

**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 simétrica
  - a. Geração de chaves (p e q primos com no mínimo de 1024 bits)
  - b. Geração de chave simétrica de sessão
  - c. Cifração simétrica de mensagem (AES modo CTR),
  - d. Cifração assimétrica da chave de sessão, 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
  - e. AES modo CTR
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), do AES-CTR, da assinatura RSA e do programa.

Data de Entrega: 01/05/2022, por email até 23:59h.

Apresentações: 02 e 04/05/2022