Relatório - Trabalho 3

Alunos

- Nataly Lacerda de Oliveira - 190093838
- Pedro Henrique dos Santos - 200026127

Introdução

O objetivo deste trabalho é implementar um gerador e verificados de assinaturas RSA. O trabalho divide-se nas seguintes partes:

- Parte I: Geração de chaves e cifra
    1. Geração de chaves (p e q primos com no mínimo de 1024 bits)
    2. 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)

Cifração

RSA

O algoritmo RSA é um algoritmo de criptografia assimétrica baseado na dificuldade de fatorar o produto de dois números primos grandes. Consiste em três etapas principais: geração de chaves, criptografia e descriptografia:

Geração de Chaves:

1. **Escolha de Números Primos:** Seleção de dois números primos grandes e distintos, geralmente denotados por p e q.
2. **Cálculo de N:** N é o produto dos números primos selecionados, ou seja, $N=p\times q$.
3. **Cálculo da Função Totiente de Euler $\varphi(N)$:** $\varphi(N)$ é o número de inteiros positivos menores que N e coprimos com N. Para primos, $\varphi(N)=(p-1)\times(q-1)$.
4. **Escolha do Expoente Público e:** e é um número inteiro coprimo com $\varphi(N)$, geralmente um número pequeno, como 65537 (um primo comum).
5. **Cálculo do Expoente Privado d:** d é o inverso multiplicativo modular de e em relação a $\varphi(N)$, ou seja, $d\times e\equiv 1 (\mod \varphi(N))$.

As chaves são então geradas: a chave pública (N,e) e a chave privada (N,d).

Criptografia:

Para criptografar uma mensagem M:

1. A mensagem é representada como um número inteiro m no intervalo $[0,N-1]$.
2. A mensagem é criptografada utilizando a chave pública (N,e) através da operação $C\equiv Me (\mod N)$.
3. C é o texto cifrado resultante.

Descriptografia:

Para descriptografar o texto cifrado C e obter a mensagem original M:

1. O texto cifrado C é descriptografado utilizando a chave privada (N,d) através da operação $M\equiv Cd (\mod N)$.
2. M é a mensagem original recuperada.

RSA-OAEP

RSA-OAEP (Optimal Asymmetric Encryption Padding) é uma extensão do algoritmo RSA que oferece maior segurança e outras propriedades desejáveis, especialmente quando usado para criptografar dados de forma segura.

O RSA-OAEP combina o algoritmo RSA com o esquema de padding OAEP para proteger a confidencialidade dos dados e reduzir os riscos de ataques de criptoanálise.

Funcionamento do RSA-OAEP:

1. **Geração de Parâmetros:**
    - RSA: Geração das chaves pública e privada conforme o procedimento padrão do RSA.
    - OAEP: Seleção de funções de hash seguras, como SHA-1 ou SHA-256.
2. **Padding (OAEP):**
    - O padding OAEP inclui duas operações principais: padding e uma função de hash.
    - A mensagem original é expandida para um comprimento fixo usando um algoritmo de padding.
    - Uma função de hash é aplicada à mensagem para introduzir aleatoriedade e tornar o ataque mais difícil.
    - Adição de uma máscara aleatória para aumentar a aleatoriedade e dificultar a análise estatística.
3. **Criptografia:**
    - Geração de uma chave de sessão aleatória para cada mensagem.
    - Aplicação da função de hash na chave de sessão e na mensagem expandida (após o padding).
    - A combinação da chave de sessão com a mensagem é criptografada usando a chave pública RSA.
4. **Descriptografia:**
    - Utilização da chave privada RSA para descriptografar a combinação de chave de sessão e mensagem.
    - Recuperação da chave de sessão.
    - Inversão da operação de hash da chave de sessão para obter a mensagem expandida.
    - Reversão do padding para obter a mensagem original.

Benefícios do RSA-OAEP:

1. **Proteção contra Ataques de Preenchimento (Padding):** OAEP reduz o risco de ataques baseados no padding utilizado no RSA padrão.
2. **Resistência a Ataques de Mãos Meio (Man-in-the-middle):** A inclusão de uma máscara aleatória ajuda a evitar ataques de substituição de mensagens.
3. **Segurança contra Ataques de Adaptação Chosen-Ciphertext (CCA):** Oferece segurança contra determinados tipos de ataques que exploram mensagens cifradas.

O RSA-OAEP é uma melhoria significativa sobre o RSA básico, proporcionando uma camada adicional de segurança e prevenindo muitos tipos de ataques criptográficos. É amplamente utilizado em sistemas de segurança que requerem criptografia robusta e eficiente.

Implementação

Realizamos a implementação da criação da chave pública e privada. E a crifração com RSA. Não conseguimos implementar o OAEP e as assinaturas.

Conclusão

Conseguimos entender bem como funciona a cifra e a implementamos corretamente. Seguimos o vídeo de orientação para a implementação da quebra da cifra, mas não tivemos sucesso. Não entendemos como exatamente poderiamos fazer para dar match nos valores da cifra com a do alfabeto. Então apesar de ficar um pouco perdidos nessa parte, deu pra passear bastante nos conceitos da cifra, e acredito que com um pouquinho mais de tempo podemos fazer uma implementação completa.