Universidade de Brasília – UnB

Departamento de Ciência da Computação - CIC

Disciplina: Segurança Computacional – 2025/1

Professora: Lorena Borges

Trabalho Prático 03

Roteiro de Programação: Gerador/Verificador de Assinaturas

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

Parte 1 – Geração de chaves e cifra

a. Geração de chaves (mínimo de 1024 bits, recomendado ≥ 2048 bits para maior segurança).
b. Serializar e armazenar as chaves em formato seguro (PEM/Base64).
c. Cifração/decifração assimétrica RSA-PSS

Parte 2 – Assinatura

a. Cálculo de hashes da mensagem em claro (função de hash SHA-3)
b. Implementar padding padrão PSS (Probabilistic Signature Scheme) para assinatura digital com RSA
c. Assinatura da mensagem (cifração do hash da mensagem)
d. Formatação do resultado (caracteres especiais e informações para verificação em BASE64)

Parte 3 – Verificação

a. Parsing do documento assinado e decifração da mensagem (de acordo com a formatação usada, no caso BASE64)
b. Decifração da assinatura (decifração do hash)
c. Verificação (cálculo e comparação do hash do arquivo)

Observações:

- Permite-se a utilização de bibliotecas públicas para aritmética modular e função de hash.
- Não é permitida a utilização de bibliotecas públicas, como OpenSSL, para primitivas criptográficas de cifração e decifração simétrica e assimétrica, bem como de geração de chaves.
- A pontuação máxima será conferida aos trabalhos que realmente implementarem as seguintes primitivas:
    i. geração de chaves com teste de primalidade (Miller-Rabin)
    ii. cifração e decifração RSA
    iii. formatação/parsing
- Implementação em grupo, preferencialmente em dupla. Linguagens preferenciais C, C++, Java e Python.