Trabalho de Implementação 2
Gerador/Verificador de Assinaturas

Bruno Vargas de Souza - 202006564
Gustavo Pierre Starling - 202006420

[1]Dep. Ciência da Computação – Universidade de Brasília (UnB)
CIC0201 - Segurança Computacional

1. Introdução

[Katz and Lindell 2007]

AES (Advanced Encryption Standard) constitui um algoritmo de criptografia, o qual opera em blocos de dados de 128 bit. O AES é considerado seguro e eficiente em termos de desempenho, sendo adotado em diversas aplicações para segurança de dados.

Já o RSA (Rivest, Shamir e Adleman) consiste em um algoritmo de criptografia assimétrica que se baseia na utilização de chaves pública e privada. A segurança do RSA está fundamentada na dificuldade computacional de fatorar números primos muito grandes, garantindo assim a confidencialidade e autenticidade das informações transmitidas.

O OAEP (Optimal Asymmetric Encryption Padding) é um esquema de padding utilizado no RSA e que proporciona maior segurança ao adicionar aleatoriedade aos dados antes da cifração, dificultando ataques baseados em padrões conhecidos.

A assinatura digital, utilizando o algoritmo RSA, consiste em uma técnica que garante a autenticidade de informações digitais. A mensagem é criptografada com a chave privada do remetente, gerando uma assinatura. O destinatário utiliza a chave pública correspondente para descriptografar a assinatura e comparar com o hash da mensagem recebida. Se forem iguais, a assinatura é considerada válida, garantindo a autenticidade e integridade dos dados.

2. AES

[Wikipedia 2005]

O AES (Advanced Encryption Standard) é um método de criptografia com chave simétrica, que pode ter tamanho de 128, 192 ou 256 bits, mas deve ser um múltiplo de 32 bits. O AES faz operações em uma matriz 4x4 composta por bytes dentro dela, 16 bytes por padrão. Para cifrar, o algoritmo faz diversas operações X vezes dependendo do tamanho da chave. Dentre as operações são elas:

- Expand Key
- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

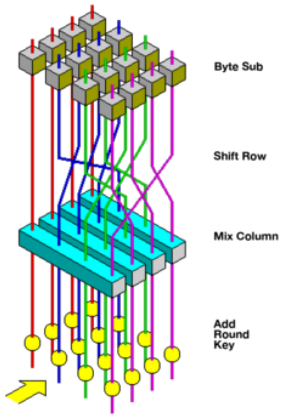

Figure 1. Operações realizadas na matriz 4x4

2.1. Expand Key

Na expansão de chave, ele pega os 16 bytes da chave e produz um novo de 176 bytes, que é o suficiente para fazer o Add Round Key 10 vezes.

2.2. Sub Bytes

Nessa operação, cada byte é substituído por algum outro byte de uma matriz fixa definida anteriormente

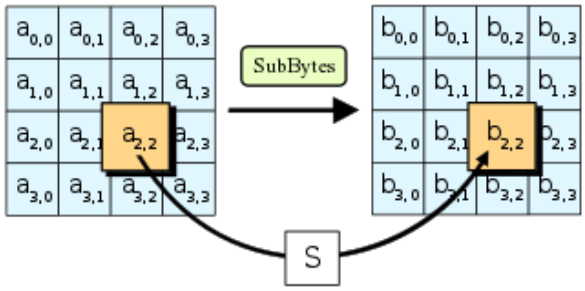

Figure 2. Sub Bytes

2.3. Shift Rows

Nessa etapa, o algoritmo irá shiftar as linhas de uma maneira cíclica, 1 shift na segunda linha, 2 shifts na terceira linha, 3 shifts na quarta linha.

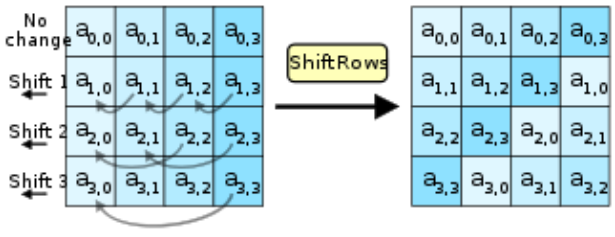

Figure 3. Shift Rows

2.4. Mix Columns

Para fazer o Mix Columns, o algoritmo pega cada coluna e faz a operação xor com uma coluna fixa da outra matriz, substituindo assim, a matriz original.

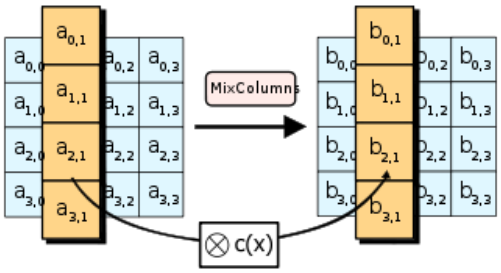

Figure 4. Mix Columns

2.5. Add Round Key

[Brainkart 2023]

No Add Round Key, ele pega a matriz original, e para cada rodada, ele pega um byte da matriz e faz a operação xor com a chave na respectiva rodada

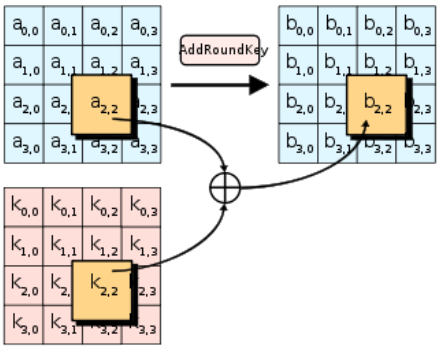

Figure 5. Add Round Key

3. RSA

[Akasatanahama] O RSA constitui um sistema de criptografia para a transmissão segura de dados, para isso, faz-se necessário gerar dois números primos de 1024 bits. Nesse contexto, a fim de testar a primalidade utiliza-se o algoritmo de Miller-Rabin que consiste em um teste probabilistico baseado no teorema de Fermat, o qual afirma que se um número primo p divide um número composto n, então $n^{p-1} \equiv 1(modp)$.

Desse modo, após obter os dois números primos, calcula-se a função totiente de Euler e o inverso modular através do algoritmo de Euclides estendido com o intuito de gerar as chaves do RSA. Além disso, para realizar a encriptação, faz-se: $m^e \equiv c(modn)$ e para a decriptação: $c^d \equiv m(modn)$

4. OAEP

[Wikipedia] Utiliza-se o OAEP (Optimal Asymmetric Encryption Padding) com o algoritmo RSA para introduzir aleatoriedade aos dados antes da criptografia e remove essa aleatoriedade durante a descriptografia, a fim de dificultar a extração de informações dos dados criptografados. Dessa forma o OAEP utiliza duas funções de hash criptográficas: SHA3-256 e a MGF1.

Nesse sentido, o OAEP após receber a mensagem à ser cifrada, cria uma hash de 32 bytes utilizando o SHA3-256 que é combinada com uma seed aleatoria de mesmo valor, após isso passa pela MGF1 para gerar uma máscara aleatória. Assim, a máscara

é aplicada aos dados de entrada antes de serem criptografados usando o RSA. Já para descriptografar os dados, aplica-se o RSA e obtém os dados encriptados com a máscara. Em seguida, a máscara é removida e o resultado é desmascarado, utilizando o MGF1 novamente.

5. Assinatura

A assinatura RSA com OAEP constitui um esquema de assinatura digital que combina o algoritmo de assinatura RSA com o esquema de padding OAEP, a fim de proporcionar maior segurança aos dados. Nesse contexto, a assinatura é gerada criptografando o resultado do padding usando a chave privada RSA.

Em relação à verificação da assinatura, realiza a descriptografia da assinatura recebida usando a chave pública, obtendo o resultado do padding OAEP. Após isso, gera a hash e compara o resultado do padding OAEP com o hash gerado, caso os valores forem iguais, a assinatura é considerada válida e que os dados não foram alterados.

6. Conclusão

Em resumo, o trabalho implementa de forma abrangente as criptografias AES, RSA, OAEP e Assinatura RSA com OAEP. Essas técnicas fornecem um ambiente seguro para a troca de informações confidenciais, garantindo a confidencialidade, autenticidade e integridade dos dados. O AES protege os dados através de operações em blocos, enquanto o RSA, em conjunto com o OAEP, utiliza chaves pública e privada para criptografia assimétrica e assinatura digital. Essas abordagens combinadas proporcionam segurança robusta, assegurando que os dados permaneçam confidenciais, não sejam adulterados e provenham de remetentes autênticos. O trabalho demonstra uma compreensão aprofundada dessas técnicas e a importância de sua implementação adequada para a proteção de dados sensíveis.

References

[Akasatanahama] Akasatanahama. Rsa guide.

[Brainkart 2023] Brainkart (2023). Aes key expansion.

[Katz and Lindell 2007] Katz, J. and Lindell, Y. (2007). *Introduction to Modern Cryptography*. CRC Press, 1th edition.

[Wikipedia] Wikipedia. Oaep.

[Wikipedia 2005] Wikipedia (2005). Advanced encryption standard.