LABORATÓRIO 2_3

Nome:**Dhulkifly Amisse Malique**

1.Duma forma resumida dando detalhe para o algoritmo de hash: openssl speed **md5 sha1 sha256 sha512**

Chave privada RSA de **512** bits: tem um nivel de Muito Baixo não é recomendado para a maioria das aplicações.

Chave privada RSA de **1024** bits:é o melhor em relacão a privk 512,é considerado fraco para aplicações modernas.

Chave privada RSA de **2048** bits

Nível de segurança: Moderado (adequado para muitas aplicações, mas pode ser necessário atualizar no futuro

Chave privada RSA de 4096 bits: Nível de segurança: Alto (considerado seguro para a maioria das aplicações).

2.1a) O tamanho das chaves RSA utilizadas é de 512 bits, como especificado pelas chaves fornecidas nos objetos `RSAPublicKeySpec` e `RSAPrivateKeySpec`.

b) O valor da chave pública RSA (exponente público) é 17 em hexadecimal, e o valor do módulo N é "d46f473a2d746537de2056ae3092c451" em hexadecimal. O valor da chave privada RSA (exponente privado) é "57791d5430d593164082036ad8b29fb1" em hexadecimal.

c) Não faz sentido o tamanho do ciphertext produzido ser maior do que o tamanho do módulo N subjacente à operação de módulo nas chaves RSA. Isso ocorre porque, na cifra RSA sem padding, o ciphertext não é reduzido automaticamente para caber no módulo N, o que pode levar a problemas de decifração.

e) Se o bloco de plaintext for maior em dimensão do que o valor N subjacente à operação mod e às chaves usadas, ocorrerá um erro. Isso não faz sentido, pois a operação **RSA** requer que o plaintext seja menor ou igual ao valor N, caso contrário, a cifragem não é possível.

f) O código fornecido não utiliza padding. Isso pode levar a problemas de segurança.

2.3A)O código fornecido demonstra o uso do padding PKCS#1 com o algoritmo RSA para criptografia de dados.

PKCS#1 é um padrão de preenchimento que é usado para garantir que os blocos de dados a serem criptografados.
No código fornecido, a implementação utiliza o PKCS#1 v1.5, pois realiza o preenchimento com bytes 0x00, 0x01 e dados aleatórios antes de criptografar. Isso é evidenciado na linha onde cria-se o objeto Cipher com o argumento "RSA/NONE/PKCS1Padding".

LAB_3

KCS1SignatureExample.java

a) O código realiza assinaturas digitais usando RSA e a função de síntese subjacente é SHA-1. Você pode experimentar outras configurações de assinatura.

b) O tamanho da assinatura depende do tamanho da chave usada. No código fornecido, uma chave de 512 bits resulta em uma assinatura de 512 bits.

c) As assinaturas são diferentes em cada execução devido à aleatoriedade introduzida pelo SecureRandom personalizado.

d) Para usar DSA em vez de RSA, faça alterações específicas no código, como inicialização e uso das chaves DSA.