Semana de Calouros 2026

Linux

Aula IV

Login:
Senha:

2026

Login e senha para o curso

Criamos contas temporárias para vocês usarem no Curso de Linux.

Observe que o computador que você está usando possui um adesivo com uma letra e um número. Exemplo: H30 ou i12.

Você vai usar esse número para o seu login e senha.

Login e senha para o curso

Computadores do LAB 12:

- Considere @ = número do seu computador.
- Exemplo: se o seu computador é o H30, @ = 30.

Computadores do LAB 3:

- Considere @ = número do seu computador + 60.
- Exemplo: se o seu computador é o i12, @ = 72.

Computadores do LAB 4:

- Considere @ = número do seu computador + 80.
- Exemplo: se o seu computador é o l23, @ = 103.

Login e senha para o curso

Sabendo o seu @, seu login e senha são:

- Login: clinux@
- Senha: clinux@#@

Relembrando...

Comandos

- `touch` - atualiza data de acesso ou cria novo arquivo
- `rm` - remove arquivo/diretório
- `mv [arquivo] [destino]` - move arquivo/diretório
- `man` - mostra o manual do comando
- `cp` - copia arquivo/diretório
- `less` - lê o arquivo de forma interativa
- `cat` - concatena e imprime o conteúdo do arquivo
- `sudo` - usa os poderes do super usuário

1.

Recomendações de programas

Navegadores Web

Firefox

Chromium

Qutebrowser

Multimídia

VLC
Vídeos e músicas

Eye of GNOME
Imagens

sxiv
Imagens

Gerenciadores de arquivos

LF

Terminal

Files for GNOME
Gráfico

Nemo
Gráfico

Office documentos, planilhas e apresentações

LibreOffice

WPS

Google Docs

Pesquise sobre o Latex!

Lista de aplicações

wiki.archlinux.org/title/List_of_applications

2.

Secure Shell

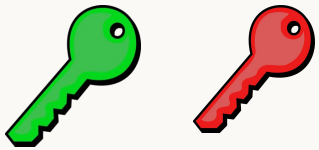
Criptografia

- Criptografia é uma área de estudo que visa desenvolver algoritmos para **codificar mensagens** de forma que sua transmissão seja segura em qualquer meio, i.e., **apenas o destino consiga lê-la** assim como o **destinatário tenha garantia da origem** da mensagem
- Algoritmos de criptografia são utilizados nos mais diversos sistemas computacionais, e.g., sistemas **bancários, https e ssh**
- 💡 Pesquise sobre criptografia simétrica e assimétrica

ssh secure **sh**ell

- O *Secure Shell* é um protocolo de rede criptografado, sendo seguro para utilizar em redes públicas (não seguras)
- É um protocolo TCP/IP na camada de aplicação, i.e., a mais alta
- Com o **ssh**, é possível fazer login em uma máquina remota, assim, tendo **acesso a um shell** naquele computador
- Utiliza a criptografia de chave pública, um algoritmo **assimétrico**
- Além de abrir um **shell em máquinas remotas**, é possível, também, mover arquivos entre os computadores
- 💡 Pesquise sobre o OpenSSH e criptografia de chave pública

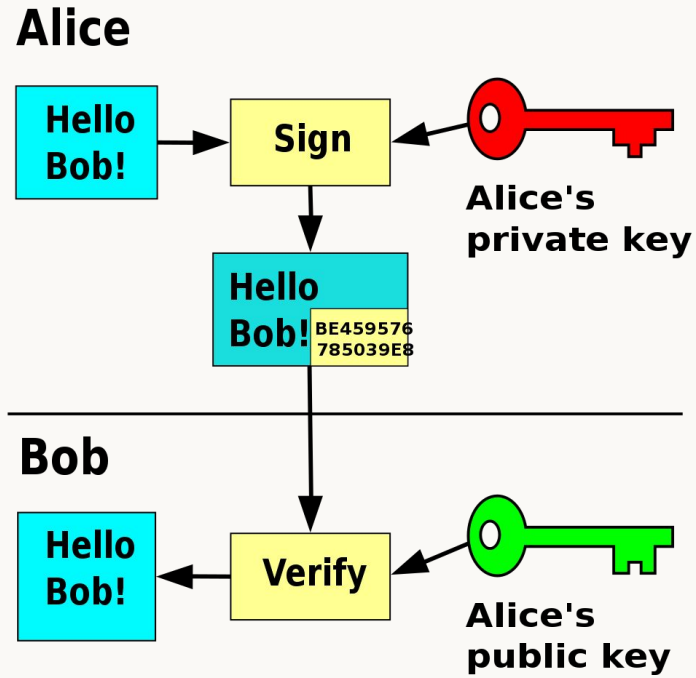
Criptografia de chave pública



- Uma chave pode ser aplicada numa mensagem, transformando ela numa mensagem criptografada (ex: olá mundo -> ahsdhajjnwbjb1io2ji0wvevji0ih0)
- Para recuperar a mensagem original, é preciso aplicar uma outra chave, que faz o processo reverso (descriptografia)
- Na criptografia de chave pública, cada pessoa tem duas chaves: uma **chave pública** (pode ser divulgada) e uma **chave privada** (deve ser guardada em segredo)
- Essas chaves fazem o **processo reverso da outra**: se aplicarmos a chave privada da pessoa numa mensagem criptografada com a chave pública dela, conseguimos recuperar a mensagem original, e vice-versa

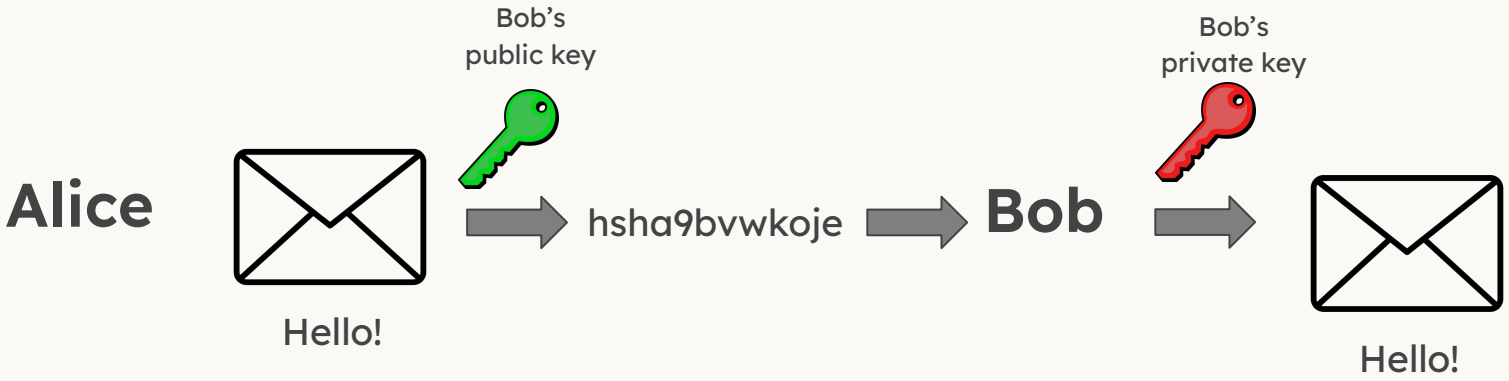
Criptografia de chave pública

- Utilização para assinar mensagens



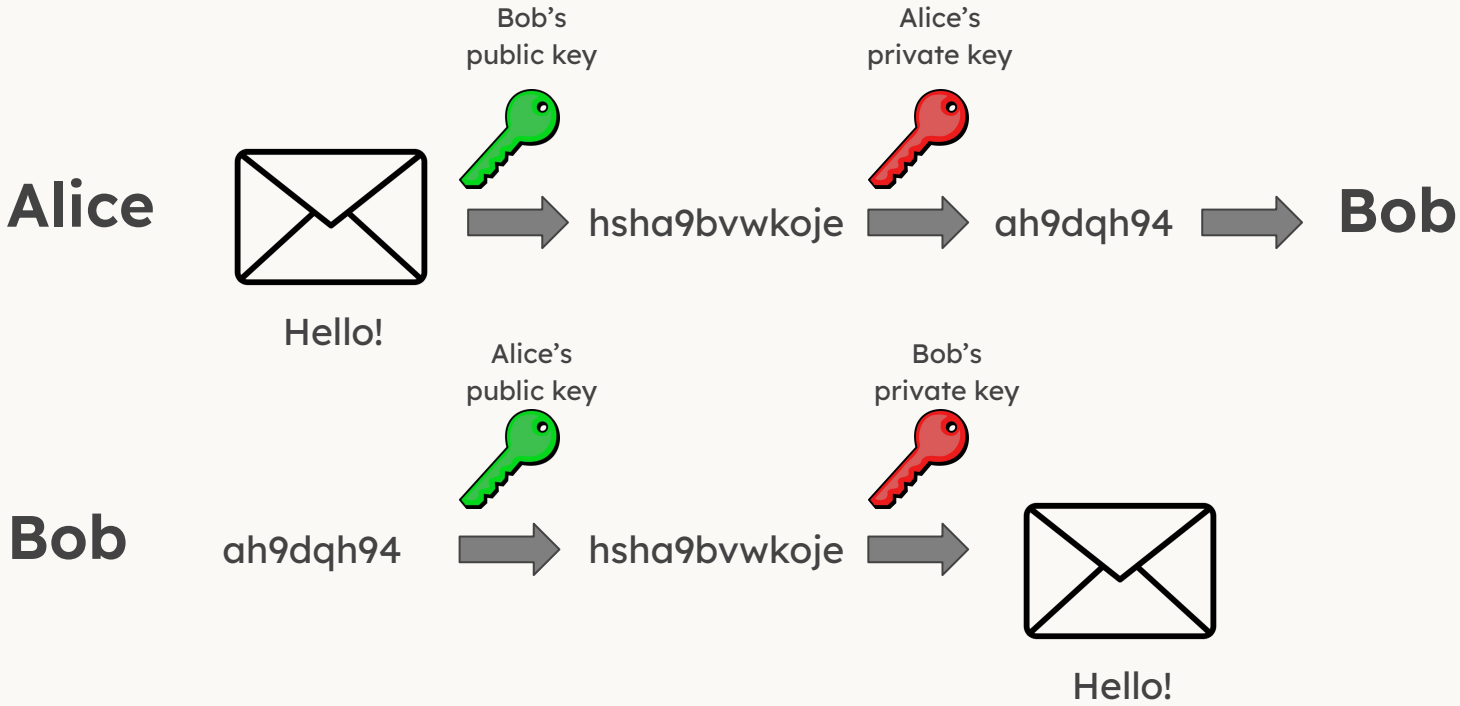
Criptografia de chave pública

- Utilização para criptografar mensagens



Criptografia de chave pública

- Utilização para criptografar e assinar mensagens



ssh secure **sh**ell

- A partir de uma shell local, cria outra shell em outra máquina de forma **remota**
  - comando: `ssh <user>@<endereço>`
  - conecta na porta 22 (TCP)

```
fontoura@nerv:~$ ssh vfa20@ssh.inf.ufpr.br
```

- As principais máquinas do DInf
  - macalan - `servidora de uso geral`
  - orval - `servidora para processamento que utiliza muitos recursos`
  - cpu1 e cpu2 - `servidoras para processamento genérico`

Primeiro acesso

```
fontoura@hubble:~$ ssh vfa20@ssh.inf.ufpr.br
The authenticity of host 'ssh.inf.ufpr.br (2801:82:80ff:8001:216:3eff:fe79:6)' can't be established.
ED25519 key fingerprint is SHA256:2CbvJkwBpGBPMN3FSO1h0lpbSIEUJjFA5sCPuYpQ4/M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ssh.inf.ufpr.br' (ED25519) to the list of known hosts.
vfa20@ssh.inf.ufpr.br's password:
Linux macalan 6.1.0-0.deb11.7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-2~bpo11+1 (2023-04-23) x86_64
================================================================================

macalan (alias ssh) tem poucos recursos de memória e processadores,
com limites rígidos de processos, memória e arquivos abertos.

    *** NÃO DEVE SER USADA PARA PROCESSAMENTO ***

Esta máquina deve ser usada apenas como acesso a outras servidoras.

Use uma das máquinas abaixo para processamento.

Servidoras virtuais:
- cpu1
- cpu2

Servidoras físicas:
- zara (16 cores, 120GB RAM)

Servidoras físicas, com GPUs:
- orval (2x GTX 750 Ti)

* Para usar CUDA, execute:
export PATH=$PATH:/usr/local/cuda/bin

Servidoras de uso exclusivo:
- fradim: exclusiva para professores
- mumm: exclusiva para C3SL

================================================================================
Last login: Thu Nov 30 19:29:19 2023 from 2001:1284:f502:5b8f:d100:94b8:8c7:37f2
vfa20@macalan:~$
```

scp secure file copy

- Copia um arquivo local para uma máquina remota
  - comando: `scp <arquivo> <user>@<endereço>:<caminho>`
- Copia um arquivo remoto para a máquina local
  - comando: `scp <user>@<endereço>:<caminhoDoArquivo> <destinoLocal>`
- Busque usar caminhos absolutos ao executar o `scp`, vai te evitar problemas

3.

Configuração do SSH

config

- Pode-se criar o arquivo *~/.ssh/config*, contendo **configurações gerais** ou para **determinados hosts**
- Por exemplo, caso você tenha que dar **ssh na máquina** com IP 200.17.202.3, é possível adicionar um ***alias***, para que **não seja necessário digitar o IP** em toda conexão
- No DInf, para acessar **qualquer uma das máquinas** dos labs é necessário antes **acessar a *macalan***
- Para contornar isso, é possível descrever uma máquina do lab no arquivo config, adicionando um **ProxyJump na macalan**, desta forma, irá automaticamente se conectar à maquina desejada

config

```
david@dsbd ~ cat .ssh/config
Host *
    SetEnv TERM=xterm-256color

Host macalan
    HostName macalan.c3sl.ufpr.br
    User dlpg21

Host pcdolab
    HostName h10
    User dlpg21
    ProxyJump macalan
```

authorized_keys

- Pode-se adicionar uma lista de **chaves públicas** permitidas no host em *~/.ssh/authorized_keys*
- Assim, ao utilizar o ssh no host utilizando o par de chaves cuja **pública** está no *authorized_keys* do **destino**, não será necessário digitar a senha do usuário, apenas a passphrase da chave privada, **se houver**

Exercício surpresa!!

- O que estes comandos fazem?
  - `sudo apt install curl`
  - `chmod g+r -R <dir>/`
  - `rm {1..10}`
  - `tar -czvf <dir>.tar.gz <dir>/`

4.

Criando chaves ssh

Criando chaves ssh

- Para criar um par de chaves (pública e privada) ssh, utiliza-se o comando `ssh-keygen`

```
ssh-keygen -t ed25519 -C "your_email@example.com"
```

Algoritmo de criptografia

E-mail

Criando chaves ssh

```
dlpg21@macalan:~$ ssh-keygen -t ed25519 -C "dlpg21@inf.ufpr.br"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/bcc/dlpg21/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/bcc/dlpg21/.ssh/id_ed25519
Your public key has been saved in /home/bcc/dlpg21/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:gOZNZGHEl0OAiWV5FxnM6+tseKWZ58pJ3aZZ2UANx/o dlpg21@inf.ufpr.br
The key's randomart image is:
+--[ED25519 256]--+
|   oo*B*+=  ...  |
|  ..+=o O    +.  |
|    o.oo o  ...  |
|   o o ..  ..    |
|    . ..S   ..   |
|        .... +E  |
|       ..*. = .  |
|      .+B..=     |
|       +*++      |
+----[SHA256]-----+
```

Criando chaves ssh

- Os arquivos das chaves serão criados no diretório *~/.ssh* **por padrão**, com a chave pública possuindo a terminação “.pub”
- A **chave privada** deve ser **guardada com segurança**, caso uma pessoa tenha acesso a ela e esta não foi encriptada com uma passphrase, poderá utilizá-la para acessar máquinas que não deveria
- Se foi encriptada, é preciso saber a passphrase para usá-la

```
dlpg21@macalan:~$ ls -lat .ssh | grep id
-rw-------  1 dlpg21 bcc   464 mar  1 12:53 id_ed25519
-rw-------  1 dlpg21 bcc   100 mar  1 12:53 id_ed25519.pub
```

Criando chaves ssh

- Exemplo de conteúdo das chaves pública e privada, respectivamente

```
dlpg21@macalan:~$ cat .ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJuQM2w4ha1Kp9yerD6iDFzU4THAdHl6NrjdXZ2sPlEm dlpg21@inf.ufpr.br
dlpg21@macalan:~$ cat .ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABBdHU7lzi
M4OQVNRycY9mGyAAAAEAAAAAEAAAAzAAAAC3NzaC1lZDI1NTE5AAAAIJuQM2w4ha1Kp9ye
rD6iDFzU4THAdHl6NrjdXZ2sPlEmAAAAoBH49FfijGZP3/HSOOjydHBEoCT1jKreKECafT
NyARvWSpEmAVxsRctJMUgkwPVNoIQlHIxVf78NDvOELUbAVQB/K21my316oRENEQq8FTgr
Icn6G4s+EagR6SQm+LjaCyvT8riQ7WmbnYW85FDii/Q1n3YE3nJ/1zG9XLUNrsMhH/FynB
1WdqOXcayl52y0LEPBPjdi0KLwg0DxaLXZCB8=
-----END OPENSSH PRIVATE KEY-----
```

5.

sshfs

mount & umount

- ***Monta* dispositivos** (USB, HD externo, etc.) em um diretório para poder acessar os arquivos
- Lembre-se, os dispositivos são **representados como arquivos** em /dev
- Ex:
  - `mkdir pendrive && mount /dev/sda1 pendrive`
- Geralmente, os SOs **montam automaticamente**
- Após a utilização, por segurança, deve-se **desmontar o dispositivo**
- Ex:
  - `umount pendrive && rmdir pendrive`

sshfs

- Monta diretórios remotos de outras máquinas na máquina local
  - comando: `sshfs <user>@<endereço>:<caminhoRemoto> <diretórioAlvo>`

- Use `fusermount` para desmontar o diretório
  - comando: `fusermount -u <diretório>`

6.

Comandos legais do ssh

Comandos utilizados durante o ssh

- `whoami` - mostra o nome do usuário no sistema
- `hostname` - mostra o nome do sistema
- `who` - mostra quem mais está conectado no sistema
- `finger` - mostra os detalhes de um usuário no sistema

Exercício surpresa!!

- O que estes comandos fazem?
  - `rm ./*.csv`
  - `ls -l | grep ^d | awk '{print $NF}'`
  - `less <arquivoDeTexto>`
  - `du -hc <dir>`

7.

Exercício em sala

Exercício

1. Crie um arquivo com o nome da sua máquina (ex: h10) na sua home
2. Dê permissão de leitura para os outros usuários (`man chmod`)
3. Use `scp` para copiar o arquivo gerado da máquina do colega ao lado
4. Copie o arquivo para a máquina do colega ao lado usando `SCP`

Exercício

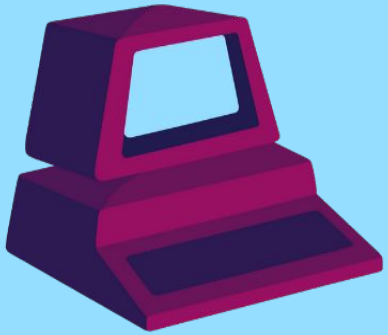
```
$ wget https://www.inf.ufpr.br/dlpg21/linux/misterio.tar.gz
$ tar -xvf misterio.tar.gz
```

Avalie a aula

forms.gle/K9wApqK69b4VRJ5o6

Conta como presença!

Obrigado!



PET
COMPUTAÇÃO

pet.inf.ufpr.br

pet@inf.ufpr.br

@petcompufpr