



Data Science Academy

www.datascienceacademy.com.br

Deep Learning II

Acesso Remoto ao Super Servidor DSA

Siga todas as instruções abaixo para acessar o servidor de Deep Learning da DSA.

Este documento está dividido em 2 seções, de acordo com seu sistema operacional: Windows e MacOSX/Linux.

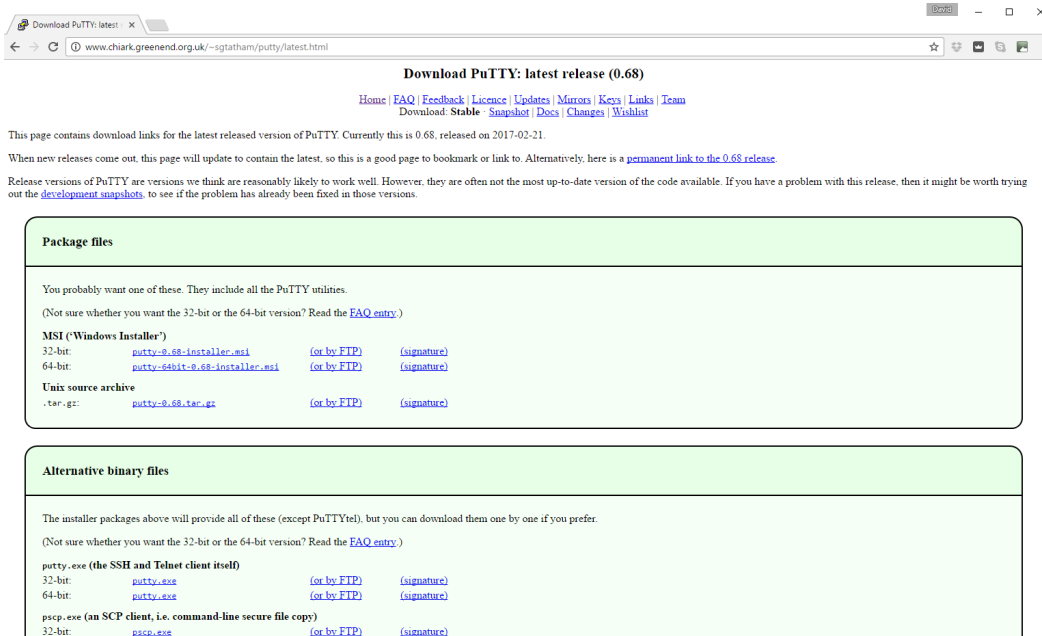
O servidor da DSA é para estudo dos temas abordados ao longo do curso. Utilize o servidor com cuidado e atenção e não armazene arquivos que não sejam relacionados ao curso.

Esse servidor não terá backup e poderá ser reinstalado a qualquer momento para atualização de hardware e/ou de software. Certifique-se de manter uma cópia de todos seus arquivos localmente no seu computador.

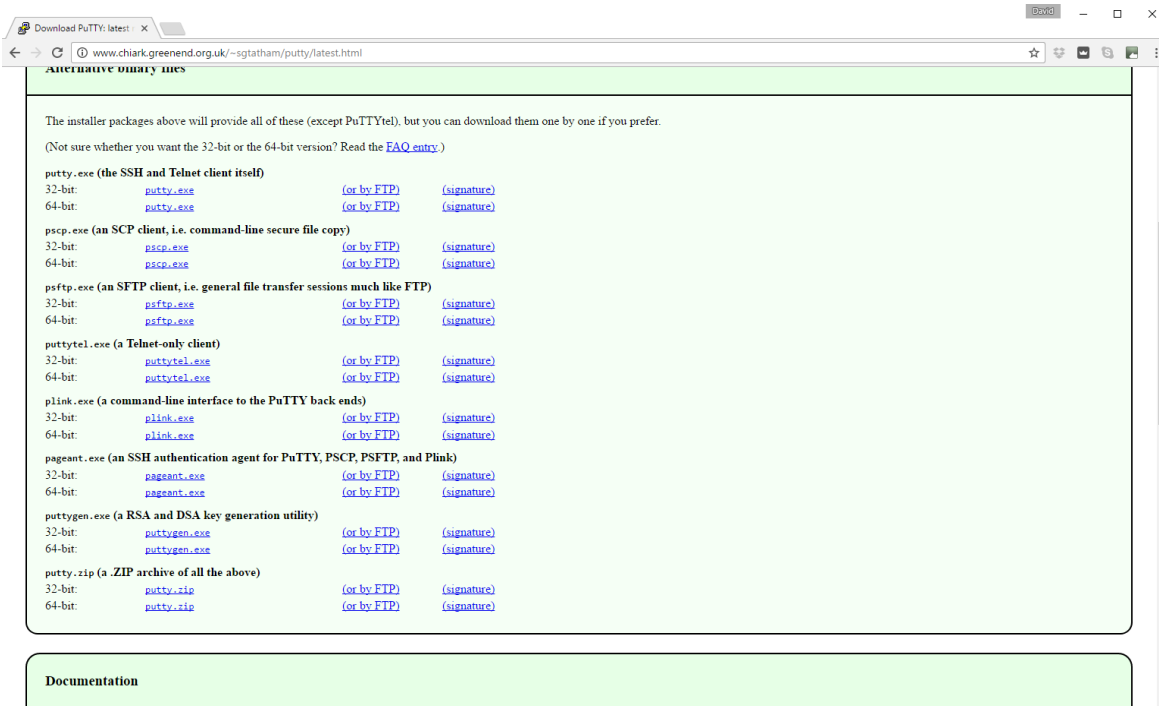
Windows

- 1- Acesse o endereço abaixo e faça o download do putty e puttygen (fique atento à versão de acordo com seu sistema operacional 32 ou 64 bits).

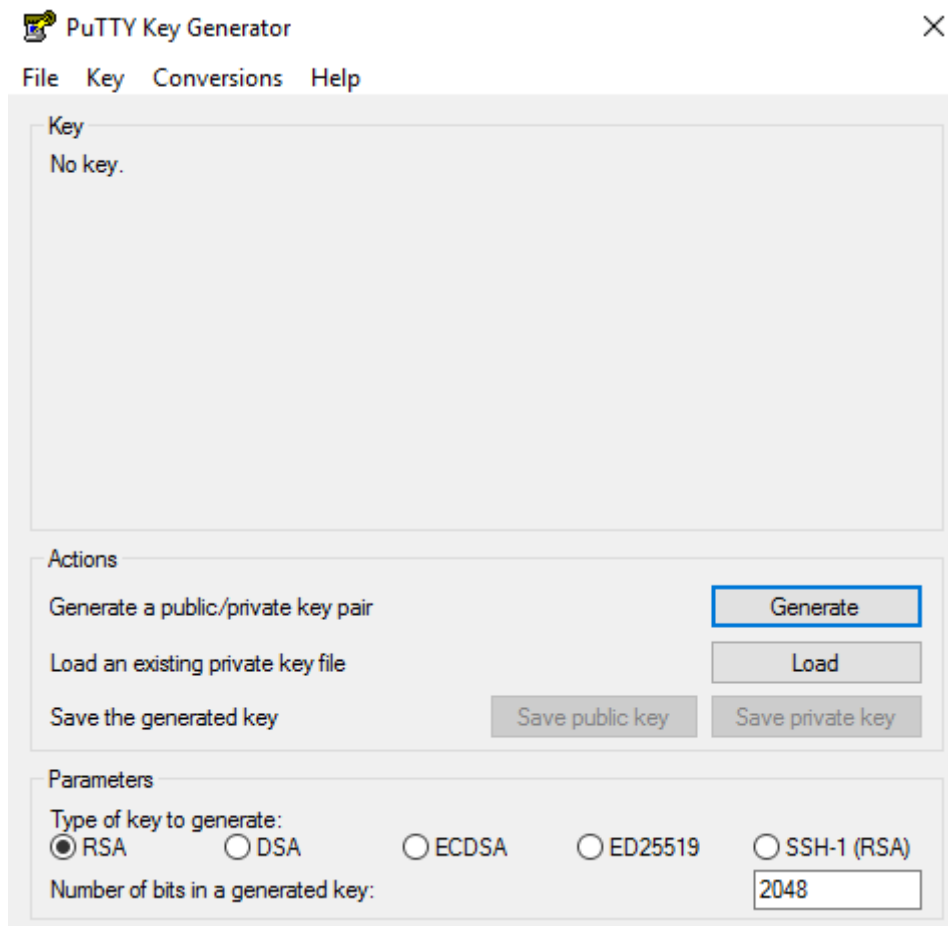
<http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>



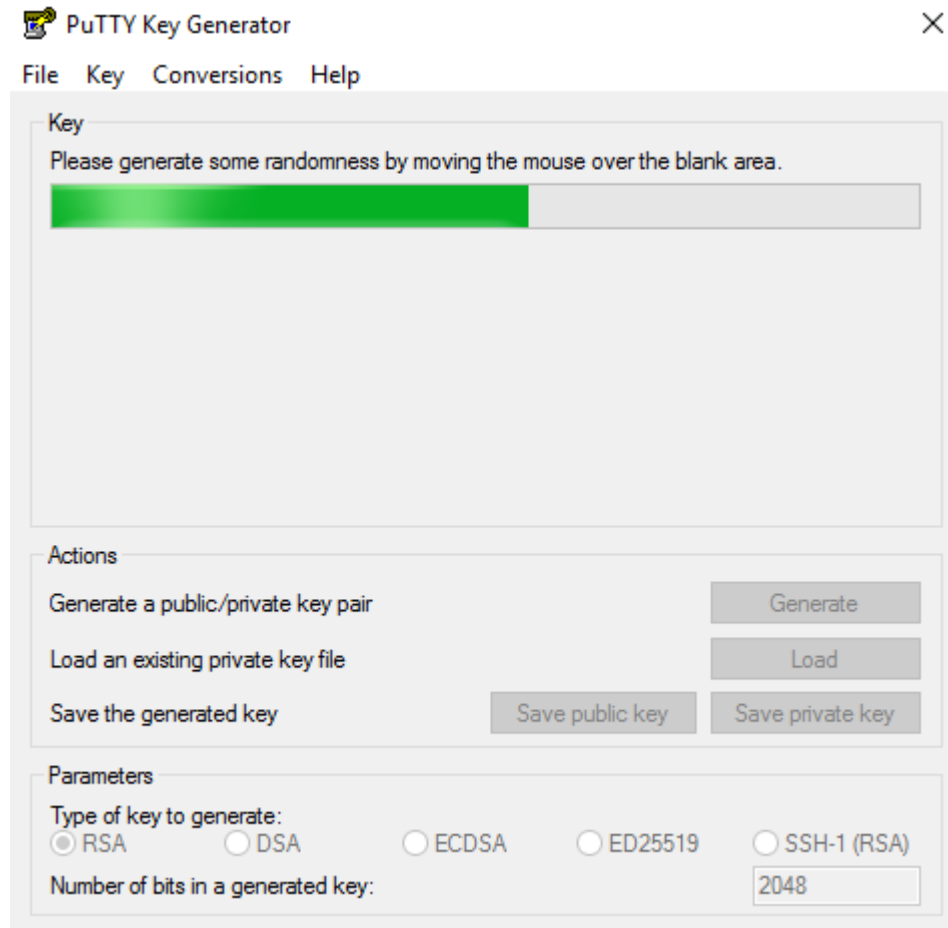
2- Download do puttygen (para gerar as chaves de segurança).



3- Abra o puttygen (2 cliques sobre o executável):

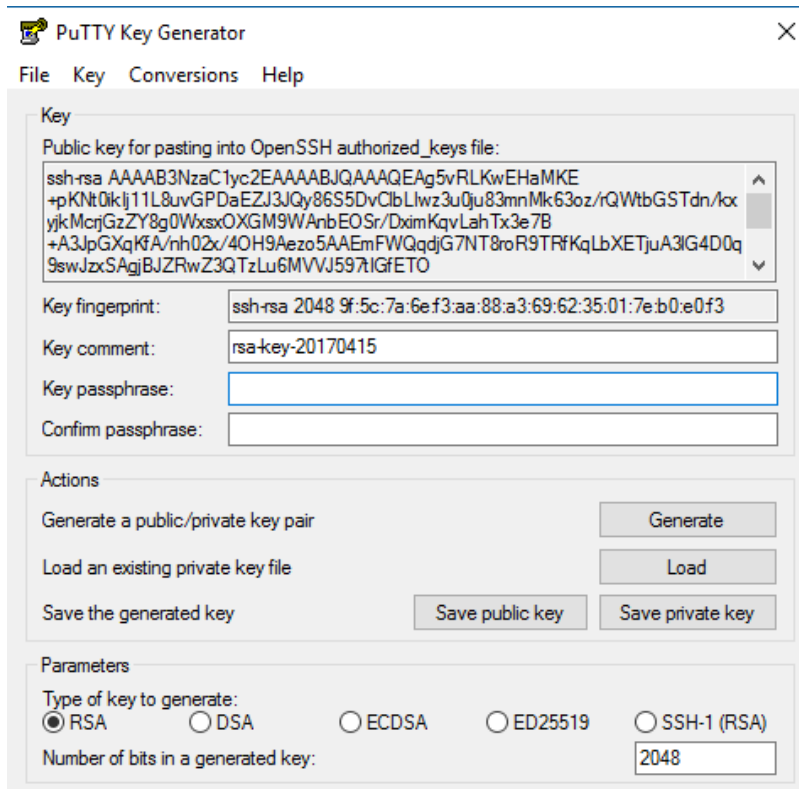


- 4- Clique no botão generate (você precisa ficar “movendo” o mouse enquanto a chave estiver sendo criada, pois a chave randômica é criada de acordo com os movimentos do mouse. Se você não movimentar o mouse, a chave não será criada).



- 5- A chave pública será gerada. Copie a chave inteira, cole no bloco de notas (não use Word ou Wordpad) e salve com o nome: `authorized_keys` (nome do arquivo sem extensão). Não use o botão “Save public key”. Copie e cole a chave pública gerada.

ATENÇÃO: depois de salvar este arquivo, compacte em formato zip e envie por e-mail para suporte@datascienceacademy.com.br. Esse arquivo será copiado para sua pasta de usuário no servidor e permitirá seu acesso remoto. Guarde esse arquivo com segurança.



The screenshot shows the PuTTY Key Generator application window. The 'Key' section displays a public key for pasting into an OpenSSH `authorized_keys` file. The key is an RSA key with a 2048-bit length. The key fingerprint is shown as `ssh-rsa 2048 9f:5c:7a:6e:f3:aa:88:a3:69:62:35:01:7e:b0:e0:f3`. The key comment is `rsa-key-20170415`. The key passphrase and confirm passphrase fields are empty. The 'Actions' section includes buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows the 'Type of key to generate' set to 'RSA' and the 'Number of bits in a generated key' set to '2048'.

Key

Public key for pasting into OpenSSH `authorized_keys` file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA5vRLKwEHAMKE
+pKNt0iklj11L8uvGPDaEZJ3JQy86S5DvClbLlwz3u0ju83mnMk63oz/rQWtbGSTdn/tx
yjkMcrlGzZY8g0WxsxOXGM9WAnbEOsr/DximKqvLahTx3e7B
+A3JpGXqKfA/nh02x/4OH9Aezo5AAEmFWQqdg7NT8roR9TRfKqLbXETjuA3IG4D0q
9swJzxSAgjBJZRwZ3QTzLu6MVVJ597iGfETO
```

Key fingerprint: `ssh-rsa 2048 9f:5c:7a:6e:f3:aa:88:a3:69:62:35:01:7e:b0:e0:f3`

Key comment: `rsa-key-20170415`

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

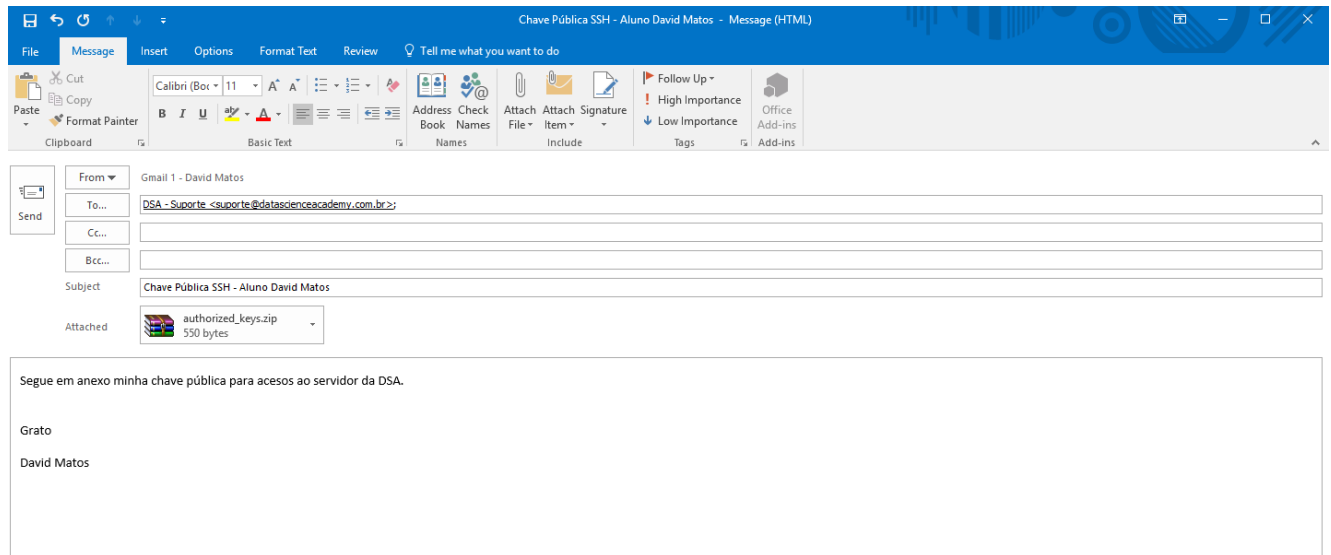
Load an existing private key file

Save the generated key

Parameters

Type of key to generate:
☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

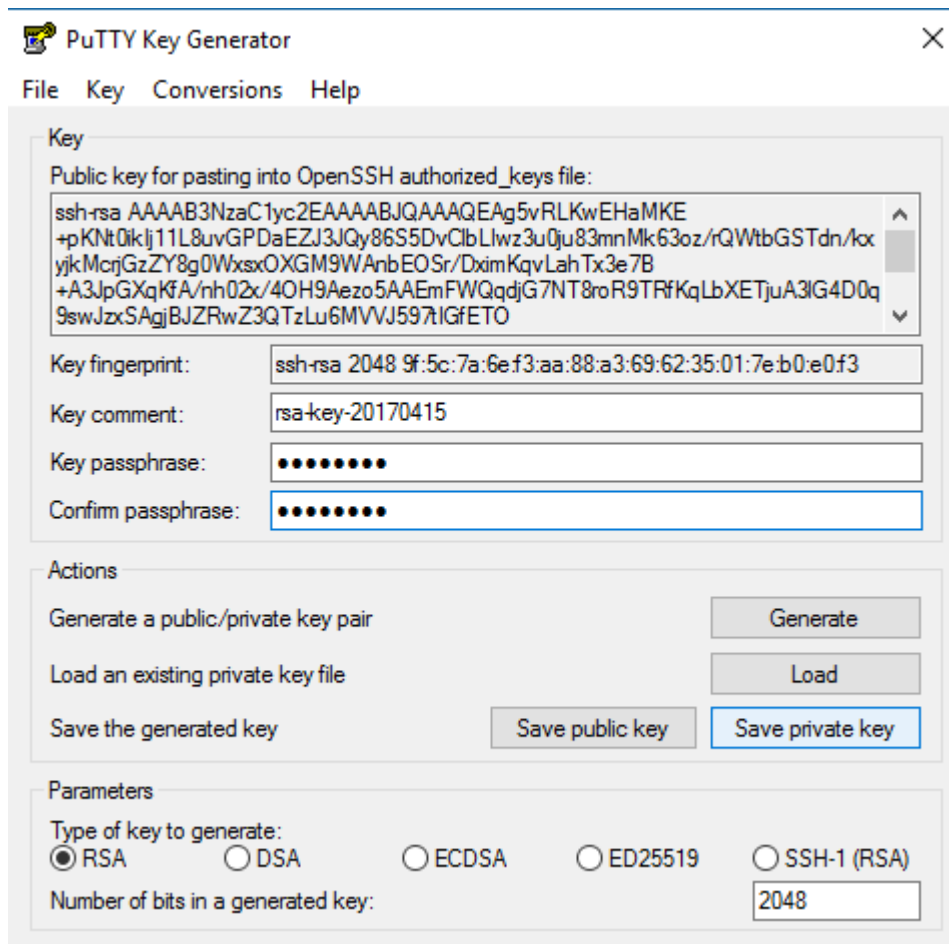
Number of bits in a generated key:



Envie o arquivo por e-mail compactado em formato zip, para evitar que o arquivo seja corrompido

- 6- Em seguida, digite uma senha no campo “Key passphrase” e confirme. Essa senha será usada para login no servidor DSA. Depois de digitar a senha, clique no botão “Save private key”.

Obs: Essa senha ficará guardada no arquivo de chave privada armazenado no seu computador. Ninguém terá acesso a esta senha, nem mesmo nós da DSA.



The screenshot shows the PuTTY Key Generator window. The 'Key' section displays the public key for pasting into the OpenSSH authorized_keys file. The 'Key fingerprint' is shown as 'ssh-rsa 2048 9f:5c:7a:6e:f3:aa:88:a3:69:62:35:01:7e:b0:e0:f3'. The 'Key comment' is 'rsa-key-20170415'. The 'Key passphrase' and 'Confirm passphrase' fields are both filled with dots. The 'Actions' section has buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows 'Type of key to generate' set to 'RSA' and 'Number of bits in a generated key' set to '2048'.

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA5vRLKwEHAMKE
+pKNt0iklj11L8uvGPDaEZJ3JQy86S5DvClbLlwz3u0ju83mnMk63oz/rQWtbGSTdn/kc
yjkMcrgZzZY8g0WxsxOXGM9WAnbEOSr/DximKqvLahTx3e7B
+A3JpGXqKfA/nh02x/4OH9Aezo5AAEmFWQqdjG7NT8roR9TRfKqLbXETjuA3IG4D0q
9swJzxSAgjBJZRwZ3QTzLu6MVVJ597IGfETO
```

Key fingerprint: ssh-rsa 2048 9f:5c:7a:6e:f3:aa:88:a3:69:62:35:01:7e:b0:e0:f3

Key comment: rsa-key-20170415

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

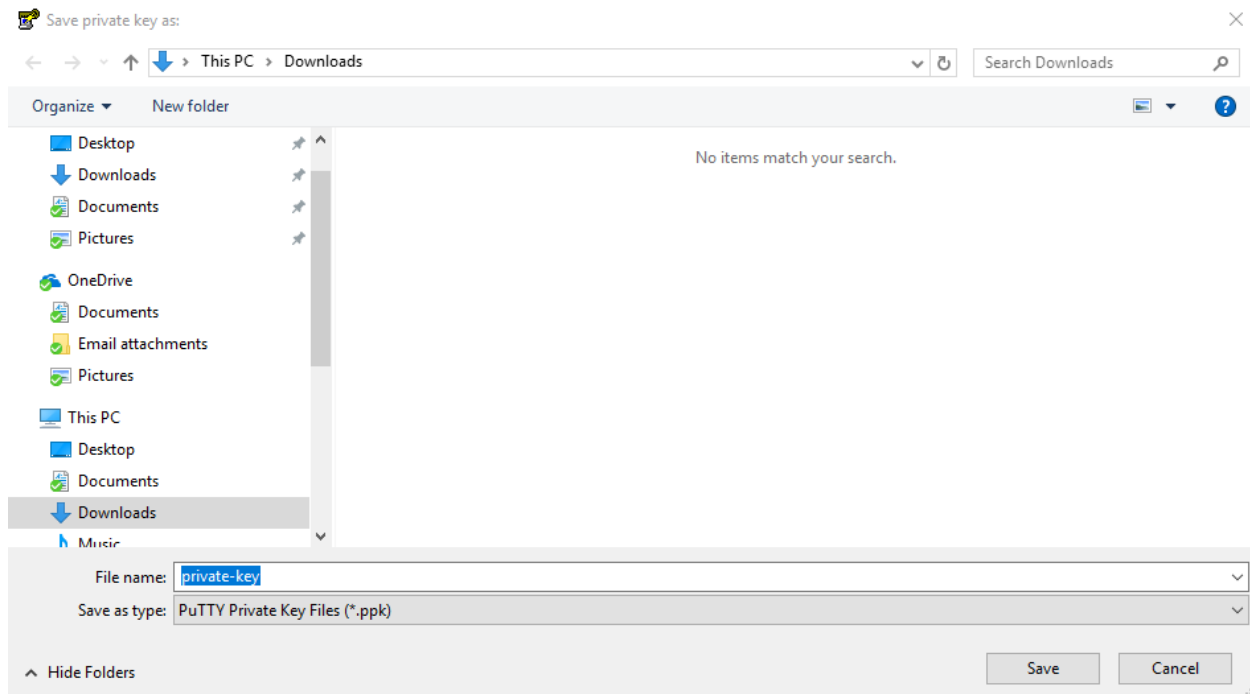
Save the generated key Save public key Save private key

Parameters

Type of key to generate:
☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

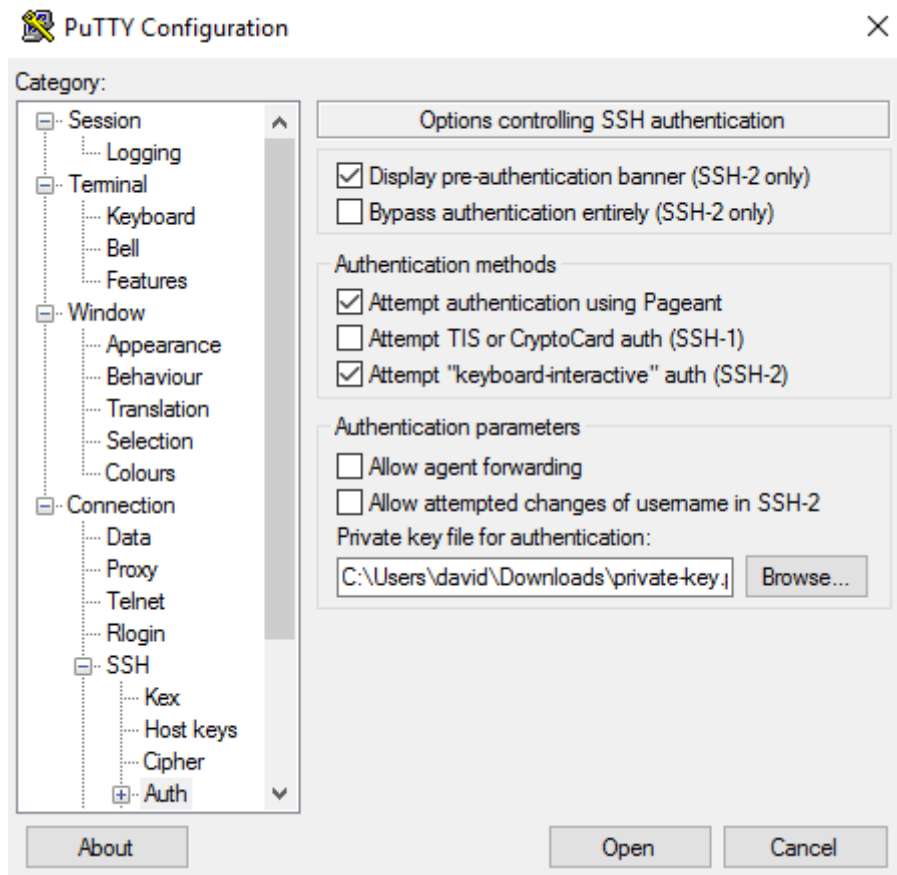
Number of bits in a generated key: 2048

7- Salve o arquivo com o nome que preferir. Sugerimos: **private-key.ppk**.



Isso finaliza a configuração com o puttygen. Pode fechar o aplicativo!

- 8- Abra o putty (você pode colocar o executável onde preferir, pois não há instalação. Sugerimos colocar o arquivo no seu desktop). No menu à esquerda, clique em **Connection – SSH – Auth**. Na caixa Private Key file for authentication, clique no botão browse e selecione a private-key criada no passo anterior.

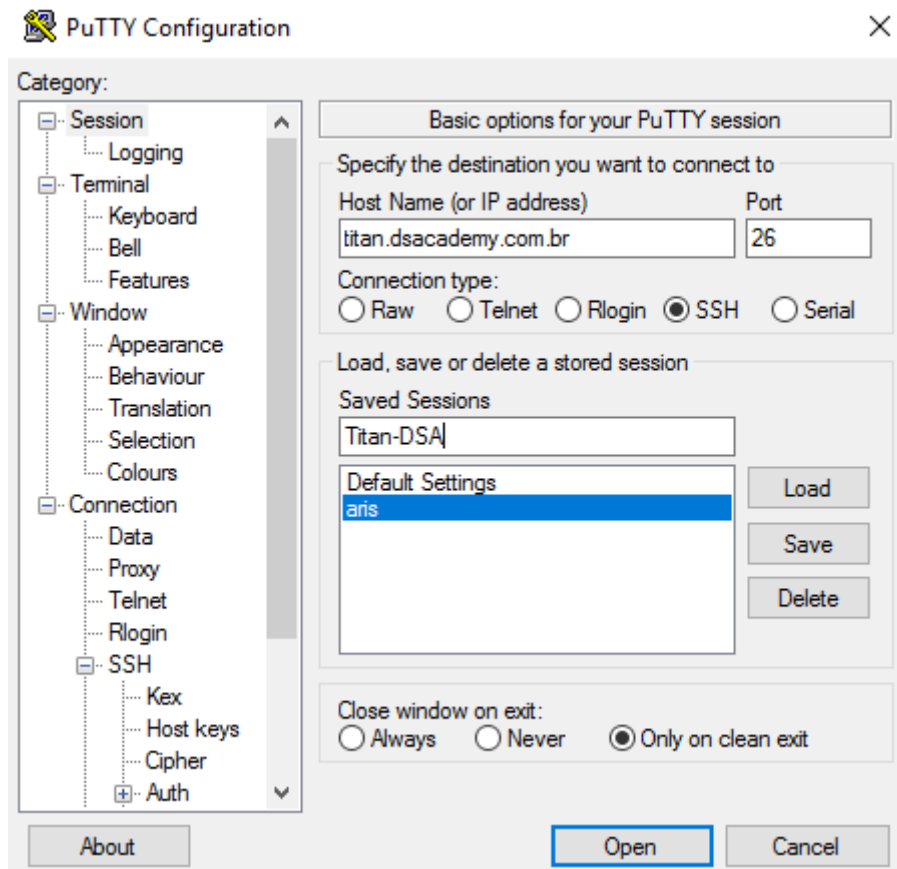


- 9- No menu à esquerda, clique em Session. Preencha os dados de acesso ao servidor e clique em salvar. Dê o nome que preferir, sugerimos: Titan-DSA.

Servidor: **titan.dsacademy.com.br**

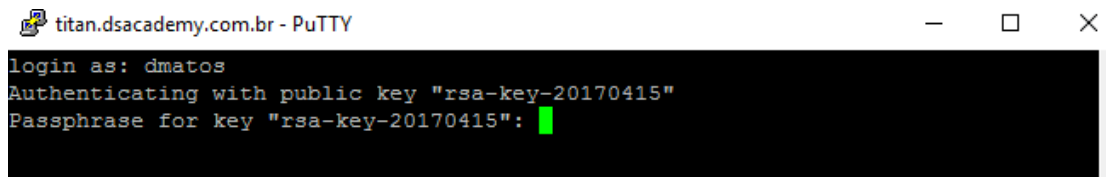
Port: **26**

Connection Type: **SSH**



- 10- Clique no botão Open e digite seu usuário de acesso e a senha que você configurou no puttygen.

ATENÇÃO: você receberá seu usuário de acesso depois de enviar a chave de segurança.



```
titan.dsacademy.com.br - PuTTY
login as: dmatos
Authenticating with public key "rsa-key-20170415"
Passphrase for key "rsa-key-20170415": █
```

11- Login efetuando com sucesso!

```
dmatos@titan: ~  
login as: dmatos  
Authenticating with public key "rsa-key-20170415"  
Passphrase for key "rsa-key-20170415":  
  
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-39-generic x86_64)  
  
* Bem-vindo ao Supercomputador de Deep Learning da Data Science Academy  
* Utilize este computador para suas atividades ao longo dos cursos da Formação Inteligência Artificial  
* Suporte: http://www.datascienceacademy.com.br  
  
9 packages can be updated.  
0 updates are security updates.  
  
Last login: Sat Apr 15 17:02:25 2017 from 192.168.1.1  
dmatos@titan:~$
```

Comece instalando o Anaconda Python. Para fazer o download digite:

wget https://repo.continuum.io/archive/Anaconda3-4.3.1-Linux-x86_64.sh

E em seguida, instale o Anaconda, com o comando abaixo. A instalação deve ser feita no seu diretório home: /home/user/anaconda3

bash Anaconda3-4.3.1-Linux-x86_64.sh

Você tem acesso completo no seu diretório home. Para copiar arquivos para o servidor faça o download e configure o WinSCP (<https://winscp.net/eng/download.php>).

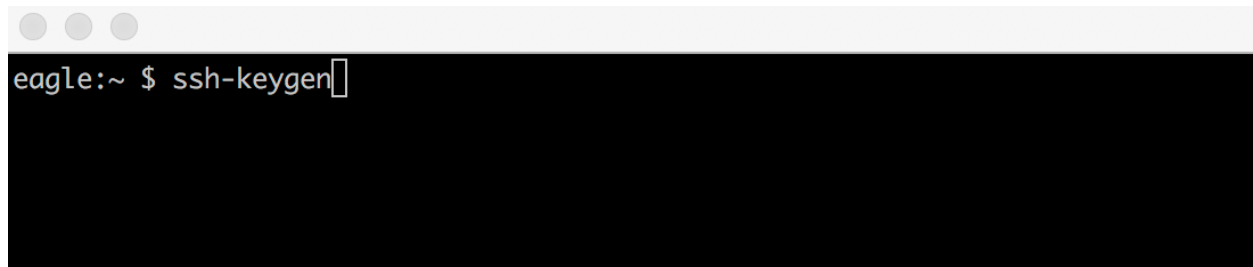
CUDA e cuDNN já estarão instalados no servidor (você precisa configurar as suas variáveis de ambiente). Você também poderá usar o Docker e Nvidia-Docker no servidor DSA.

Bons estudos!

Equipe DSA

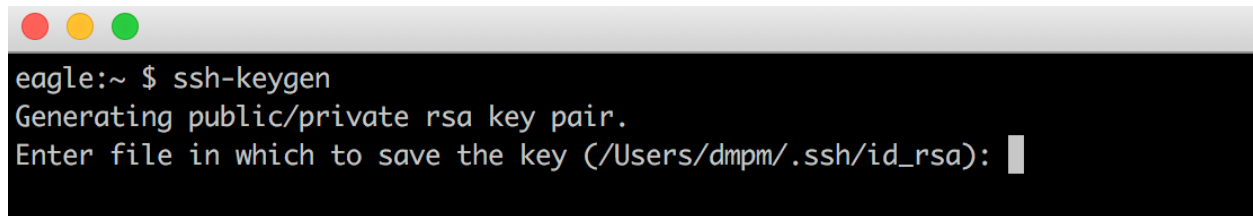
MacOSX / Linux

- 1- Abra o terminal e digite **ssh-keygen** para gerar sua chave de segurança.

A screenshot of a terminal window with a light gray title bar containing three window control buttons. The terminal background is black, and the text is white. The prompt 'eagle:~ \$' is followed by the command 'ssh-keygen' and a cursor. The rest of the terminal area is empty.

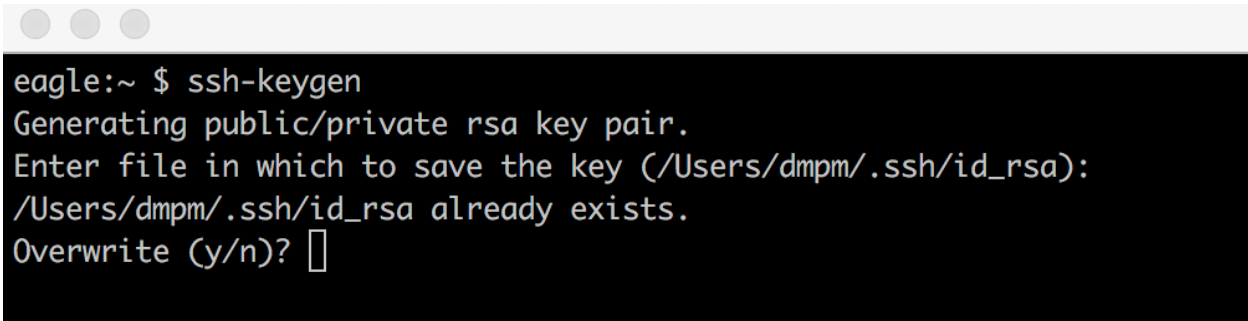
```
eagle:~ $ ssh-keygen
```

2- Pressione enter para confirmar o diretório onde serão salvos os arquivos.

A terminal window with a dark background and light gray text. The window has a title bar with three colored circles (red, yellow, green) on the left. The text inside the terminal reads: eagle:~ \$ ssh-keygen, followed by a new line, Generating public/private rsa key pair., followed by another new line, and Enter file in which to save the key (/Users/dmpm/.ssh/id_rsa): followed by a white cursor bar.

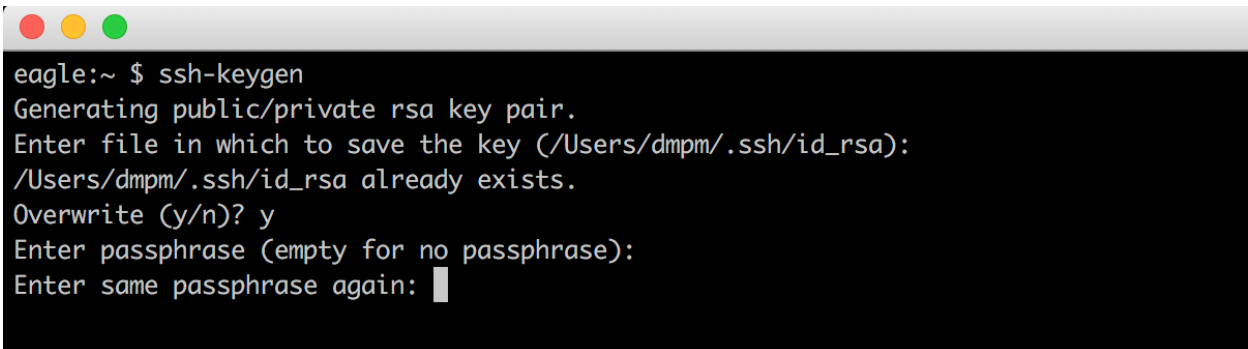
```
eagle:~ $ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/dmpm/.ssh/id_rsa):
```


- 3- Caso você já tenha alguma chave no diretório, você receberá uma mensagem para sobrescrever. Certifique-se de salvar qualquer arquivo antes de realizar o procedimento.

A terminal window with a dark background and light text. The window has three small circles in the top-left corner, representing window control buttons. The text inside the terminal shows the execution of the 'ssh-keygen' command, followed by prompts and messages indicating that a key pair is being generated and that an existing file will be overwritten.

```
eagle:~ $ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/dmpm/.ssh/id_rsa):
/Users/dmpm/.ssh/id_rsa already exists.
Overwrite (y/n)? ☐
```

- 4- Digite a senha e confirme. Essa senha será usada para efetuar login no servidor.

A terminal window with a dark background and a light gray title bar containing three colored window control buttons (red, yellow, green). The terminal text is as follows:

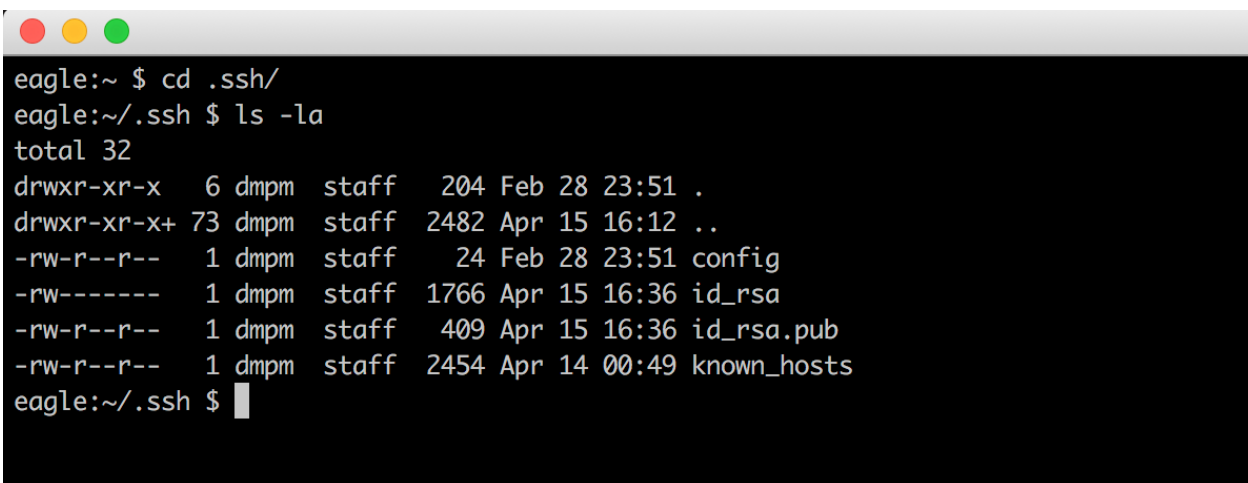
```
eagle:~ $ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/dmpm/.ssh/id_rsa):
/Users/dmpm/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again: █
```

5- Serão gerados 2 arquivos:

`id_rsa` (chave privada)

`id_rsa.pub` (chave pública)

ATENÇÃO: depois de gerar os arquivos, compacte o arquivo com a chave pública em formato zip e envie por e-mail para suporte@datascienceacademy.com.br. Esse arquivo será copiado para sua pasta de usuário no servidor e permitirá seu acesso remoto. Guarde esse arquivo com segurança.

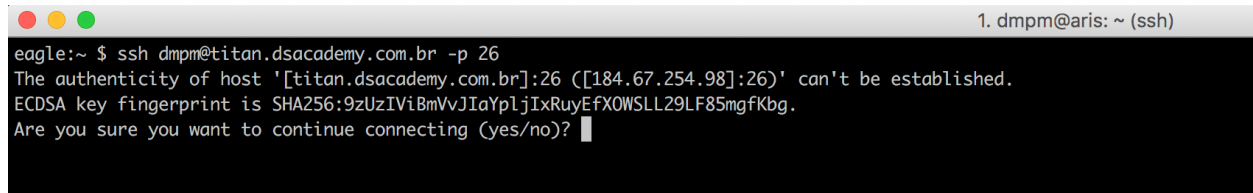


```
eagle:~ $ cd .ssh/  
eagle:~/ssh $ ls -la  
total 32  
drwxr-xr-x  6 dmpm  staff   204 Feb 28 23:51 .  
drwxr-xr-x+ 73 dmpm  staff  2482 Apr 15 16:12 ..  
-rw-r--r--  1 dmpm  staff    24 Feb 28 23:51 config  
-rw-----  1 dmpm  staff  1766 Apr 15 16:36 id_rsa  
-rw-r--r--  1 dmpm  staff   409 Apr 15 16:36 id_rsa.pub  
-rw-r--r--  1 dmpm  staff  2454 Apr 14 00:49 known_hosts  
eagle:~/ssh $
```

6- Depois de enviar o arquivo do item anterior, você receberá seu usuário de acesso. Para efetuar login, digite no terminal:

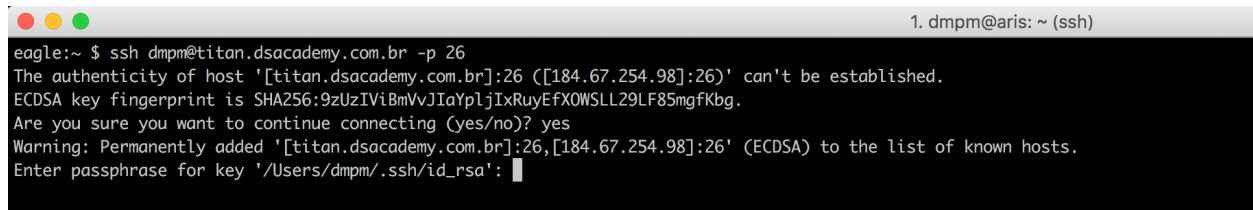
ssh user@titan.dsacademy.com.br -p 26

No primeiro acesso será solicitado a confirmação da chave. Digite yes e pressione enter.

A screenshot of a terminal window with a dark background. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left and the text '1. dmpm@aris: ~ (ssh)' on the right. The terminal text shows a user at a prompt 'eagle:~ \$' typing the command 'ssh dmpm@titan.dsacademy.com.br -p 26'. The output shows a warning about the host's authenticity, an ECDSA key fingerprint, and a prompt asking for confirmation to continue connecting. The cursor is positioned at the end of the prompt line.

```
eagle:~ $ ssh dmpm@titan.dsacademy.com.br -p 26
The authenticity of host '[titan.dsacademy.com.br]:26 ([184.67.254.98]:26)' can't be established.
ECDSA key fingerprint is SHA256:9zUzIViBmVvJIaYpljIxRuyEfXOWSLL29LF85mgfKbg.
Are you sure you want to continue connecting (yes/no)?
```

7- Digite a senha.



```
eagle:~ $ ssh dmpm@titan.dsacademy.com.br -p 26
1. dmpm@aris: ~ (ssh)
The authenticity of host '[titan.dsacademy.com.br]:26 ([184.67.254.98]:26)' can't be established.
ECDSA key fingerprint is SHA256:9zUzIViBmVvJIaYpljIxRuyEfxOWSLL29LF85mgfKbg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[titan.dsacademy.com.br]:26,[184.67.254.98]:26' (ECDSA) to the list of known hosts.
Enter passphrase for key '/Users/dmpm/.ssh/id_rsa':
```

8- Login efetuado com sucesso!

```
1. dmpm@titan: ~ (ssh)
eagle:~ $ ssh dmpm@titan.dsacademy.com.br -p 26
The authenticity of host '[titan.dsacademy.com.br]:26 ([184.67.254.98]:26)' can't be established.
ECDSA key fingerprint is SHA256:9zUzIViBmVvJJaYpljIxRuyEfXOWSLL29LF85mgfKbg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[titan.dsacademy.com.br]:26,[184.67.254.98]:26' (ECDSA) to the list of known hosts.
Enter passphrase for key '/Users/dmpm/.ssh/id_rsa':

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-39-generic x86_64)

 * Bem-vindo ao Supercomputador de Deep Learning da Data Science Academy
 * Utilize este computador para suas atividades ao longo dos cursos da Formação Inteligência Artificial
 * Suporte: http://www.datascienceacademy.com.br

9 packages can be updated.
0 updates are security updates.

Last login: Fri Apr 14 23:59:17 2017 from 192.168.1.139
dmpm@titan:~$
```

Comece instalando o Anaconda Python. Para fazer o download digite:

wget https://repo.continuum.io/archive/Anaconda3-4.3.1-Linux-x86_64.sh

E em seguida, instale o Anaconda, com o comando abaixo. A instalação deve ser feita no seu diretório home: /home/user/anaconda3

bash Anaconda3-4.3.1-Linux-x86_64.sh

Você tem acesso completo no seu diretório home. Para copiar arquivos para o servidor use o comando scp.

CUDA e cuDNN já estarão instalados no servidor (você precisa configurar as suas variáveis de ambiente). Você também poderá usar o Docker e Nvidia-Docker no servidor DSA.

Bons estudos!

Equipe DSA