CIC0201 - Segurança Computacional - 2025/2

Profa. Priscila Solis Barreto

Trabalho de Implementação 2

Gerador/Verificador de Assinaturas

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

- Parte I: Geração de chaves e cifra
  a. Geração de chaves (p e q primos com no mínimo de 1024 bits)
  b. Cifração/decifração assimétrica RSA usando OAEP.
- Parte II: Assinatura
  1. Cálculo de hashes da mensagem em claro (função de hash SHA-3)
  2. Assinatura da mensagem (cifração do hash da mensagem)
  3. Formatação do resultado (caracteres especiais e informações para verificação em BASE64)
- Parte III: Verificação:
  1. Parsing do documento assinado e decifração da mensagem (de acordo com a formatação usada, no caso BASE64)
  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 simétrica e assimétrica, bem como de geração de chaves.
3. A pontuação máxima será conferida 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 em grupos de 3 pessoas. Linguagens preferenciais C, C++, Java e Python.

Data de Entrega e Apresentações : 09/10/2025, plataforma Moodle, até 23:55h.