Atividade: Criptografia em Java ou Python

UNIVERSIDADE SÃO JUDAS TADEU – CAMPUS MOOCA

CIÊNCIAS DA COMPUTAÇÃO

RAFAELA MARIA DA SILVA – ATIVIDADE MINISTRADA POR PROFESSOR ROBSON CALVETTI.

SÃO PAULO

2025

1. Criptografia Simétrica em Python

A criptografia simétrica utiliza a mesma chave para criptografar e descriptografar os dados. Um exemplo comum é o algoritmo AES (Advanced Encryption Standard). Vamos utilizar a biblioteca cryptography.

Bash: pip install cryptography

Python: from cryptography.fernet import Fernet

# Gerar uma chave simétrica

key = Fernet.generate\_key()

cipher = Fernet(key)

# Mensagem a ser criptografada

mensagem = b"Aula 06 do professor Calvetti criptografando em Python"

# Criptografar a mensagem

criptografada = cipher.encrypt(mensagem)

print("Mensagem Criptografada:", criptografada)

# Descriptografar a mensagem

descriptografada = cipher.decrypt(criptografada)

print("Mensagem Descriptografada:", descriptografada.decode())

2. Criptografia Assimétrica em Python:

Na criptografia assimétrica, utilizamos um par de chaves (pública e privada). Vamos usar a biblioteca cryptography com o algoritmo RSA.

Python: from cryptography.hazmat.primitives.asymmetric import rsa

from cryptography.hazmat.primitives.asymmetric import padding

from cryptography.hazmat.primitives import hashes

# Gerar chaves pública e privada

private\_key = rsa.generate\_private\_key(public\_exponent=65537, key\_size=2048)

public\_key = private\_key.public\_key()

# Mensagem a ser criptografada

mensagem = b"Aula 06 do professor Calvetti criptografando em Python"

# Criptografar com a chave pública

criptografada = public\_key.encrypt(

mensagem,

padding.OAEP(mgf=padding.MGF1(algorithm=hashes.SHA256()),

algorithm=hashes.SHA256(),

label=None)

)

print("Mensagem Criptografada:", criptografada)

# Descriptografar com a chave privada

descriptografada = private\_key.decrypt(

criptografada,

padding.OAEP(mgf=padding.MGF1(algorithm=hashes.SHA256()),

algorithm=hashes.SHA256(),

label=None)

)

print("Mensagem Descriptografada:", descriptografada.decode())

3. Função Hash em Python

As funções hash geram valores únicos e fixos para entradas específicas, mas não permitem a reversão para o dado original. Um exemplo popular é o SHA-256.

Python: import hashlib

# Mensagem a ser criptografada

mensagem = "Aula 06 do professor Calvetti criptografando em Python"

# Gerar o hash (SHA-256)

hash\_obj = hashlib.sha256(mensagem.encode())

hash\_gerado = hash\_obj.hexdigest()

print("Hash Gerado (SHA-256):", hash\_gerado)