

# Segurança Computacional

U2FsdGVkX18+VqX7cccxEsilYKuWe1BKyo/9gQ5TwCM=

Ricardo de la Rocha Ladeira

{ricardo.ladeira@ifc.edu.br}



**INSTITUTO FEDERAL**

Catarinense

Campus Blumenau

# Criptografia

- ▶ U2FsdGVkX18+VqX7cccxEsilYKuWe1BKyo/9gQ5TwCM=
- ▶ O que é isso?

# Criptografia

- ▶ U2FsdGVkX18+VqX7cccxEsilYKuWe1BKyo/9gQ5TwCM=
- ▶ O que é isso?
- ▶ `sh blowfish_encryption.sh`
- ▶ `sh blowfish_decryption.sh`
- ▶ A chave é **Chave**.

# Criptografia

► PxIB4Gr/Nc6TigOdDxWu7Q==

# Criptografia

► Px1B4Gr/Nc6TigOdDxWu7Q==

1. `http://www.tools4noobs.com/online_tools/decrypt/`
2. Em **Key**, digite **Chave**
3. Algoritmo **Blowfish**, Modo **CBC** e **Base64**.
4. No textarea, digite **Px1B4Gr/Nc6TigOdDxWu7Q==** e pressione **Decrypt this!**

**ATENÇÃO!** diferencia letras maiúsculas e minúsculas!

# Criptografia



# Criptografia

- ▶ Escrita escondida.
- ▶ Conjunto de técnicas que tornam um texto (ou uma imagem, um arquivo etc.) ilegível.
- ▶ **Criptografar** ou **cifrar** é o ato de tornar ilegível uma mensagem. O oposto, ou seja, a partir da mensagem ilegível obter-se a original, é chamado de decifragem.
- ▶ Técnica extremamente antiga (do tempo dos egípcios).

# Criptografia

[globo.com](#) [notícias](#) [esportes](#) [entretenimento](#) [vídeos](#) [e-mail](#) [central globo.com](#) [assine já](#) [todos os sites](#)

 **Política**  [buscar](#)

[Brasil](#) | [Mundo](#) | [Economia](#) | [Política](#) | [Esportes](#) | [Carros](#) | [Emprego](#) | [Educação](#) | [Saúde](#) | [Tech](#) | [Bizarro](#) | [Pop&Arte](#) | [MG](#) | [RJ](#) | [SP](#) | [Telejornais](#) | [Virada de ano](#)

CES 2014  
25/06/2010 08h49 - Atualizado em 28/06/2010 11h40

## Nem FBI consegue decifrar arquivos de Daniel Dantas, diz jornal

HDs foram apreendidos pela PF durante a Operação Satiagraha, em 2008. Informações estão protegidas por sofisticado sistema de criptografia.

Do G1, em Brasília 

O FBI não conseguiu quebrar o sistema de criptografia dos discos rígidos apreendidos pela Polícia Federal no apartamento do banqueiro Daniel Dantas, no Rio, durante a Operação Satiagraha, deflagrada em julho de 2008. Segundo reportagem publicada nesta sexta-feira (25) pelo jornal "Folha de S.Paulo", após um ano de tentativas frustradas, em abril a polícia federal norte-americana devolveu os equipamentos ao Brasil.

**saiba mais**

**Justiça aceita denúncia, e Daniel Dantas vira réu no processo da Satiagraha**

**Caso Satiagraha: Daniel Dantas enfrenta à**

A ajuda aos EUA, de acordo com a reportagem, só foi pedida no início de 2009, após os peritos do Instituto Nacional de Criminalística (INC) terem falhado nos esforços de decodificar as senhas dos HDs. O governo

PUBLICIDADE

Agora é Time Brasil. Agora é BRA.

*CLIQUE E DESCUBRA  
QUAL ESPORTE MAIS  
COMBINA COM VOCÊ*

 **Bradesco**  
Mais de 100 anos para você.

**Política**

23 JUL



19:08

Advogada chamada pela CPI desiste de clientes: OAB pode ir ao Supremo



# Criptografia

Por que usar?

- ▶ Proteção de informações.
- ▶ Confidencialidade nas comunicações.
  - ▶ E integridade?

# Criptografia

## Por que usar?

- ▶ *Sniffers*<sup>1</sup> (farejadores) podem interceptar pacotes que trafegam na rede.
- ▶ E se os seus dados, tais como número do cartão de crédito, mensagens de e-mail e senhas de banco, fossem capturados e estivessem em texto claro?
- ▶ Será que os mais populares serviços de mensagem criptografam as conversas?

---

<sup>1</sup>Exemplos: Wireshark, Microsoft Network Monitor, Capsa Packet Sniffer, NetworkMiner, SniffPass

# Criptografia

## Aplicação

- ▶ Transações bancárias.
- ▶ Armazenamento e transporte de dados confidenciais.
- ▶ Comunicação (telefonema, e-mail, chats...).
- ▶ Está presente na maioria dos serviços que utilizam protocolos criptográficos (SSL/TLS).
- ▶ Ofuscadores

# Criptografia

## Aplicação

- ▶ Usada para geração de *hashes*.
- ▶ Base para a existência de protocolos que implementam soluções de segurança.
- ▶ Base para a tecnologia de certificação digital.

# Criptografia

## Criptoanálise

- ▶ Em oposição à criptografia está a criptoanálise.
- ▶ Consiste na arte de descobrir o texto cifrado ou a chave para sua codificação.

# Criptografia

## Hash

- ▶ **Hash** (resumo) é uma função ou um algoritmo que transforma um conjunto de dados de tamanho variável em um conjunto de dados de tamanho fixo, sem que seja possível retornar ao valor inicial.
- ▶ Usado para verificar a integridade de arquivos.
- ▶ Exemplo: função MOD (%) por um número  $M$  fixo.

# Criptografia

## Hash

- ▶ De acordo com Kauffman (2021), quando falamos em funções de *hashes* criptográficos, estamos falando de funções de hash que tenham as seguintes propriedades:
  - ▶ Fácil de computar o valor do *hash* para qualquer mensagem.
  - ▶ Inviável de gerar uma mensagem que tenha um determinado *hash*.
  - ▶ Inviável de modificar a mensagem sem modificar o *hash*.
  - ▶ Inviável encontrar duas mensagens diferentes com o mesmo *hash*.
- ▶ O *hash* deve ser resistente contra:
  - ▶ Colisões (duas mensagens diferentes gerando o mesmo *hash*).
  - ▶ Resistência à pré-imagem: dado um *hash*, deve ser difícil encontrar uma mensagem que possa ser resumida neste *hash*.
  - ▶ Resistência a segundas pré-imagens: dado  $m$ , é inviável encontrar  $m'$  ( $m' \neq m$ ) tal que  $\text{hash}(m) = \text{hash}(m')$ .

# Criptografia

## Hash

- ▶ *Hashes* criptográficos costumam ser utilizados para armazenamento de dados sensíveis em Bancos de Dados.
- ▶ A ideia é que, caso o BD seja acessado indevidamente, a tarefa de obter os dados em texto claro seja dolorosa para o invasor. Nesse caso o *hash* serve como uma contenção de danos.



# Criptografia

## Hash

### ▶ Algoritmos conhecidos:

- ▶ MD4
- ▶ MD5
- ▶ SHA
- ▶ Whirlpool

# Criptografia

## Hash

- ▶ Exemplos de uso:

```
echo 'sdsdsdsdsdssdsdsdsdsdsds' | md5sum
```

```
echo 'sdsdsdsdsdssdsdsdsdsdsds ' | md5sum
```

```
echo -n 'sdsdsdsdsdssdsdsdsdsdsds' | md5sum
```

```
echo -n 'sdsdsdsdsdssdsdsdsdsdsds ' | md5sum
```

- ▶ A resposta foi a mesma?

# Criptografia

## Hash

- ▶ Arquivos diferentes:  
`diff message1.bin message2.bin`
- ▶ Colisão no hash com MD5:  
`md5sum message1.bin message2.bin`
- ▶ Sem colisão com SHA256:  
`sha256sum message1.bin message2.bin`

# Criptografia

## Hash









- ▶ Arquivos diferentes:  
`diff shattered-1.pdf shattered-2.pdf`
- ▶ Colisão no hash com SHA1:  
`sha1sum shattered-1.pdf shattered-2.pdf`
- ▶ Sem colisão com SHA256:  
`sha256sum shattered-1.pdf shattered-2.pdf`

# Criptografia

## Hash

Figura: Exemplo de *hash*.

Home / 7-Zip / 9.22

Name ▾	Modified ▾	Size ▾	Downloads / Week ▾
↑ Parent folder			
<a href="#">7z922-arm.exe</a>	2011-04-18	592.0 kB	126  
<a href="#">7z922-x64.msi</a>	2011-04-18	1.4 MB	4,477  
<a href="#">7z922_extra.7z</a>	2011-04-18	710.1 kB	189  
<a href="#">7z922.tar.bz2</a>	2011-04-18	790.0 kB	1,941  

**SHA1:** 1aaec46fc08aa26d0758cecbab06f37ab6f89c62 **is (All-Time):** 528,920

**MD5:** 7529738373924ca3ef9b3e2a2235a7bf

Fonte: Source Forge, 2016.

# Criptografia

## Cifra de César

- Uma das primeiras formas de cifragem que se tem conhecimento é a **Cifra de César**.



# Criptografia

## Cifra de César

- ▶ Consistia em escrever uma mensagem com as letras do alfabeto três casas acima.
- ▶ Exemplo: IFC  $\rightarrow$  LIF.
- ▶ Interceptamos o texto abaixo e sabemos que ele foi codificado com a Cifra de César. Qual é a mensagem original?  
HVWDPRV QR ODERUDWRULR GR LIF DSUHQGHQGR  
VREUH D FLIUD GH FHVDU!

# Criptografia

## Cifra de César

### ► Resposta:

```
> echo HVWDPRV QR ODERUDWRULR GR LIF  
    DSUHQGHQGR VREUH D FLIUD GH FHVDU! |  
    caesar
```

### ► Ferramenta `caesar` (pacote `bsdgames`)



# Criptografia

- Suponha que você dispõe de uma máquina que só consegue testar 15 chaves por segundo. Em até quanto tempo ele obterá a mensagem original de um texto com 1024 caracteres criptografado com a Cifra de César? Despreze os tempos de leitura e escrita.

# Criptografia

- ▶ Este tipo de criptografia, no entanto, é muito simples. Existem métodos mais sofisticados e que podem fazer com que bilhões de anos sejam necessários para decifrar uma mensagem.
- ▶ Filme sobre o assunto: O jogo da imitação. Mostra a importância da criptografia, mudando os rumos da Segunda Guerra Mundial.

# Criptografia

- ▶ Se interceptamos a mensagem “LIF” e sabemos que ela está criptografada, o que mais precisamos saber?
- ▶ E se a mensagem fosse MHG? Se fosse uma espécie de variação da Cifra de César, onde uma letra fica 4 posições à frente no alfabeto, mas a letra seguinte fica 2 posições, depois novamente 4 posições e assim por diante?

# Criptografia

- ▶ **Obter a chave** é importante para o processo de decifragem, ou seja, saber como descobrir o significado de qualquer mensagem criptografada. A chave tem papel semelhante ao de uma senha.
- ▶ No caso da Cifra de César, a chave é saber que o texto cifrado contém caracteres 3 posições à frente do caractere original. Sabendo isto, toda mensagem pode ser decifrada.

# Criptografia

- ▶ Existem várias classificações para criptografia. A que nos interessa é a classificação entre **simétrica** e **assimétrica**.
- ▶ Simétrica: mais rápida.
- ▶ Assimétrica: mais segura.

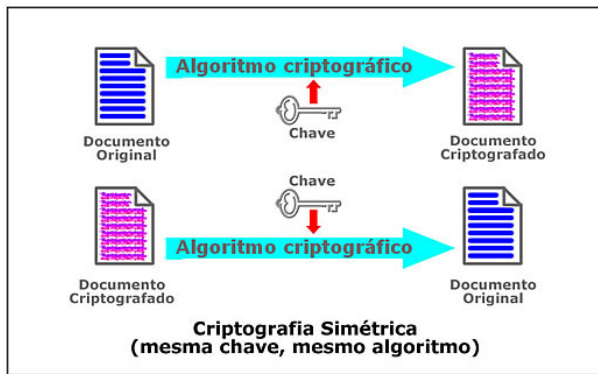
# Criptografia

## Criptografia Simétrica

- ▶ A criptografia simétrica utiliza a mesma chave para os processos de cifragem e decifragem.
- ▶ A Cifra de César é um exemplo de criptografia simétrica. Basta saber que um caractere deve ser substituído por outro três posições à frente para cifrar que, automaticamente, sabe-se que, a partir da mensagem cifrada, obtém-se o caractere original substituindo o caractere da mensagem criptografada por outro três posições para trás no alfabeto.

# Criptografia

## Criptografia Simétrica



- Pense na fechadura da porta. Em geral, a chave que tranca é a mesma que destranca.

# Criptografia

## Criptografia Simétrica

- ▶ Este tipo de criptografia é rápido, já que os procedimentos para cifragem e decifragem envolvem o mesmo algoritmo.
- ▶ **Problema:** para cada comunicação é necessário gerar uma chave diferente.
  - > Comunicação(A, B) = Chave 3
  - > Comunicação(A, C) = Chave 4
  - > Comunicação(A, N) = Chave 5
  - ...
  - > Comunicação(A, Z) = Chave 3 (!!!!) # Z poderia ler as mensagens destinadas a B e vice-versa, comprometendo a confidencialidade das informações.



# Criptografia

## Criptografia Simétrica

- ▶ O problema é que para cada comunicação é necessário gerar uma chave diferente.
- ▶ No exemplo dado, estamos falando de 4 linhas de comunicação. Imagine um ambiente onde milhões de usuários precisam trocar informações seguras (exemplo: Internet).

# Criptografia

## Criptografia Simétrica

- ▶ O que acontece se uma chave diferente for utilizada?
- ▶ Teste em [http://www.tools4noobs.com/online\\_tools/decrypt/](http://www.tools4noobs.com/online_tools/decrypt/) ou nos arquivos do Blowfish.

# Criptografia

## Criptografia Simétrica

- ▶ A Cifra de César é considerada uma **cifra de substituição**.
- ▶ Neste caso, uma **cifra de substituição monoalfabética** que obedece uma relação de ordem.

# Criptografia

## Criptografia Simétrica

Tabela: Exemplo de Cifragem com Substituição Monoalfabética.

Original	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	...	<b>Z</b>
Chave	<b>R</b>	<b>X</b>	<b>F</b>	<b>S</b>	<b>Z</b>	...	<b>Q</b>

► Mensagem: BECA → XZFR.

# Criptografia

## Criptografia Simétrica

- ▶ Sem relação de ordem, a quantidade de chaves testadas é maior.
- ▶ Uma tabela de frequência ajuda a decifrar a mensagem.

# Criptografia

## Criptografia Simétrica

- ▶ Na **cifra de substituição polialfabética**, símbolos são mapeados em múltiplos alfabetos (*tabula recta*).
- ▶ A **Cifra de Vigenère** é um exemplo.

# Criptografia

## Criptografia Simétrica

Texto Claro: MICHIGAN TECHNOLOGICAL UNIVERSITY. Chave: HOUGHTON.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Michigan Technological University, 2016.

# Criptografia

## Criptografia Simétrica

- ▶ MICHIGAN TECHNOLOGICAL UNIVERSITY (texto claro)
- ▶ HOUGHTON HOUGHTONHOUGH TONHOUGHTO (chave)
- ▶ TWWNPZOA ASWNUHZBNWWGS NBVCSLYPMM (texto cifrado)



# Criptografia

## Criptografia Simétrica

Decifre: ORC QCJR. Chave: GRUPO.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

# Criptografia

## Criptografia Simétrica

- ▶ Outros métodos
  - ▶ Transposição alfabética
  - ▶ Substituição por código

# Criptografia

## Criptografia Assimétrica

- ▶ A criptografia assimétrica, também chamada de criptografia de chave pública, utiliza os conceitos de chave pública e chave privada.
- ▶ Aqui, a chave que cifra não é a mesma que decifra!
- ▶ Pense em um tipo novo e mais moderno de fechadura. A chave que tranca não é a mesma que destranca!

# Criptografia

## Criptografia Assimétrica



# Criptografia

## Criptografia Assimétrica

- ▶ A criptografia assimétrica não possui o problema da distribuição de chaves, apresentado pela criptografia de chave simétrica.
- ▶ Aqui, a chave pública é distribuída livremente, não é necessária uma chave para cada comunicação!
- ▶ A desvantagem é o custo, pois, normalmente, possui chaves maiores e seus algoritmos são mais complexos, sendo mais lento criptografar de forma assimétrica.

# Criptografia

## Criptografia Assimétrica

- ▶ A chave pública é distribuída livremente.
- ▶ A chave privada não é distribuída, deve ser mantida em segredo pelo seu dono.

# Criptografia

## Criptografia Assimétrica

- ▶ Um exemplo de algoritmo de chave assimétrica é o PGP (*Pretty Good Privacy* – Privacidade muito boa).
- ▶ Utilizada para assinatura digital, cifragem e decifragem de textos, e-mails (hushmail), arquivos...

# Criptografia

## Criptografia Assimétrica

- ▶ Entre em <https://onlinepgp.com/> e gere suas chaves:
  - ▶ Clique em CREATING NEW PGP KEYS PAIR.
  - ▶ Preencha as informações.
  - ▶ Clique em GENERATE NEW PGP KEYS PAIR.
- ▶ Utilize a chave pública e escreva uma mensagem a ser criptografada.
  - ▶ Clique em ENCRYPTION/DECRYPTION PGP MESSAGE.
  - ▶ Na seção ENCRYPTION, insira a chave pública e o texto a ser cifrado.
  - ▶ Clique em ENCRYPT TEXT.
- ▶ Utilize a mensagem cifrada e a chave privada para obter a mensagem original.
  - ▶ Clique em ENCRYPTION/DECRYPTION PGP MESSAGE.
  - ▶ Na seção DECRYPTION, insira a chave privada, a senha e o texto cifrado.
  - ▶ Clique em DECRYPT TEXT e o texto original aparecerá.



# Criptografia

## Criptografia Assimétrica – Exercício

- ▶ Utilizando a página citada (<https://onlinepgp.com/>), gere seu par de chaves e envie para o(a) seu(sua) colega do lado a sua chave pública. O(A) colega deverá criar uma mensagem e criptografá-la utilizando sua chave pública. A mensagem criptografada deve ser enviada a você. Utilizando sua chave privada, descubra qual era a mensagem.
- ▶ Outras opções caso a página esteja indisponível:
  - ▶ <http://www.2pih.com/pgp.html>
  - ▶ <https://youritmate.us/pgp/>
  - ▶ <https://webencrypt.org/openpgpjs/>
  - ▶ <https://aliceandbob.io/online-pgp-tool>
  - ▶ <https://8gwifi.org/pgpencdec.jsp>
  - ▶ <https://codref.org/tools/pgp/>
  - ▶ <https://pgptool.org/>

# Criptografia

## Ferramentas

- ▶ AxCrypt
- ▶ miniLock
- ▶ Safe House Explorer USB Disk Encryption
- ▶ Ccrypt

# Criptografia

## Ferramentas

- ▶ Ccrypt.
- ▶ Ferramenta para criptografar e descriptografar arquivos e pastas.
- ▶ Disponível para Linux (`apt-get install ccrypt`).

# Criptografia

## Ferramentas

- ▶ `ccrypt "/home/usuario/Termo.pdf"`
- ▶ Coloca-se uma senha (chave) para criptografar o arquivo.
- ▶ O arquivo recebe a extensão `.cpt`.

# Criptografia

## Ferramentas

- ▶ `ccdecrypt "/home/usuario/Termo.pdf.cpt"`
- ▶ Exige a senha para decifrar o arquivo e obter novamente o original.

# Criptografia

## Ferramentas

- ▶ `ccdecrypt "/home/usuario/Termo.pdf.cpt"`
- ▶ Exige a senha para decifrar o arquivo e obter novamente o original.
- ▶ Que tipo de criptografia é essa que usa a mesma chave para cifrar e decifrar?

# Exercícios

## Leitura

- ▶ Ler a matéria abaixo:
- ▶ 5 DICAS DE EDWARD SNOWDEN PARA PROTEGER SUA PRIVACIDADE NA INTERNET

# Concluindo

- ▶ A criptografia é importante para a segurança das informações.
- ▶ Possibilita o uso de *hashes*, criação de protocolos seguros, assinatura digital...
- ▶ “*Criptografia é a melhor defesa contra as trevas*” (SNOWDEN, Edward)



## Referências e Sugestões de Leituras

- ▶ <https://cloud101.eu/about-secure-password-hashing-86e8e8ff338e>
- ▶ [www.tecmundo.com.br/seguranca/1795-confira-programas-para-criptografar-arquivos.htm](http://www.tecmundo.com.br/seguranca/1795-confira-programas-para-criptografar-arquivos.htm)
- ▶ <https://exame.com/tecnologia/criptografia-e-a-melhor-defesa-contras-trevas-diz-snowden>
- ▶ <https://cartilha.cert.br/>

# Segurança Computacional

U2FsdGVkX18+VqX7cccxEsilYKuWe1BKyo/9gQ5TwCM=

Ricardo de la Rocha Ladeira

{ricardo.ladeira@ifc.edu.br}



**INSTITUTO FEDERAL**

Catarinense

Campus Blumenau