
 - <https://pt.wikipedia.org/wiki/Criptografia>
- Tipos
 - Chave pública
 - Chave privada

Criptografia



Fonte: Autor, inspirado por Tanenbaum
(Sistemas Operacionais)



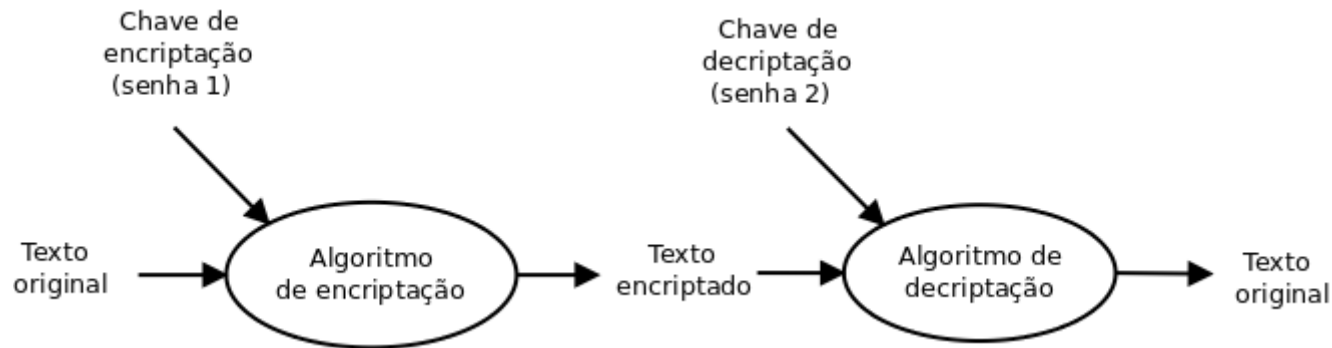
Criptografia de chave privada

- Baseada em compartilhar uma chave (“senha”) entre dois agentes confiáveis
- Exemplo clássico: cifra de César
- Problema básico: como compartilhar a senha?

Criptografia de chave pública

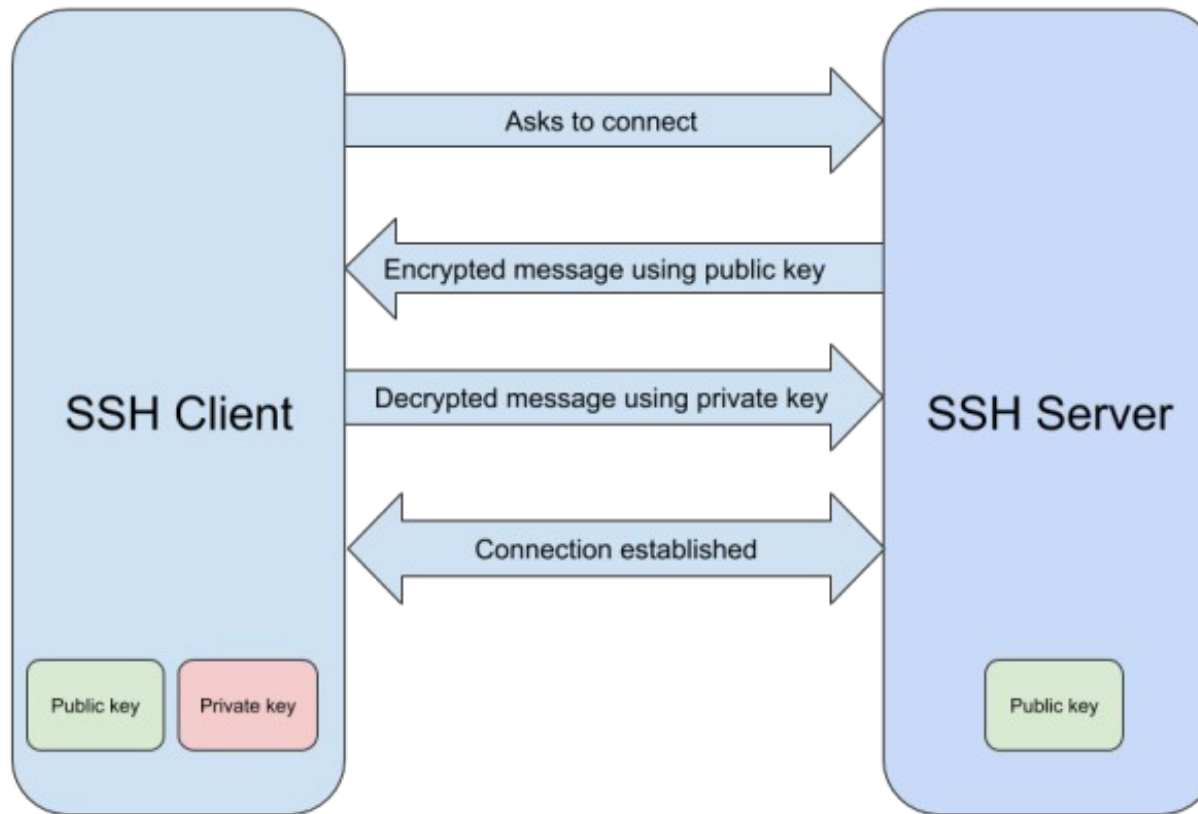
- Se baseia no fato de que algumas funções são de mão única, ou seja
 - Calcular: $f(a) = b$, é fácil
 - Mas calcular $\text{InvF}(b) = a$, é inviável computacionalmente
 - Exemplo:
 - Descubra quais números primos que multiplicados resultam em 187. Resposta: 11 e 17 (demorado)
 - Qual o resultado da multiplicação dos dois números primos 11 e 17? (rápido)

Criptografia de chave pública (2)



- Nessa caso a chave de encriptação é a chave pública (conhecida). A chave de deciptação é a chave privada.
- Se A quer mandar uma mensagem para B, ele criptografa a mensagem usando a chave pública de B. Só B pode ler a mensagem pois só ele tem a chave privada.

SSH sem senha



Fonte: Krasnov (2020)

SSH sem senha (na prática)

- Gerando a chave no cliente:

```
$ ssh-keygen
```

```
Your identification has been saved in /home/vinicius/.ssh/id_rsa  
Your public key has been saved in /home/vinicius/.ssh/id_rsa.pub
```

- Copiando a chave para o servidor:

```
$ ssh-copy-id USERNAME@HOST
```

- Testando

```
$ ssh USERNAME@HOST
```

Arquivo de configuração do SSH

- O arquivo de configuração do servidor SSH é o `/etc/ssh/sshd_config`
(Sempre faça backups antes de fazer alterações!)



Referências

- <https://everyday.codes/linux/how-passwordless-ssh-login-works/>
- Notas de aula do professor Marcelo Kwecko