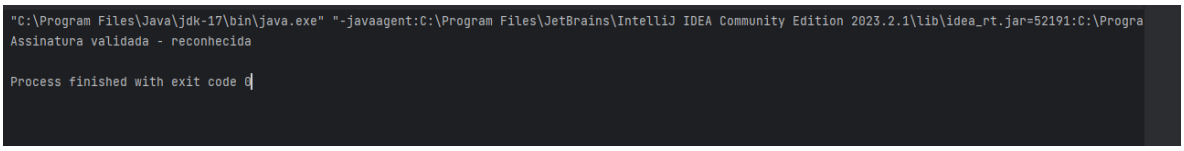
Segurança Informática e de Redes de Computadores

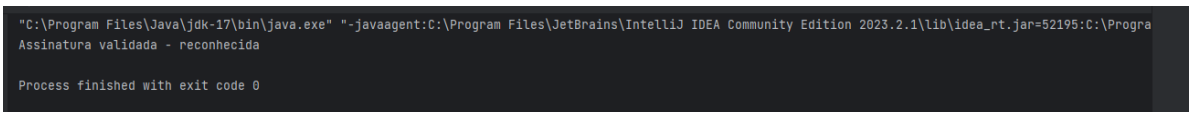
Nome: Mateus Fernando Jó Matazeus

LAB2

1. a) O código PKCS1SignatureExample demonstra como fazer uma assinatura digital usando o algoritmo RSA com a função de síntese SHA-1 subjacente à assinatura. A função de síntese SHA-1 é usada para calcular um resumo (hash) da mensagem que será assinada. Em seguida, esse hash é assinado com a chave privada do remetente para criar a assinatura digital. Pode-se ver os resultados abaixo:
   Com SHA1withRSA:



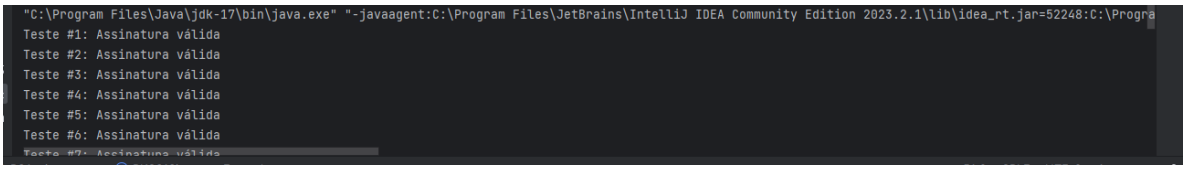
   Com SHA256withRSA:



   b) O tamanho das assinaturas geradas depende do tamanho da chave usada para o algoritmo RSA. No código fornecido, uma chave de 512 bits é usada, o que resultará em assinaturas de tamanho proporcional a essa chave.

   c) O valor da assinatura é sempre diferente em diferentes corridas do programa, mesmo com a mesma mensagem, porque o processo de assinatura inclui uma componente aleatória. A geração de um par de chaves RSA envolve a geração de números aleatórios, e essa aleatoriedade é usada no processo de assinatura. Criando um loop de 10 repetições é

possível verificar valor da assinatura. Se a assinatura não for válida o loop será quebrado, no resultado abaixo é possível verificar que todas os valores são válidos:



d) Para produzir e verificar uma assinatura digital usando o algoritmo DSA (Digital Signature Algorithm), deve-se substituir as partes específicas do algoritmo RSA pelas correspondentes do DSA. Isso inclui a geração de um par de chaves DSA, a inicialização do objeto Signature com "SHA1withDSA" (ou outro algoritmo DSA suportado) e a substituição do uso de initSign e initVerify pelas funções correspondentes do DSA. O resultado verifica-se abaixo: