Criptografia RSA com OAEP e SHA3-256

Implementação de Geração de Chaves, Assinatura Digital e Verificação

Alunos:
Lucas Alves Rodrigues
Jean Bueno Karia

Introdução Teórica

- Segurança na comunicação assimétrica
  - Proteção contra Ataques
    - Resistência a CPA (Chosen-Plaintext Attacks) via padding estruturado
    - Ataques de Plaintext:
      - OAEP adiciona aleatoriedade ao processo de cifração
      - Evita padrões identificáveis no texto cifrado (ex: mesma mensagem → cifras diferentes)
- Pilares da Segurança:
  - RSA: Baseado na dificuldade de fatoração de primos grandes
  - OAEP: Transforma cifração determinística em probabilística (padding)
  - SHA3-256: Garante unicidade do hash (resistência a colisões)

Introdução Teórica

- Garantias Obtidas
  - Autenticidade:
    - Assinatura vinculada à chave privada única do remetente
    - Verificação via chave pública correspondente
  - Integridade:
    - Hash SHA3-256 detecta alterações de 1 bit na mensagem

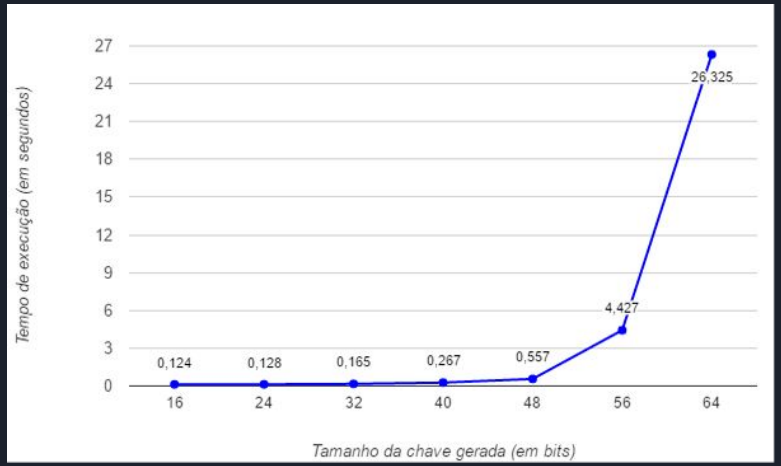
Arquitetura do Programa

- Geração de Chaves (Miller-Rabin)
- Primos de 1024 bits
- Cálculo de n, φ(n), e, d
- Assinatura Digital:
  - Hash SHA3-256 → OAEP → RSA (privada) → Base64
- Verificação:
  - Base64 → RSA (pública) → $OAEP^{-1}$ → Validação do Hash

Geração de Chaves

- Algoritmo Miller-Rabin
  - Teste probabilístico (40 iterações ≈ 2^{-80} erro)

- Chaves RSA:
  - Pública: (n, e)
  - Privada: (n, d)



Assinatura Digital

- Processo de Codificação OAEP
  - Hash do Rótulo (Label) - l_hash = SHA3-256(b"")
  - Construção do Bloco de Dados (DB)
    - DB = l_hash || PS || 0x01 || mensagem
    - PS: Preenchimento com bytes 0x00 para ajustar tamanho
    - 0x01: Delimitador único para separar padding da mensagem
  - Seed aleatório + MGF1 (XOR duplo)
    - Garante aleatoriedade mesmo para mensagens idênticas
    - Função de máscara baseada em SHA3-256
  - Resultado: 0x00 || masked_seed || masked_DB
- SHA3-256:
  - Resistente a colisões
  - Saída fixa de 256 bits

Verificação

- Fluxo de Validação
  - Decodificação Base64 → Inteiro
  - RSA com chave pública: S^e mod n
  - OAEP Decode:
    - Extração do seed
    - Reversão das máscaras MGF1
  - Comparação byte-a-byte dos hashes
- Vantagens:
  - Não repúdio
  - Detecção de adulteração

Implementação

- Desafios e Soluções
  - Manipulação de big integers (os2ip/i2osp)
  - Compatibilidade de encoding (UTF-8/BASE64)/
- Bibliotecas:
  - hashlib (SHA3)
  - secrets (primos seguros)
  - base64