Segurança Informática e de Redes de Computadores

Laboratório 3

Djocodjo Lourenço Pihale

1.a) No código fornecido, a função de síntese subjacente à assinatura é hash SHA-1.

1.b) No trecho do código keyGen.initialize(512, new SecureRandom()); podemos ver o tamanho da assinatura gerada é determinado pelo tamanho da chave RSA usada para a assinatura. O tamanho da assinatura gerada será de 512 bits. O tamanho é esperado, Isso acontece porque o RSA cria uma assinatura criptografando o resumo da mensagem com a chave privada. A criptografia RSA produz uma saída do mesmo tamanho que a chave.

1.c) A assinatura será diferente em diferentes execuções do programa se um elemento de aleatoriedade for introduzido no processo de assinatura. No código que você forneceu, a aleatoriedade é introduzida através do uso de SecureRandom durante a geração do par de chaves e Utils3.createFixedRandom() durante a inicialização da assinatura.

SecureRandom é uma classe em Java que fornece um gerador de números pseudoaleatórios criptograficamente forte. Utils3.createFixedRandom() é uma função personalizada que provavelmente retorna uma instância de SecureRandom ou similar.