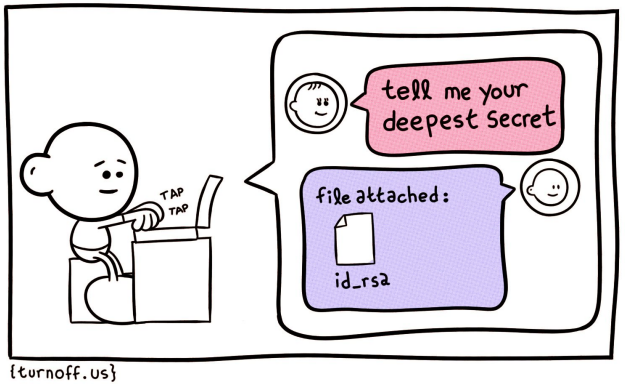


Nuvem e Acesso Remoto

Paulo Ricardo Lisboa de Almeida

DSBD

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

Um pouco de criptografia

Desejamos **cifrar** nossas mensagens.

> Qualquer um que as intercepte não vai saber o que está escrito.

Para isso, utilizamos um algoritmo de cifragem.

Encriptação ou Cifragem

Encriptar (cifrar) uma mensagem a transforma em algo ilegível para quem não tem a chave de descriptografia.

Vantagens:

- Confidencialidade: a mensagem só pode ser lida pelos recipientes desejados.
- Integridade: é muito difícil modificar a mensagem sem que isso seja detectado.
- Não repúdio: é possível validar a autenticidade da mensagem (é difícil forjar que X enviou uma mensagem).

Como as coisas funcionam

Desejamos cifrar a mensagem.

Transformar em algo que ninguém, exceto quem desejamos, possa ler.

Alice 

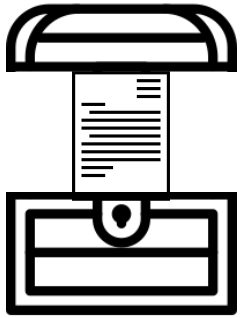
Rede Pública 

 Bob

Como as coisas funcionam

Cifrar a mensagem é colocar ela em um “baú” antes de enviar. Fechamos o baú com uma **chave**.

Alice



Rede Pública

Bob

Como as coisas funcionam

Cifrar a mensagem é colocar ela em um “baú” antes de enviar. Fechamos o baú com uma **chave**.

Alice

Rede Pública

Bob

Como as coisas funcionam

Enviamos pela rede.

Alice

Rede Pública

Bob

Como as coisas funcionam

Mas e agora, como Bob vai abrir o Baú?

Alice

Rede Pública

Bob

Como as coisas funcionam

Primeira opção. Bob já tinha a chave, que passamos a ele em outra ocasião (e.g., em uma rede privada).

O nome disso é **criptografia simétrica**.

Alice 

Rede Pública 

 Bob

Como as coisas funcionam

Primeira opção. Bob já tinha a chave, que passamos a ele em outra ocasião (e.g., em uma rede privada).

Funciona, mas muitas vezes não é prático. Precisamos primeiro estabelecer uma “rede privada”.

Alice 

Rede Pública 

 Bob

Como as coisas funcionam

Enviar a chave pela rede **não** é uma opção!

Alice

Rede Pública

Bob

Como as coisas funcionam

Vamos criar um “Baú” particularmente estranho.

Ele pode ser **fechado** com uma **chave azul**, mas só pode ser **aberto** com uma **chave vermelha**.

Alice 

 Rede Pública

 Bob

Como as coisas funcionam

Bob tem as duas chaves.

Alice 

Rede Pública 


Bob

Como as coisas funcionam

Bob envia a **chave azul** para Alice.

A chave azul serve para fechar um baú, mas não o abre. Essa é a **chave pública**.

Alice

Rede Pública

Bob

Como as coisas funcionam

Bob envia a **chave azul** para Alice.

A chave azul serve para fechar um baú, mas não o abre. Essa é a **chave pública**.

Alice

Rede Pública

Bob

Como as coisas funcionam

Bob envia a **chave azul** para Alice.

A chave azul serve para fechar um baú, mas não o abre. Essa é a **chave pública**.

Alice

Rede Pública

Bob

Como as coisas funcionam

Alice usa a **chave pública** de Bob para cifrar a mensagem.

Alice

Rede Pública

Bob

Como as coisas funcionam

Alice usa a **chave pública** de Bob para cifrar a mensagem.

Alice

Rede Pública

Bob

Como as coisas funcionam

A mensagem **cifrada** é enviada para Bob.

Alice

Rede Pública

Bob

Como as coisas funcionam

A mensagem **cifrada** é enviada para Bob.

Alice

Rede Pública

Bob

Como as coisas funcionam

Bob é o único que tem a **chave vermelha**, capaz de abrir a mensagem.

Chave **privada**.

Alice

Rede Pública

Bob

Como as coisas funcionam

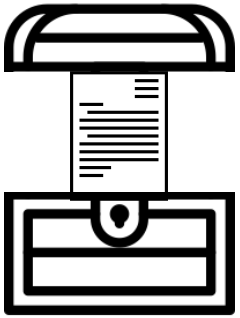
Bob é o único que tem a **chave vermelha**, capaz de abrir a mensagem.

Chave **privada**.

Alice

Rede Pública

Bob



Criptografia de chave pública

Essa forma de criptografia é chamada de:

Criptografia de chave pública, ou

Criptografia assimétrica.

Existem duas chaves, uma **pública** e uma **privada**.

Criptografia de chave pública

Essa forma de criptografia é chamada de:

Criptografia de chave pública, ou

Criptografia assimétrica.

Existem duas chaves, uma **pública** e uma **privada**.

Essa é a ideia por trás de toda comunicação segura que você faz na internet:

HTTPS, SSH, TLS, ...

Criptografia de chave pública

As chaves públicas e privadas podem ser vistas como sequências numéricas.

Funções matemáticas são usadas para compor uma mensagem cifrada a partir de uma chave pública.

$f(p, x) = c$ é uma função que cifra a mensagem x usando uma chave pública p, gerando a mensagem cifrada c.

Criptografia de chave pública

As chaves públicas e privadas podem ser vistas como sequências numéricas.

Funções matemáticas são usadas para compor uma mensagem cifrada a partir de uma chave pública.

$f(p, x) = c$ é uma função que cifra a mensagem x usando uma chave pública p, gerando a mensagem cifrada c.

$g(r, c) = x$ é uma função que decifra a mensagem c de volta para x, usando a chave privada r.

RSA

O algoritmo RSA - criado por, **R**on Rivest, Adi **S**hamir e Leonard **A**dleman é comumente usado para fazer a transmissão segura de dados.

Usa operações de módulo.

Exemplos:

10 mod 3 = 1

20 mod 7 = 6

RSA

O algoritmo possui duas fases:

1. Escolher as chaves pública e privada
2. Cifrar e decifrar as mensagens

Gerando as Chaves

1. Escolha dois números primos grandes, p e q.

    Quanto maiores p e q:

    + Mais seguro.

    - Computacionalmente mais caro cifrar/decifrar.

Gerando as Chaves

1. Escolha dois números primos grandes, p e q.

   Quanto maiores p e q:

   + Mais seguro.

   - Computacionalmente mais caro cifrar/decifrar.

2. Compute $n = pq$ e $z = (p - 1)(q - 1)$.

Gerando as Chaves

1. Escolha dois números primos grandes, p e q.

   Quanto maiores p e q:

   + Mais seguro.

   - Computacionalmente mais caro cifrar/decifrar.

2. Compute $n = pq$ e $z = (p - 1)(q - 1)$.
3. Escolha um número $e < n$, tal que e e z não possuem fatores comuns, exceto o 1.

Gerando as Chaves

1. Escolha dois números primos grandes, p e q.

   Quanto maiores p e q:

   + Mais seguro.

   - Computacionalmente mais caro cifrar/decifrar.

2. Compute $n = pq$ e $z = (p - 1)(q - 1)$.
3. Escolha um número $e < n$, tal que e e z não possuem fatores comuns, exceto o 1.
4. Encontre um número d, de forma que $ed - 1 \bmod z = 0$.

   Ou, de outra forma, ed mod z = 1.

Gerando as Chaves

1. Escolha dois números primos grandes, p e q.

   Quanto maiores p e q:

   + Mais seguro.

   - Computacionalmente mais caro cifrar/decifrar.

2. Compute $n = pq$ e $z = (p - 1)(q - 1)$.
3. Escolha um número $e < n$, tal que e e z não possuem fatores comuns, exceto o 1.
4. Encontre um número d, de forma que $ed - 1 \bmod z = 0$.

   Ou, de outra forma, ed mod z = 1.

5. As chaves são:
   a. Chave pública: (n, e);
   b. Chave privada: (n, d).

Cifrando e decifrando

Chave pública: (n, e);

Chave privada: (n, d).

Suponha um único caractere (ou um bloco de bits) *m*.

Cifrar: $c = m^e \bmod n$

Decifrar: $m = c^d \bmod n$

Um exemplo

Suponha $p=5$ e $q=7$.

$n = pq = ?$

$z = (p - 1)(q - 1) = ?$

Um exemplo

Suponha $p=5$ e $q=7$.

$n = pq = 35$

$z = (p - 1)(q - 1) = 24$

$e = 5$

$d = 29$ já que $(5*29 - 1 \bmod 24) = 0$

Chave pública (35,5).

Chave privada (35,29).

Cifrar

Chave pública (35,5).

Texto	m^e	Cifrado $c = m^e \bmod n$
D (3)	243	33
S (18)	1889568	23
B (1)	1	1
D (3)	243	33

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Decifrar

Chave pública (35,5).

Texto	m^e	Cifrado $c = m^e \bmod n$
D (3)	243	33
S (18)	1889568	23
B (1)	1	1
D (3)	243	33

Chave privada (35,29).

Cifrado $c = m^e \bmod n$	Decifrado $m = c^d \bmod n$
33	D (3)
23	S (18)
1	B (1)
33	D (3)

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Detalhes

Escolhemos p e q pequenos para simplificar as contas.

Em aplicações seguras, recomenda-se números primos com pelo menos 1024 bits.

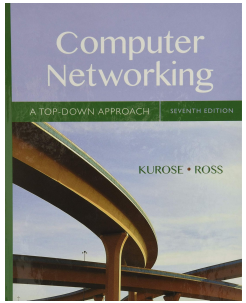
A “segurança” está no fato de **não existir um algoritmo conhecido eficiente** para se fatorar um número *n* em seus primos *p* e *q*.

Ficou curioso?

Assista a esse vídeo:

How Quantum Computers Break The Internet... Starting Now
https://youtu.be/-UrdExQW0cs

Veja uma discussão sobre o RSA, e a prova dele conseguir cifrar e decifrar mensagens em Kurose (2013).



Mais detalhes

A criptografia assimétrica (de chave pública e privada) é computacionalmente custosa.

Mais detalhes

A criptografia assimétrica (de chave pública e privada) é computacionalmente custosa.

O que geralmente se faz é:

1. Estabelecer um meio de comunicação seguro entre os pares através de uma criptografia assimétrica.

Mais detalhes

A criptografia assimétrica (de chave pública e privada) é computacionalmente custosa.

O que geralmente se faz é:

1. Estabelecer um meio de comunicação seguro entre os pares através de uma criptografia assimétrica.
2. Usar esse meio para trocar uma chave de criptografia **simétrica**.

Mais detalhes

A criptografia assimétrica (de chave pública e privada) é computacionalmente custosa.

O que geralmente se faz é:

1. Estabelecer um meio de comunicação seguro entre os pares através de uma criptografia assimétrica.
2. Usar esse meio para trocar uma chave de criptografia **simétrica**.
3. Usar criptografia simétrica para se comunicar.

No Linux

No Linux, o par de chaves públicas e privadas geralmente fica no diretório `/home/seu_usuario/.ssh`

Entre nesse diretório:

```
cd /home/seu_usuario/.ssh
```

No Linux

No Linux, o par de chaves públicas e privadas geralmente fica no diretório `/home/seu_usuario/.ssh`

Entre nesse diretório:

```
cd /home/seu_usuario/.ssh
```

Dentro do diretório devem existir os arquivos *id_rsa* e id_rsa.pub, **caso não existam**, você vai precisar gerar as chaves pública e privada.

```
ssh-keygen -t rsa
```

Quando perguntado, indique que você quer armazenar a chave no diretório padrão. Coloque uma senha quando perguntado.

No Linux

O arquivo ***id_rsa.pub*** é sua **chave pública**.

Você pode compartilhar esse arquivo sem problemas.

Abra o arquivo e veja seu conteúdo:

```
cat id_rsa.pub
```

No Linux

O arquivo ***id_rsa.pub*** é sua **chave pública**.

Você pode compartilhar esse arquivo sem problemas.

Abra o arquivo e veja seu conteúdo:

```
cat id_rsa.pub
```

O arquivo **id_rsa** é sua **chave privada**.

Nunca compartilhe esse arquivo.

Faça você mesmo

Vamos criptografar uma mensagem.

Vamos usar o Openssl (só porque é mais fácil).

Crie um diretório vazio em um local qualquer, e abra um terminal apontando para esse diretório.

Faça você mesmo

Crie um diretório vazio em um local qualquer, e abra um terminal apontando para esse diretório.

Digite os comandos:

```
openssl genrsa -out chave_privada.pem 1024
openssl rsa -in chave_privada.pem -pubout -out chave_publica.pem
```

Faça você mesmo

Crie um diretório vazio em um local qualquer, e abra um terminal apontando para esse diretório.

Digite os comandos:

```
openssl genrsa -out chave_privada.pem 1024
openssl rsa -in chave_privada.pem -pubout -out chave_publica.pem
```

Agora temos uma chave pública e privada que podemos usar com o Openssl.

Crie um arquivo txt qualquer.

Cifrar

openssl pkeyutl -encrypt -inkey chave_publica.pem -pubin -in SEU_ARQUIVO.txt -out encriptado

Decifrar

openssl pkeyutl -decrypt -inkey chave_privada.pem -in encriptado

Faça você mesmo

Depois de cifrar sua mensagem, tente mudar qualquer coisa na mensagem cifrada, e depois decifrar.

Cifrar:

```
openssl rsautl -encrypt -inkey chave_publica.pem -pubin -in SEU_ARQUIVO.txt -out encriptado
```

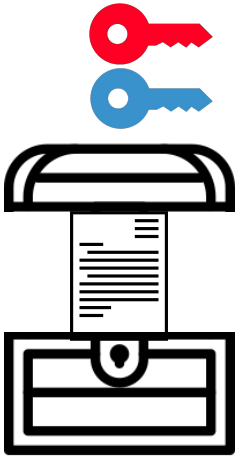
Decifrar:

```
openssl rsautl -decrypt -inkey chave_privada.pem -in encriptado
```

Mais Detalhes

Na criptografia assimétrica, na verdade, as chaves podem ser usadas de forma intercambiada.

Uma mensagem pode ser **cifrada** com a chave **pública**, e **decifrada** com a chave **privada**.

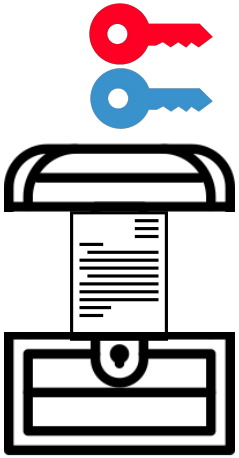


Mais Detalhes

Na criptografia assimétrica, na verdade, as chaves podem ser usadas de forma intercambiada.

Uma mensagem pode ser **cifrada** com a chave **pública**, e **decifrada** com a chave **privada**.

Uma mensagem também pode ser **cifrada** com a chave **privada**, e **decifrada** com a chave **pública**.



Cifrando com a chave privada

Alice vai cifrar a mensagem com a sua chave privada, **e enviar a mensagem e a chave pública.**

Alice

Rede Pública

Bob

Cifrando com a chave privada

Alice vai cifrar a mensagem com a sua chave privada, **e enviar a mensagem e a chave pública.**

Alice

Rede Pública

Bob

Cifrando com a chave privada

Alice vai cifrar a mensagem com a sua chave privada, **e enviar a mensagem e a chave pública.**

Alice

Rede Pública

Bob

Cifrando com a chave privada

Alice vai cifrar a mensagem com a sua chave privada, **e enviar a mensagem e a chave pública.**

Alice

Rede Pública

Bob

Cifrando com a chave privada

Qualquer um podia abrir o baú no caminho e ver a mensagem. O que ganhamos com isso?

Alice

Rede Pública

Bob

Cifrando com a chave privada

Se conseguimos decifrar a mensagem (abrir o baú) com a **chave pública** de Alice, significa que a mensagem realmente foi enviada por Alice.

Alice

Rede Pública

Bob

Cifrando com a chave privada

É muito difícil forjar uma mensagem se passando por Alice.

Alice

Rede Pública

Mensagem fake tentando
se passar por Alice.

Bob

Cifrando com a chave privada

É muito difícil forjar uma mensagem se passando por Alice.

Alice

Rede Pública

Bob

Mensagem fake tentando se passar por Alice.

Cifrando com a chave privada

Isso se chama **assinar uma mensagem**.

Alice

Rede Pública

Bob

Mensagem fake tentando se passar por Alice.

Dica

Para cifrar com a chave privada (e não com a pública) alguns parâmetros precisam ser modificados no openssl, como o uso da opção sign para assinar, e verify para abrir.

Faça você mesmo

Crie uma mensagem, e a assine (cifre) com sua chave privada.

Abra (verifique) com a chave pública.

Assinar:

```
openssl pkeyutl -sign -inkey chave_privada.pem -in SEU_ARQUIVO.txt -out ASSINADO.bin
```

Verificar:

```
openssl pkeyutl -verify -pubin -inkey chave_publica.pem -sigfile ASSINADO.bin -in
SEU_ARQUIVO.txt
```

Mais Problemas...

Considere que Alice enviou a sua chave pública para Bob.

Alice 

Rede Pública 

 Bob

Mais Problemas...

Considere que Alice enviou a sua chave pública para Bob.

Alice

Rede Pública

Bob

Mais Problemas...

Considere que Alice enviou a sua chave pública para Bob.

Como **garantir** que essa realmente é a chave pública de Alice?

Alice

Rede Pública

Bob

Mais Problemas...

Entidades “confiáveis” chamadas de *Certificate Authority* – CA (Autoridade de certificação).

Os componentes da rede confiam no CA.

O CA assina a chave de Alice. Bob usa a chave pública do CA para verificar se essa realmente é a chave de Alice.

Alice

Rede Pública

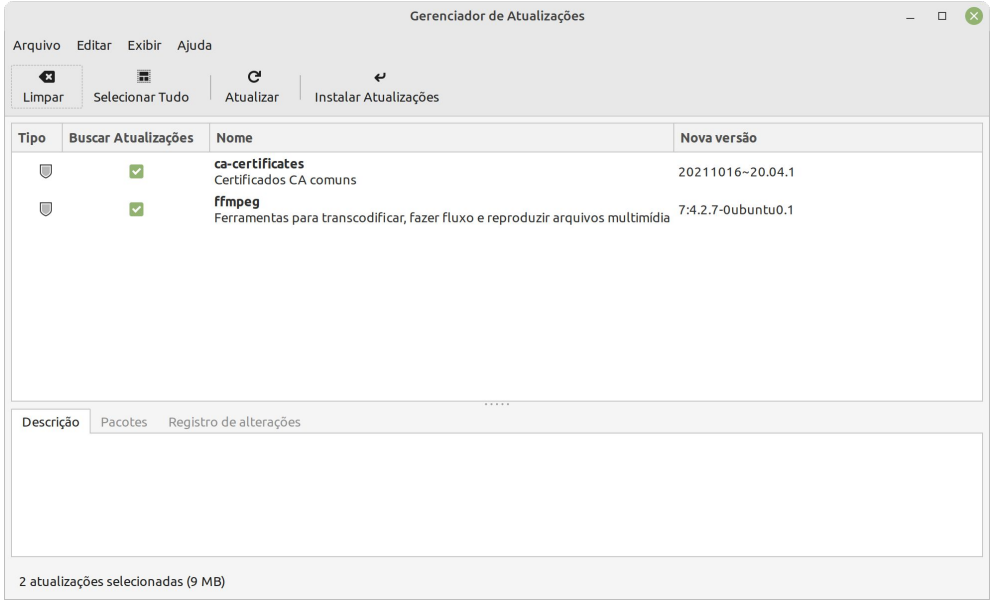
Bob

Mais Problemas...

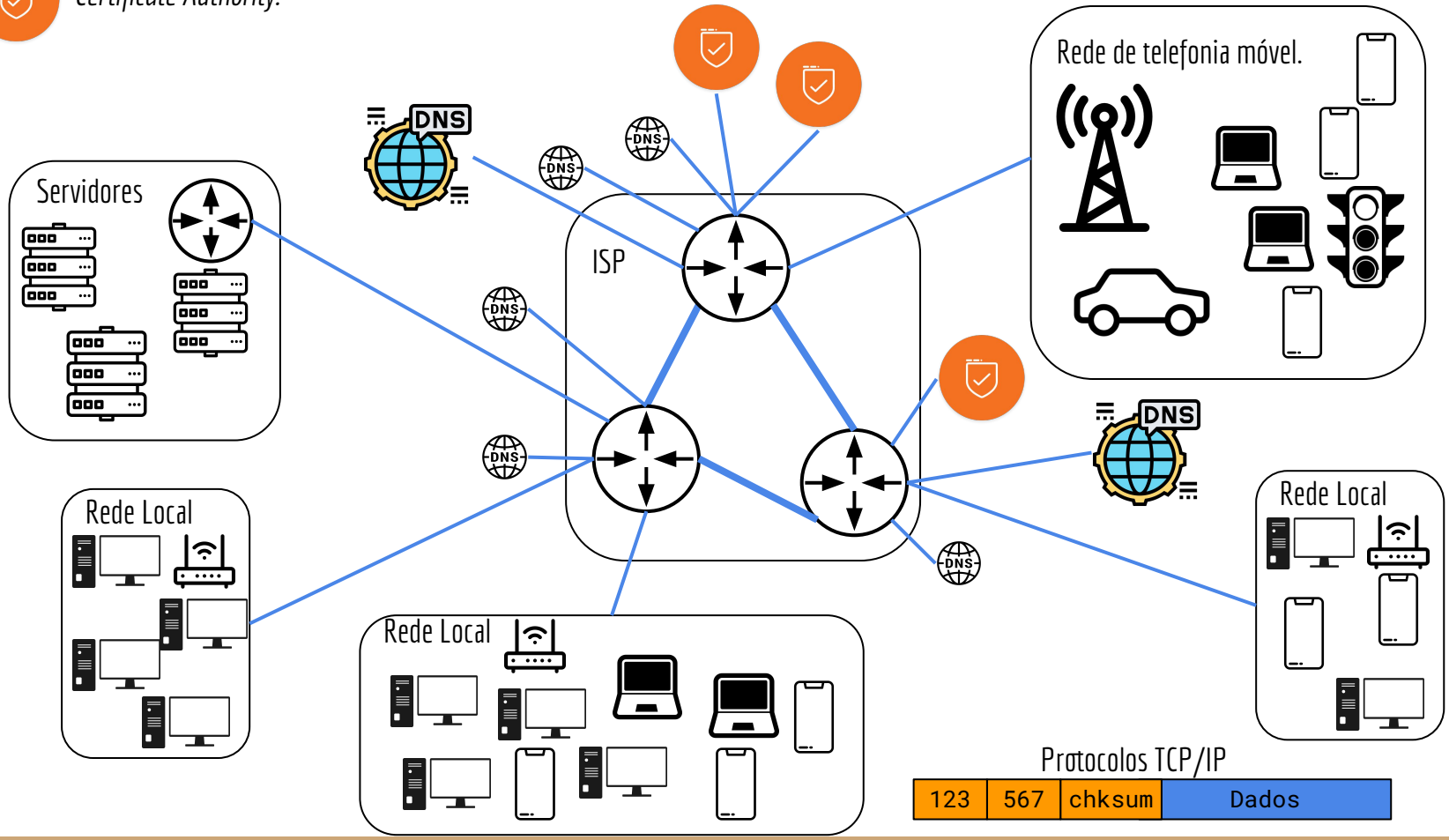
Os CAs cobram para assinar as chaves.

Se você tem um site, por exemplo, vai precisar comprar um certificado de algum CA.

Exemplo de CA - Geotrust.



Certificate Authority.



SSH

SSH - Secure Shell.

Protocolo cliente/servidor criptografado para logins remotos seguros em redes inseguras.

- Execução de comandos remotos.
- Acesso a Shell remoto.
- Transferência de arquivos.
- ...

SSH

SSH - Secure Shell.

Protocolo cliente/servidor criptografado para logins remotos seguros em redes inseguras.

- Execução de comandos remotos.
- Acesso a Shell remoto.
- Transferência de arquivos.
- ...

Uma das implementações mais comuns do protocolo é o OpenSSH, incluso por padrão na maioria das distribuições Linux.

SSH

A comunicação geralmente é feita de forma similar à estudada no começo da aula, usando criptografia assimétrica.

O SSH suporta vários tipos de comunicação.

Formato básico:

```
ssh Nome_Usuario@endereço
```

Para opções, veja *man ssh*

Faça você mesmo

Conecte via SSH na máquina macalan do departamento de informática.

```
ssh seu_usuario@ssh.inf.ufpr.br
```

Ou se você estiver em uma rede interna do DInf:

```
ssh seu_usuario@macalan
```

Para fechar a conexão, você pode usar o comando `exit`, ou então teclar `Control+D`.

Faça você mesmo

Você também pode enviar comandos via SSH.

O SSH vai abrir a conexão, enviar o comando para a máquina remota, exibir o resultado, e fechar a conexão.

Veja o espaço disponível para o seu usuário nos servidores do DInf.

```
ssh seu_usuario@ssh.inf.ufpr.br "quota -s"
```

Faça você mesmo

Conecte via SSH na máquina Macalan novamente, mas agora use o parâmetro -v para mostrar informações de debug.

Dê uma olhada nas informações.

```
ssh -v seu_usuario@ssh.inf.ufpr.br
```

Transferindo Arquivos

O OpenSSH possui em sua suíte de aplicativos softwares para transferência segura de arquivos.

O **scp** (*Secure File Copy*) pode ser usado para este fim.

Sintaxe similar ao comando cp (copy).

Comando básico:

```
scp ARQUIVO nome_usuario@servidor:diretorio_destino
```

Faça você mesmo

Crie um arquivo qualquer em seu computador.

Transfira esse arquivo para a sua *home* no servidor Macalan.

```
scp ARQUIVO nome_usuario@ssh.inf.ufpr.br:diretorio_destino
```

Dicas

Senhas de usuário em um banco de dados **nunca devem ser criptografadas**.

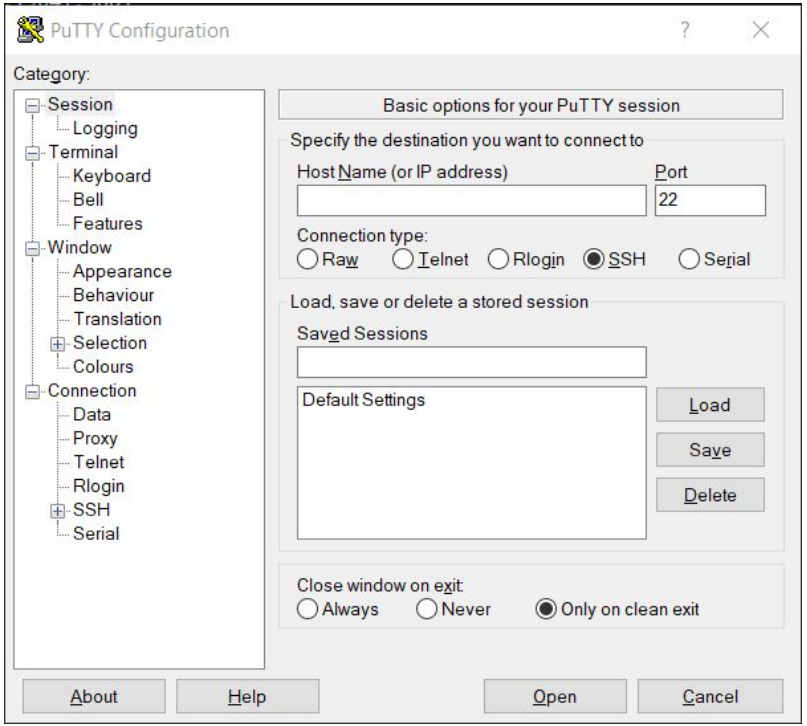
Por exemplo: o Twitter (espero) não guarda suas senhas diretamente em seu banco de dados, e também não guarda as senhas criptografadas.

Para isso, deve-se usar um **Hash Seguro**, e **armazenar o hash da senha**. Veja na literatura.

Dicas

No Windows, você pode usar o Putty para fazer uma conexão SSH.

www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

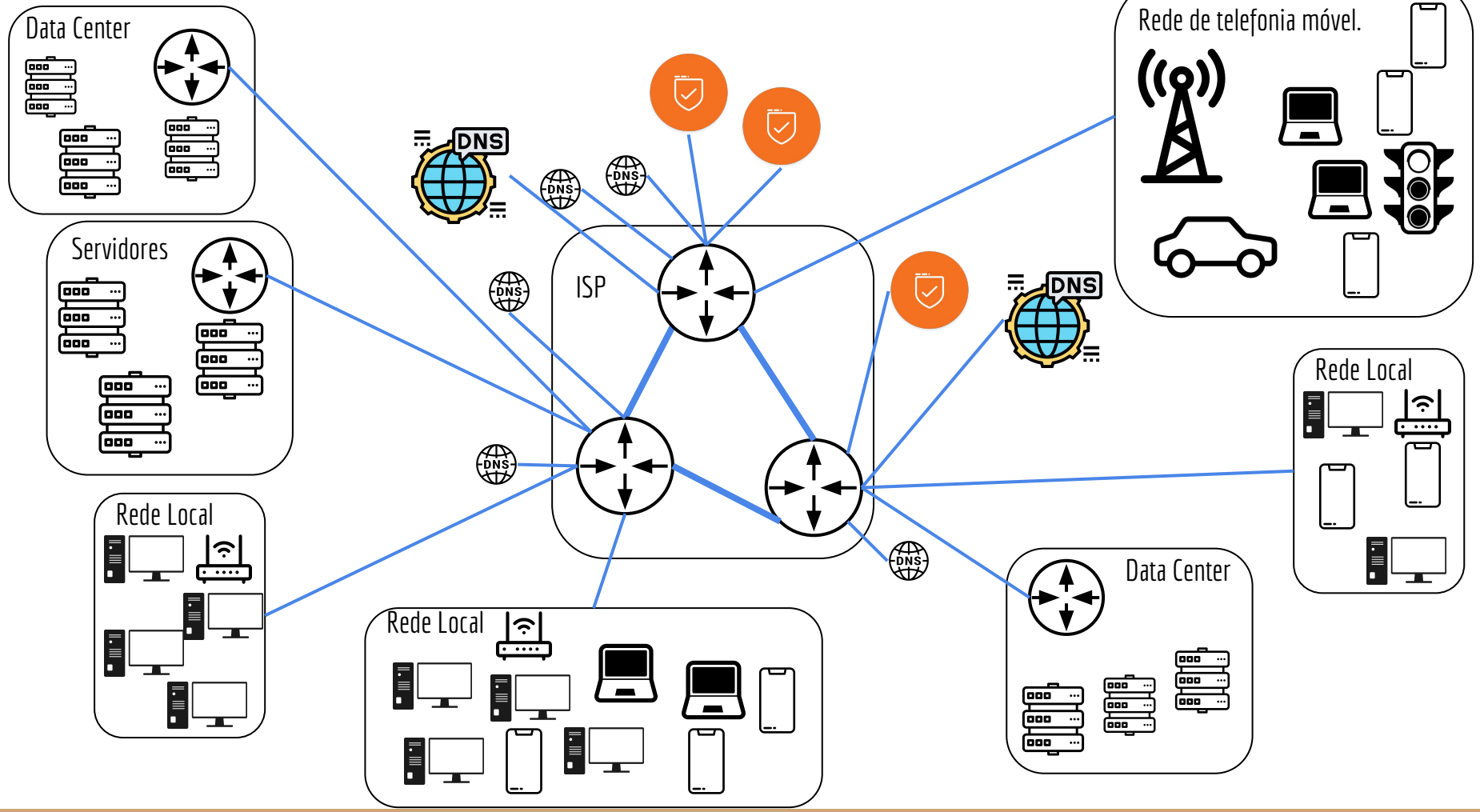


Computação em nuvem:

- Alugar poder computacional de um parque compartilhado de computadores.
- Parques computacionais são comumente chamados de ***data centers***.

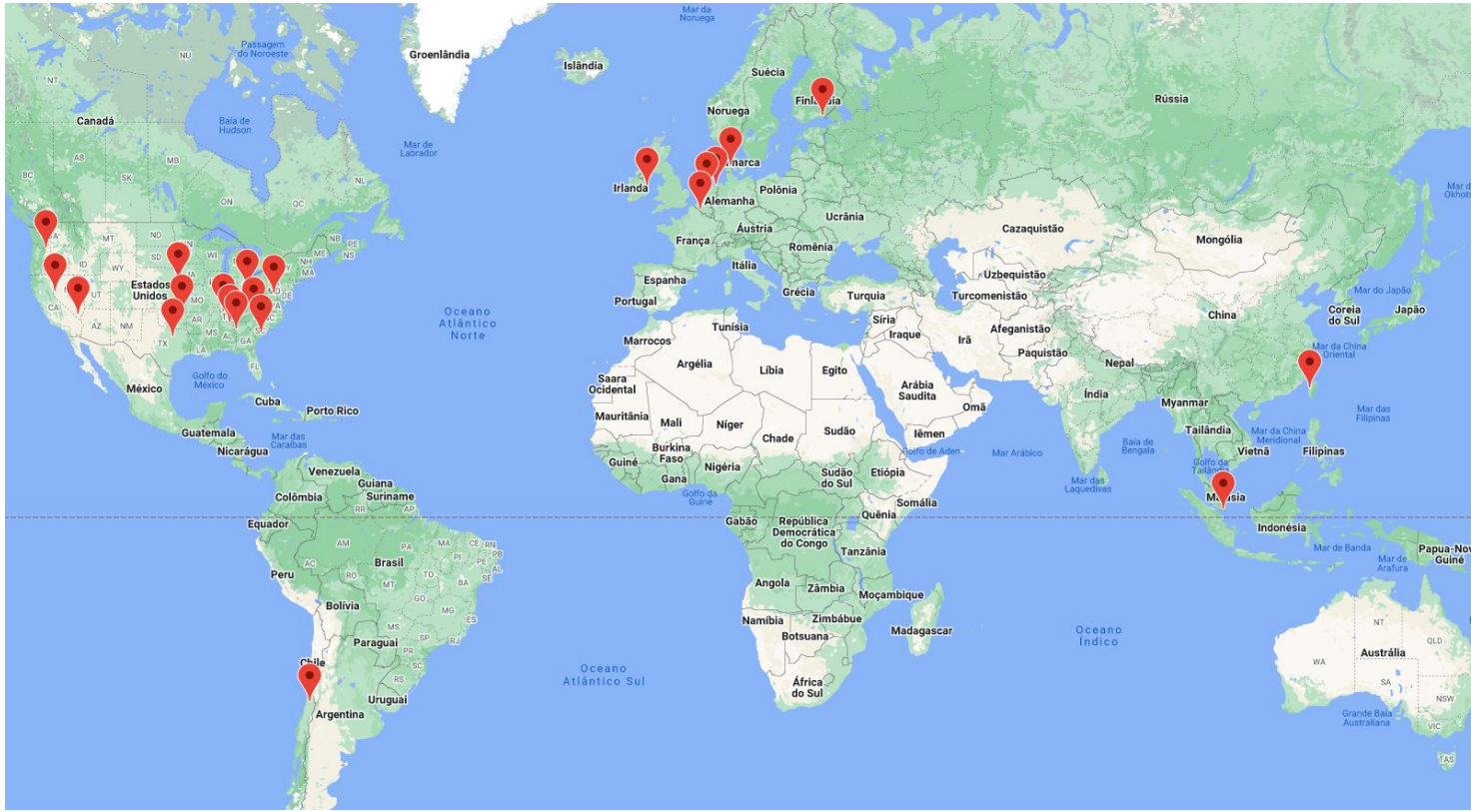
O poder computacional é acessível a partir da internet.

Pagamento pelo uso.


Data Center
Servidores
Rede Local
Rede Local
Rede de telefonia móvel.
Rede Local
Data Center
ISP
DNS
DNS
DNS
DNS
DNS
DNS
DNS

Curiosidade - Data Centers do Google

www.google.com/about/datacenters/locations



Curiosidade - Data Centers do Google

Eemshaven, Holanda – www.google.com/about/datacenters/locations/eemshaven

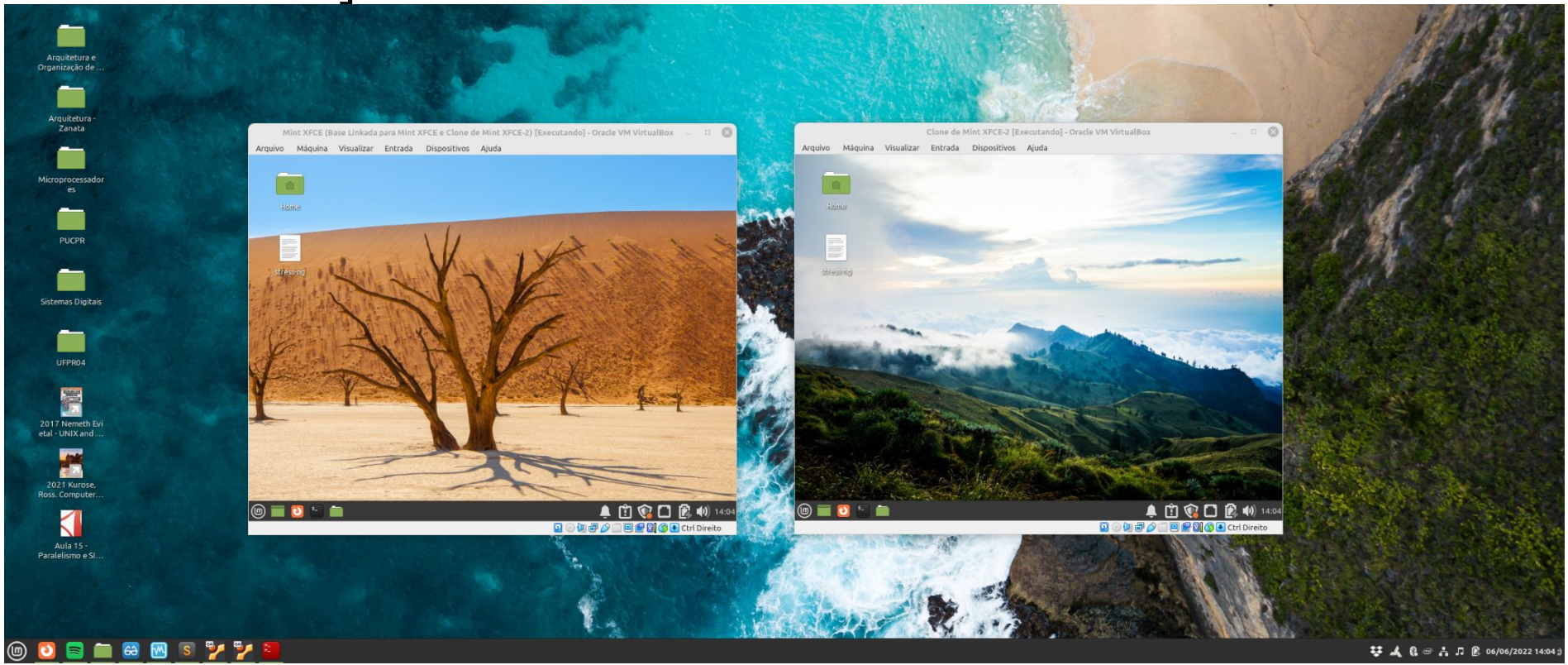
Virtualização

Os conceitos chave da computação em nuvem são a conexão remota, e a virtualização.

Conexão remota: comunicar com computadores através de uma rede (e.g., a Internet).

Virtualização: compartimentar os recursos computacionais de uma máquina, criando uma **máquina virtual**. Os recursos virtuais são de uso exclusivo de um usuário. Mas múltiplos recursos virtuais podem estar em uma única máquina física.

Virtualização



Alguns serviços de nuvem

Amazon Web Services (AWS);

Google Cloud Platform;

Microsoft Azure;

Locaweb;

IBM Softlayer;

...

Categorias Básicas

- Infrastructure-as-a-Service – IaaS.
- Platform-as-a-Service – PaaS.
- Software-as-a-Service – SaaS.

Infrastructure-as-a-Service – IaaS

Os usuários solicitam um computador com determinada configuração.

CPU, memória, armazenamento , largura de banda, ...

O usuário é responsável por configurar e manter a máquina.

Instalar S.O., softwares de usuário, softwares de gerência, ...

É como alugar um computador físico.

Obs.: geralmente o computador não é realmente físico, mas sim uma Máquina Virtual (VM).

Infrastructure-as-a-Service – IaaS

Os usuários solicitam um computador com determinada configuração.

CPU, memória, armazenamento , largura de banda, ...

O usuário é responsável por configurar e manter a máquina.

Instalar S.O., softwares de usuário, softwares de gerência, ...

É como alugar um computador físico.

Obs.: geralmente o computador não é realmente físico, mas sim uma Máquina Virtual (VM).

Se o computador não for uma Máquina Virtual, geralmente você verá o termo Bare Metal.

Não é uma máquina virtual, mas o “Metal Puro”.

Platform-as-a-Service – PaaS

O usuário requisita um determinado pacote de aplicativos.

Banco de dados, servidor de aplicação, gerenciador de aplicação, ...

O vendedor do serviço instala os softwares em seus servidores, e libera para o usuário.

O usuário utiliza os softwares para implantar sua aplicação.

Por exemplo: executar uma página PHP em um servidor apache.

O usuário é responsável pelo código da aplicação final.

Os demais itens são de responsabilidade do vendedor.

Hardware, sistema operacional, softwares contratados (e.g., banco de dados, servidor de aplicação, ...)

Software-as-a-Service – SaaS

Tudo é gerenciado pelo vendedor.

Hardware e software.

O cliente especifica o software que deseja, e o vendedor o mantém, dando ao usuário alguma forma de acesso.

Exemplos: Office 365 e aplicações do Google Drive.

Quais são as suas responsabilidades

Camada	Local	IaaS	PaaS	SaaS
Aplicação	✓	✓	✓	
Bancos de Dados	✓	✓	✓	
Sistema Operacional	✓	✓	✓	
Rede, armazenamento e servidores virtuais	✓	✓		
Plataforma de virtualização (e.g., VMware)	✓			
Servidores Físicos	✓			
Armazenamento Físico	✓			
Redes Físicas	✓			
Energia	✓			
Espaço e refrigeração	✓			

Snyder et al (2017).

Cobrança

Geralmente a cobrança envolve:

Recursos de CPU;
Recursos de GPU;
Uso de internet - Largura de banda (MiB/s) e quantidade (GiB) utilizada;
Armazenamento (GiBs utilizados de “disco”).

Cobrança

Geralmente a cobrança envolve:

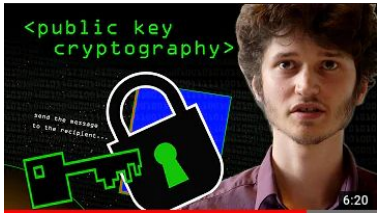
- Recursos de CPU;
- Recursos de GPU;
- Uso de internet - Largura de banda (MiB/s) e quantidade (GiB) utilizada;
- Armazenamento (GiBs utilizados de “disco”).

Você pode contratar, por exemplo, uma quantidade fixa por mês, ou então fazer sob demanda.

- Sob demanda: conforme mais recursos são gastos, mais são contratados automaticamente.
  - Pode sair caro.

Para aprender mais...

Veja esses vídeos sobre a história e alguns detalhes de implementação relacionados a segurança:



Chaves Públicas e Privadas: youtu.be/GSIDS_lvRv4

Um pouco sobre TLS: youtu.be/0TLDTodL7Lc

Para aprender mais...

Veja esses vídeos sobre a história e alguns detalhes de implementação relacionados a segurança:

Como uma conexão TLS é estabelecida: youtu.be/86cQJ0MMses

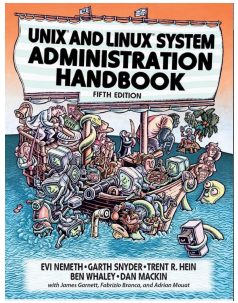
Ideia do algoritmo Diffie-Hellman para troca de chaves públicas e Privadas youtu.be/NmM9HA2MQGI

Exercícios

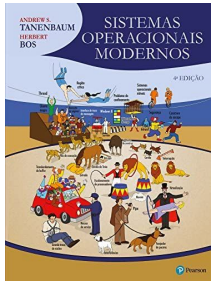
1. Replique todos os comandos dados nos slides.
2. Instale o VirtualBox ou similar em sua máquina. Coloque um ou mais sistemas operacionais Linux para ser executado no VirtualBox como máquinas virtuais.
3. Resolva os exercícios disponibilizados no Moodle.

Bibliografia

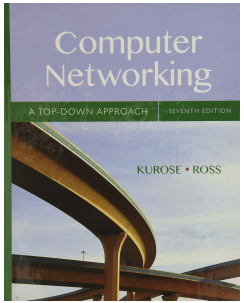
Snyder et al. UNIX and Linux System Administration Handbook. 5a ed. 2017.



Tanenbaum, Bos. Sistemas operacionais modernos. 4a ed. 2016.



Kurose, , Ross. Redes de computadores e a internet: uma abordagem top-down. 2013.



Licença