

Implementação de Criptografia Assimétrica e Simétrica

Objetivo:

Vocês como analistas e desenvolvedores de sistemas, deverão implementar dois tipos de criptografia em Java: assimétrica (RSA) e simétrica (AES).

Instruções:

1. Grupo ou Individual

Cada grupo/aluno será responsável por implementar **duas soluções**: uma para **criptografia assimétrica** e outra para **criptografia simétrica**.

2. Etapas da Atividade:

Parte 1: Criptografia Assimétrica (RSA)

- Implemente a criptografia assimétrica utilizando RSA.
- O programa deve gerar um par de chaves (pública e privada) para dois "usuários fictícios", como Wallace e Arthur, por exemplo.
- **Wallace** enviará uma mensagem criptografada para **Arthur**, usando a chave pública de **Arthur**, e **Arthur** deverá descriptografar a mensagem usando sua chave privada.
- Faça o inverso: Arthur enviará uma mensagem criptografada para Wallace.

Requisitos:

- Gere as chaves pública e privada usando o algoritmo RSA.
- Implemente métodos para **criptografar** e **descriptografar** as mensagens.
- Exiba no console as mensagens criptografadas e descriptografadas.

Dica: Use a classe '**Cipher**' disponível no pacote '**javax.crypto**' para realizar as operações de criptografia/descriptografia.

Parte 2: Criptografia Simétrica (AES)

- Implemente a criptografia simétrica utilizando o algoritmo AES.
- O programa deve usar uma única **chave secreta** para criptografar e descriptografar as mensagens.
- Uma mensagem deverá ser criptografada, e depois a mesma mensagem deverá ser descriptografada, demonstrando o funcionamento da criptografia simétrica.

Requisitos:

- Utilize o algoritmo AES para gerar uma chave secreta.
- Implemente métodos para criptografar e descriptografar a mensagem.

--	--	--

- Exiba no console as mensagens criptografadas e descriptografadas.

Dica: Utilize o **'Cipher'** para realizar a criptografia/descriptografia com AES.

3. Discussão Final: Comparação de Algoritmos

Após a implementação, os alunos devem responder às seguintes questões e discutir os resultados:

1. Qual algoritmo é mais rápido? Teste o desempenho ao criptografar/descriptografar grandes mensagens.
2. Em que situação você utilizaria criptografia assimétrica?
3. Quando a criptografia simétrica é mais adequada?
4. Explique como os dois algoritmos podem ser combinados (modelo híbrido) para maximizar a segurança e o desempenho.

Entrega:

- O código fonte das duas implementações.
- Um relatório curto explicando as diferenças entre criptografia assimétrica e simétrica com base na experiência prática da atividade.

Material de Apoio:

- Revise as classes do Java: **'Cipher'**, **'KeyPairGenerator'**, **'SecretKey'**, **'KeyGenerator'**.

--	--	--