

CC8130: SEGURANÇA NA INFORMAÇÃO

Atividade 2 - Função Hash

Abril 2023

- **Aluno:**
 - Lucas Mateus de Moraes (RA: 22.220.004-0)
- **Professor:** Dr. Ricardo Carvalho Destro

1 Descrição do experimento:

Identificar quais frases abaixo podem ser consideradas verdadeiras ou falsas conforme os hashes que foram fornecidos para validação. Cada frase possui um hash SHA256 e um MD5.

1.1 Repositório:

Os códigos e arquivos relacionados a essa atividade podem ser consultados no seguinte repositório:

- <https://github.com/luca-moraes/atividade2SegInfo>

2 Exemplos de frases corretas e seus hashes (SHA256 e MD5, respectivamente):

- "SHA256 e MD5 corretos"

c034489664dd98c3a2b0d7c1afc0717378827d9fa778288c8bb1c567c8bc2ec1
19406b49ace5073c806a79061f58dbd3

- "Somente SHA256 correto"

5b22f6bf621c2116f0d4589c3b5405ed3b5d768b9ba1dfafbae9292331ce9827
cfe69ac7a0b07810b391c27b1ea838cd

- "Somente MD5 correto"

58d909cc5c6ac58bb509d4651528c66a8b9bd8a197ec260dd7d6754b98b6b63e
c4e28d48ac81f88aaade5ed31f2e2c26

- "Nenhum dos dois corretos"

d55825a0c3ee133ac29986b3fcef30432968e99967787191bb48be89e485cf8
8bdf3218ccd26f327220ad0daf3d3ce0

2.1 Análise pelo código:

Como pode ser verificado na imagem Figura 1, as informações fornecidas estão em concordância com aquilo que a execução do código resultou em sua verificação.

```

EXPLORADOR
  ...
  ATIVIDADE2SEGINFO [CODESPACES...]
    CC8130-HASH.py
    conversorFrases.py
    frases.csv
    frases.txt
    $ installEnv.sh
    README.md
    referenciasCorretas.csv
    referenciasCorretas.txt
    $ runMyCode.sh

CC8130-HASH.py
61 arquivo_csv = 'referenciasCorretas.csv'
62 #arquivo_csv = 'frases.csv'
63 verificar_hashes(arquivo_csv)

PROBLEMAS SAÍDA CONSOLE DE DEPURACÃO TERMINAL PORTAS COMENTÁRIOS
@luca-moraes → /workspaces/atividade2SegInfo (main) $ ./runMyCode.sh
SHA256 e MD5 corretos - SHA256: OK; MD5: OK

SHA256 calculado: c034489664dd98c3a2b0d7c1afc0717378827d9fa778288c8bb1c567c8bc2ec1
SHA256 fornecido: c034489664dd98c3a2b0d7c1afc0717378827d9fa778288c8bb1c567c8bc2ec1

MD5 calculado: 19406b49ace5073c806a79061f58dbd3
MD5 fornecido: 19406b49ace5073c806a79061f58dbd3

Somente SHA256 correto - SHA256: OK; MD5: Erro

SHA256 calculado: 5b22f6bf621c2116f0d4589c3b5405ed3b5d768b9ba1dfafbae9292331ce9827
SHA256 fornecido: 5b22f6bf621c2116f0d4589c3b5405ed3b5d768b9ba1dfafbae9292331ce9827

MD5 calculado: cfe69ac7a0b07810d391c27b1ea838cd
MD5 fornecido: cfe69ac7a0b07810b391c27b1ea838cd

Somente MD5 correto - SHA256: Erro; MD5: OK

SHA256 calculado: 58d909cc5c6ac58bb509d4651528c66a8b9bd8a197ec260dd7d6754b98b6b63e
SHA256 fornecido: 58d909cc5c6ac58bb509d4651528c66a8b9bd8a197ec260dd7d6754b98b6b63e

MD5 calculado: c4e28d48ac81f88aaade5ed31f2e2c26
MD5 fornecido: c4e28d48ac81f88aaade5ed31f2e2c26

Nenhum dos dois corretos - SHA256: Erro; MD5: Erro

SHA256 calculado: d55825a0c3ee133ac29986b3fcef30432968e99967787191bb48be89e485cf8
SHA256 fornecido: d55825a0c3ee133ac29986b3fcef30432968e99967787191bb48be89e485cf8

MD5 calculado: 8bdf3218ccd26f327220ad0daf3d3ce0
MD5 fornecido: 8bdf3218ccd26f327220ad0daf3d3ce0

@luca-moraes → /workspaces/atividade2SegInfo (main) $

```

Figura 1: Figura 1

3 Frases e resultados do experimento:

3.1 Tabela de frases:

A Tabela 1 resume os resultados encontrados, a justificativa detalhada para cada caso do experimento pode ser encontrada na seção 3.2, após as tabela:

Frase	Status	SHA256 Calculado	SHA256 Fornecido	MD5 Calculado	MD5 Fornecido
A primeira das instituições criadas pelo Pe. Roberto Sabóia De Medeiros foi a antiga Escola Superior de Administração De Negócios de São Paulo - ESAN/SP.	OK;OK	d24de3ec3835115c576a55188a31761b73af93ed2c45a171c810bb66b24b08f9	d24de3ec3835115c576a55188a31761b73af93ed2c45a171c810bb66b24b08f9	c850e1a34a6ed572e0758ccd9c615bda	c850e1a34a6ed572e0758ccd9c615bda
A FEI é uma instituição vinculada estatutariamente A Companhia de Jesus	Erro;Erro	6979a3d7a19e5921ae00ca7db9b814e1b83831dcedfca33dbb72e761ca084437	6979a3d7a19e5921ae00ca7db9b814e1b83831dcedfca33dbb72e761ca084437	b710771da8d752152445233ea9bb9e1	b710771da8d752152445233ea9bb9e1
Em 20 de janeiro de 1951 foi realizada a sessão solene da congregação para a Colação de Grau da primeira turma da Faculdade de Engenharia Industrial.	OK;OK	6c582a93ba3ea454f11221a374878e534cfe666060c87ba03127de07f1ca4e6	6c582a93ba3ea454f11221a374878e534cfe666060c87ba03127de07f1ca4e6	55748c2cb669a9d9508677cb914cb025	55748c2cb669a9d9508677cb914cb025
A Capela Santo Inácio de Loyola foi construída no ano de 1978, Em concreto aparente.	Erro;Erro	245e695d0f8835651bc231f9cf1b2a7a097b849648f05f79f1855a55f85b089e	254e695d0f8835651bc231f9cf1b2a7a097b849648f05f79f1855a55f85b089e	f4a8a299fd4da2a5d70b374be2e48417	f4a8a299fd4da2a5d70b374be2e48417
Tendo como função principal a promoção do aprimoramento profissional no campo administrativo e tecnológico, o IECAT (Instituto de Especialização em Ciências Administrativas e Tecnológicas) foi criado em 1982	OK;OK	d2150d688c337fc57e235adafd57f86d7aba0b8682c249b1006ba592706f88a0	d2150d688c337fc57e235adafd57f86d7aba0b8682c249b1006ba592706f88a0	1c4ecc238571333ae507f82ff6a5e9e4	1c4ecc238571333ae507f82ff6a5e9e4
Dentro de uma proposta de integração e de agregação de competências, visando a excelência de seus cursos, as instituições FEI, FCI e ESAN foram transformadas no Centro Universitário da FEI no ano de 2002.	Erro;Erro	faefb927a21dd282ee09effe42bc0688f649450677a61edce15863a15461b721	faefb927a21dd282ee09effe42bc0688f649450677a61edce15863a15461b721	98420532cbf1be32a98be579f502cd72	98420532cbf1be32a98be579f502cd72
O Centro Universitário da FEI passou a fazer parte do seletor grupo que produz ciência no Brasil, quando a CAPES aprovou o Primeiro curso de Mestrado em Engenharia Elétrica em 2005.	OK;OK	da9f214449005850f4fd552238658820434c15ca06389d018b1814bb376abaa6	da9f214449005850f4fd552238658820434c15ca06389d018b1814bb376abaa6	2e20bfbece6f6dc62de4c4bb80a77ba1f	2e20bfbece6f6dc62de4c4bb80a77ba1f
Em 2016 foi realizada a primeira edição do congresso de Inovação - Megatendências 2050.	OK;OK	56f4ba0ea34d91fe386f09dc6871c35c757009b0230a828fa43e48ac08f8d0c	56f4ba0ea34d91fe386f09dc6871c35c757009b0230a828fa43e48ac08f8d0c	5cbf7c58bf9acd451c3bf1b48392a9e6	5cbf7c58bf9acd451c3bf1b48392a9e6
Em 2012 o Centro Universitário FEI celebrou 70 anos de história e de excelência na inovação e na formação de mais de 50 mil profissionais altamente qualificados para o setor empresarial, entre Administradores, Engenheiros e Cientistas da Computação.	OK;OK	2707325bd4929bbbadb422851a2248615bf7998bf3607b6ad934168be6a45859	2707325bd4929bbbadb422851a2248615bf7998bf3607b6ad934168be6a45859	a0a80cbc42bcd7b4b6ab317d0d2efa33	a0a80cbc42bcd7b4b6ab317d0d2efa33
Em 1999 iniciam-se as atividades da FCI (Faculdade de Informática), Como o curso de Ciência da Computação.	Erro;Erro	b2f0457c8c20ccd04e20cd72f06c08140b8ea472d6a6848a5c291319bf9e4a8	b2f0457c8c20ccd04e20cd72f06c08140b8ea472d6a6848a5c291319bf9e4a8	0288b32009adf2f237ba8410f8415e50	0288b32001adf2f237ba8410f8415e50

Figura 2: Tabela 1

3.2 Hashs (SHA256 e MD5, respectivamente) e justificativas com as verificações::

Abaixo as diferenças entre cada resultado calculado e o valor previamente fornecido estão demonstradas em maiores detalhes:

- "A primeira das instituições criadas pelo Pe. Roberto Sabóia de Medeiros foi a antiga Escola Superior de Administração de Negócios de São Paulo - ESAN/SP."

d24de3ec3835115c576a55188a31761b73af93ed2c45a171c810bb66b24b08f9

c850e1a34a6ed572e0758ccd9c615bda

```
A primeira das instituições criadas pelo Pe. Roberto Sabóia de Medeiros foi a antiga Escola Superior de Administração de Negócios de São Paulo - ESAN/SP. - SHA256: OK; MD5: OK

SHA256 calculado: d24de3ec3835115c576a55188a31761b73af93ed2c45a171c810bb66b24b08f9
SHA256 fornecido: d24de3ec3835115c576a55188a31761b73af93ed2c45a171c810bb66b24b08f9

MD5 calculado: c850e1a34a6ed572e0758ccd9c615bda
MD5 fornecido: c850e1a34a6ed572e0758ccd9c615bda
```

Figura 3: Frase 1

- "A FEI é uma instituição vinculada estatutariamente à Companhia de Jesus"

6979a3d7a19e5921ae00ca7db9b814e1b83831dcedfca33dbb72e761ca084337

b710771da8d7521524f45233ea9dd9e1

```
A FEI é uma instituição vinculada estatutariamente à Companhia de Jesus - SHA256: Erro; MD5: Erro

SHA256 calculado: 6979a3d7a19e5921ae00ca7db9b814e1b83831dcedfca33dbb72e761ca084437
SHA256 fornecido: 6979a3d7a19e5921ae00ca7db9b814e1b83831dcedfca33dbb72e761ca084337

MD5 calculado: b710771da8d7521524f45233ea9bb9e1
MD5 fornecido: b710771da8d7521524f45233ea9dd9e1
```

Figura 4: Frase 2

- "Em 20 de janeiro de 1951 foi realizada a sessão solene da congregação para a Colação de Grau da primeira turma da Faculdade de Engenharia Industrial."

6c582a993ba3ea454f11221a374878e534cfe666060c87ba03127de07f1ca4e6

55748c2cb669a9d9508677cb914cb025

```
Em 20 de janeiro de 1951 foi realizada a sessão solene da congregação para a Colação de Grau da primeira turma da Faculdade de Engenharia Industrial. - SHA256: OK; MD5: OK

SHA256 calculado: 6c582a993ba3ea454f11221a374878e534cfe666060c87ba03127de07f1ca4e6
SHA256 fornecido: 6c582a993ba3ea454f11221a374878e534cfe666060c87ba03127de07f1ca4e6

MD5 calculado: 55748c2cb669a9d9508677cb914cb025
MD5 fornecido: 55748c2cb669a9d9508677cb914cb025
```

Figura 5: Frase 3

- "A Capela Santo Inácio de Loyola foi construída no ano de 1978, em concreto aparente."

254e695d0f8835651bc231f9cf1b2a7a097b849648f05f79f1855a55f85b089e

f4a8a299fd4da2a5d70b374be2e48147

```
A Capela Santo Inácio de Loyola foi construída no ano de 1978, em concreto aparente. - SHA256: Erro; MD5: Erro
SHA256 calculado: 245e695d0f8835651bc231f9cf1b2a7a097b849648f05f79f1855a55f85b089e
SHA256 fornecido: 254e695d0f8835651bc231f9cf1b2a7a097b849648f05f79f1855a55f85b089e
MD5 calculado: f4a8a299fd4da2a5d70b374be2e48147
MD5 fornecido: f4a8a299fd4da2a5d70b374be2e48147
```

Figura 6: Frase 4

- "Tendo como função principal a promoção do aprimoramento profissional no campo administrativo e tecnológico, o IECAT (Instituto de Especialização em Ciências Administrativas e Tecnológicas) foi criado em 1982"

d2150d688c337fc57e235adafd57f86d7aba0b8682c249b1006ba592706f88a0

1c4ecc238571333ae507f82ff6a5e9e4

```
Tendo como função principal a promoção do aprimoramento profissional no campo administrativo e tecnológico, o IECAT (Instituto de Especialização em Ciências Administrativas e Tecnológicas) foi criado em 1982 - SHA256: OK; MD5: OK
SHA256 calculado: d2150d688c337fc57e235adafd57f86d7aba0b8682c249b1006ba592706f88a0
SHA256 fornecido: d2150d688c337fc57e235adafd57f86d7aba0b8682c249b1006ba592706f88a0
MD5 calculado: 1c4ecc238571333ae507f82ff6a5e9e4
MD5 fornecido: 1c4ecc238571333ae507f82ff6a5e9e4
```

Figura 7: Frase 5

- "Dentro de uma proposta de integração e de agregação de competências, visando a excelência de seus cursos, as instituições FEI, FCI e ESAN foram transformadas no Centro Universitário da FEI no ano de 2002."

faefb927a21dd282ee00effe42bc0688f649450677a61edce15863a15461b721

98420532cbf1be32a98be579f592cd72

```
Dentro de uma proposta de integração e de agregação de competências, visando a excelência de seus cursos, as instituições FEI, FCI e ESAN foram transformadas no Centro Universitário da FEI no ano de 2002. - SHA256: Erro; MD5: Erro
SHA256 calculado: faefb927a21dd282ee00effe42bc0688f649450677a61edce15863a15461b721
SHA256 fornecido: faefb927a21dd282ee00effe42bc0688f649450677a61edce15863a15461b721
MD5 calculado: 98420532cbf1be32a98be579f592cd72
MD5 fornecido: 98420532cbf1be32a98be579f592cd72
```

Figura 8: Frase 6

- "O Centro Universitário da FEI passou a fazer parte do seleto grupo que produz ciência no Brasil, quando a CAPES aprovou o primeiro curso de Mestrado em Engenharia Elétrica em 2005."

da9f214449005850f4fd552238658820434c15ca06389d018b1814bb376abaa6

2e20bfbece6fdc62de4c4bb80a77ba1f

```
O Centro Universitário da FEI passou a fazer parte do seleto grupo que produz ciência no Brasil, quando a CAPES aprovou o primeiro curso de Mestrado em Engenharia Elétrica em 2005. - SHA256: OK; MD5: OK
SHA256 calculado: da9f214449005850f4fd552238658820434c15ca06389d018b1814bb376abaa6
SHA256 fornecido: da9f214449005850f4fd552238658820434c15ca06389d018b1814bb376abaa6
MD5 calculado: 2e20bfbece6fdc62de4c4bb80a77ba1f
MD5 fornecido: 2e20bfbece6fdc62de4c4bb80a77ba1f
```

Figura 9: Frase 7

- "Em 2016 foi realizada a primeira edição do congresso de inovação - Megatendências 2050."

56f4ba0ea34d91fe386f09dc687f1c35c757009b0230a828fa43e48ac08f8d0c

5cbf7c58bf9acd451c3bf1b48392a9e6

```
Em 2016 foi realizada a primeira edição do congresso de inovação - Megatendências 2050. - SHA256: OK; MD5: OK
SHA256 calculado: 56f4ba0ea34d91fe386f09dc687f1c35c757009b0230a828fa43e48ac08f8d0c
SHA256 fornecido: 56f4ba0ea34d91fe386f09dc687f1c35c757009b0230a828fa43e48ac08f8d0c
MD5 calculado: 5cbf7c58bf9acd451c3bf1b48392a9e6
MD5 fornecido: 5cbf7c58bf9acd451c3bf1b48392a9e6
```

Figura 10: Frase 8

- "Em 2012 o Centro Universitário FEI celebrou 70 anos de história e de excelência na inovação e na formação de mais de 50 mil profissionais altamente qualificados para o setor empresarial, entre Administradores, Engenheiros e Cientistas da Computação."

2707325bd4929bbbadb422851a2248615bf7998bf3607b6ad934168be6a45859

a0a80cbc42bcd7b4b6ab317d0d2efa33

```
Em 2012 o Centro Universitário FEI celebrou 70 anos de história e de excelência na inovação e na formação de mais de 50 mil profissionais altamente qualificados para o setor empresarial, entre Administradores, Engenheiros e Cientistas da Computação. - SHA256: OK; MD5: OK
SHA256 calculado: 2707325bd4929bbbadb422851a2248615bf7998bf3607b6ad934168be6a45859
SHA256 fornecido: 2707325bd4929bbbadb422851a2248615bf7998bf3607b6ad934168be6a45859
MD5 calculado: a0a80cbc42bcd7b4b6ab317d0d2efa33
MD5 fornecido: a0a80cbc42bcd7b4b6ab317d0d2efa33
```

Figura 11: Frase 9

- "Em 1999 iniciam-se as atividades da FCI (Faculdade de Informática), como o curso de Ciência da Computação."

b2ff0457c8c20ccd84e20cd72f06c08140b8ea472d6a6848a5c291319bf9e4a8

0288b32001adf2f237ba8410f8415e50

```
Em 1999 iniciam-se as atividades da FCI (Faculdade de Informática), como o curso de Ciência da Computação. - SHA256: Erro; MD5: Erro  
SHA256 calculado: b2ff0457c8c20ccd04e20cd72f06c08140b8ea472d6a6848a5c291319bf9e4a8  
SHA256 fornecido: b2ff0457c8c20ccd84e20cd72f06c08140b8ea472d6a6848a5c291319bf9e4a8  
MD5 calculado: 0288b32009adf2f237ba8410f8415e50  
MD5 fornecido: 0288b32001adf2f237ba8410f8415e50
```

Figura 12: Frase 10