

Trabalho de Implementação

Gerador/Verificador de Assinaturas

Como atividade de implementação, deve-se implementar um gerador e verificador de assinaturas RSA em arquivos. Assim, deve-se implementar um programa com as seguintes funcionalidades:

- Geração de chaves (mínimo de 1024 bits)
- Assinatura
 1. Cálculo de hashes (função de hash SHA-3)
 2. Assinatura da mensagem (cifração do hash)
 3. Formatação do resultado (caracteres especiais e informações para verificação)
- Verificação
 1. Parsing do documento assinado (de acordo com a formatação usada)
 2. Decifração da assinatura (decifração do hash)
 3. Verificação (cálculo e comparação do hash do arquivo)

Observações:

1. Permite-se a utilização de bibliotecas públicas para aritmética modular e função de hash.
2. Não é permitida a utilização de bibliotecas públicas, como OpenSSL, para primitivas de criptográficas de cifração e decifração assimétrica, e geração de chaves.
3. A pontuação máxima será auferida os trabalhos que realmente implementarem as seguintes primitivas:
 - a. geração de chaves com teste de primalidade (Miller-Rabin)
 - b. cifração e decifração RSA
 - c. OAEP
 - d. formatação/parsing
4. A avaliação será mediante apresentação do trabalho, com a verificação das funcionalidades e inspeção do código.
5. Implementação preferencialmente individual, podendo ser em dupla. Linguagens preferenciais C, C++, Java e Python.

O que deve ser entregue: o código fonte e seu executável, descritivo (4 pg max) da assinatura RSA e do programa.

Data de Entrega: 10/05/2021, por email até 10h.

Apresentações: a partir de 10/05/2021