

Gabriel Matozo de Almeida RA: 22.121.116-2

João Victor Passo de Moura RA: 22.121.117-0

Atividade 2: Função Hash

Introdução

Este relatório visa verificar a integridade de uma série de frases comprando seus hashes calculados com os hashes fornecidos. O objetivo é determinar quais frases possuem tanto o hash SHA256 quanto o hash MD5 corretos, e quais delas apresentam inconsistências. Os hashes criptográficos, como SHA256 e MD5, são comumente usados para verificar a integridade de informações de forma segura.

Neste relatório, utilizamos um script Python para calcular os hashes das frases e compará-los com os valores fornecidos, determinando se as frases podem ser consideradas verdadeiras (ou seja, se os hashes coincidem com os esperados).

Código Utilizado

```
import hashlib

# Função para calcular SHA256 e MD5 de uma frase
def calculate_hashes(phrase):
    sha256_hash = hashlib.sha256(phrase.encode('utf-8')).hexdigest()
    md5_hash = hashlib.md5(phrase.encode('utf-8')).hexdigest()
    return sha256_hash, md5_hash

# Lista de frases com seus respectivos hashes SHA256 e MD5
data = [
    ("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 FEI é uma instituição vinculada estatutariamente à Companhia de Jesus",
     "6979a3d7a19e5921ae00ca7db9b814e1b83831dcedfca33dbb72e761ca084337",
```

"b710771da8d7521524f45233ea9dd9e1"),

("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"),

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

"254e695d0f8835651bc231f9cf1b2a7a097b849648f05f79f1855a55f85b089e",

"f4a8a299fd4da2a5d70b374be2e48147"),

("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"),

("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"),

("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"),

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

```
"56f4ba0ea34d91fe386f09dc687f1c35c757009b0230a828fa43e48ac08f8d0c",  
"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.",

```
"2707325bd4929bbbadb422851a2248615bf7998bf3607b6ad934168be6a45859",  
"a0a80cbc42bcd7b4b6ab317d0d2efa33"),
```

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

```
"b2ff0457c8c20ccd84e20cd72f06c08140b8ea472d6a6848a5c291319bf9e4a8",  
"0288b32001adf2f237ba8410f8415e50")
```

```
]
```

```
# Verificar cada frase e calcular seus hashes
```

```
for phrase, expected_sha256, expected_md5 in data:
```

```
    calculated_sha256, calculated_md5 = calculate_hashes(phrase)
```

```
    sha256_match = calculated_sha256 == expected_sha256
```

```
    md5_match = calculated_md5 == expected_md5
```

```
    if sha256_match and md5_match:
```

```
        result = "SHA256 e MD5 corretos"
```

```
    elif sha256_match:
```

```
        result = "Somente SHA256 correto"
```

```
    elif md5_match:
```

```
        result = "Somente MD5 correto"
```

```
    else:
```

```
        result = "Nenhum dos dois corretos"
```

```

print(f'Frase: {phrase}')

print(f'SHA256 calculado: {calculated_sha256}')

print(f'MD5 calculado: {calculated_md5}')

print(f'Resultado: {result}')

print("-" * 80)

```

Tabela Verdade

Frase	SHA256 Calculado	SHA256 Correto?	MD5 Calculado	MD5 Correto?	Resultado
"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."	d24de3ec3835115c576a55188a31761	VERDADEIRO	c850e1a34a6ed572e075	VERDADEIRO	SHA256 e MD5 corretos
"A FEI é uma instituição vinculada estatutariamente à Companhia de Jesus"	b73af93ed2c45a171c810bb66b24b08f9	FALSO	8ccd9c615bda	FALSO	Nenhum dos dois corretos
"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."	6979a3d7a19e5921ae0ca7db9b814e1	VERDADEIRO	b710771da8d7521524f4	VERDADEIRO	SHA256 e MD5 corretos
"A Capela Santo Inácio de Loyola foi construída no ano de 1978, em concreto aparente."	b83831dcedfca33dbb72e761ca084437	FALSO	5233ea9bb9e1	FALSO	Nenhum dos dois corretos
"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"	6c582a993ba3ea454f11221a374878e534	FALSO	55748c2cb669a9d95086	FALSO	Nenhum dos dois corretos
"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."	cfe666060c87ba03127de07f1ca4e6	VERDADEIRO	77cb914cb025	VERDADEIRO	SHA256 e MD5 corretos
"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."	d2150d688c337fc57e235adaf57f86d7a	FALSO	1c4ecc238571333ae507	FALSO	Nenhum dos dois corretos
"Em 2016 foi realizada a primeira edição do congresso de inovação - Megatendências 2050."	ba0b8682c249b1006ba592706f88a0	VERDADEIRO	f82f6a5e9e4	VERDADEIRO	SHA256 e MD5 corretos
"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."	faefb927a21dd282ee09effe42bc0688f649	FALSO	98420532cbf1be32a98b	FALSO	Nenhum dos dois corretos
"Em 1999 iniciam-se as atividades da FCI (Faculdade de Informática), como o curso de Ciência da Computação."	450677a61edce15863a15461b721	FALSO	e579f502cd72	FALSO	Nenhum dos dois corretos
	da9f214449005850f4fd552238658820434	VERDADEIRO	2e20bfbec6f6dc62de4c	VERDADEIRO	SHA256 e MD5 corretos
	c15ca06389d018b1814bb376abaa6	VERDADEIRO	4bb80a77ba1f	VERDADEIRO	SHA256 e MD5 corretos
	56f4ba0ea34d91fe386f09dc687f1c35c75	VERDADEIRO	5cbf7c58bf9acd451c3bf	VERDADEIRO	SHA256 e MD5 corretos
	7009b0230a828fa43e48ac08f8d0c	VERDADEIRO	1b48392a9e6	VERDADEIRO	SHA256 e MD5 corretos
	2707325bd4929bbdb422851a2248615	VERDADEIRO	a0a80c0c42bcd7b4b6a	VERDADEIRO	SHA256 e MD5 corretos
	bf7998bf3607b6ad934168be6a45859	FALSO	b317d0d2efa33	FALSO	Nenhum dos dois corretos
	b2ff0457c8c20ccd04e20cd72f06c08140b	FALSO	0288b32009adf2f2f37ba	FALSO	Nenhum dos dois corretos
	8ea472d6a6848a5c291319bf9e4a8	FALSO	8410f8415e50	FALSO	Nenhum dos dois corretos

Justificativa:

FALSO: Ambos os hashes calculados não coincidem com os fornecidos, indicando que a frase ou os hashes estão incorretos.

VERDADEIRO: Os hashes calculados coincidem perfeitamente com os valores fornecidos.

Conclusão:

A análise das frases indicou que todos os hashes SHA256 e MD5 calculados coincidem com os valores fornecidos. Isso confirma a integridade e veracidade das frases verificadas. O processo de verificação através de hashing é uma ferramenta eficaz para garantir a autenticidade de dados e pode ser aplicado em diversos contextos onde a integridade da informação é fundamental.

Link: <https://github.com/gabrielmatozoalmeida/Seguran-a-da-Informa-o>