Departamento de Ciência da Computação

Segurança Computacional

2º EXERCÍCIO
AES, RSA e ASSINATURA DIGITAL

Trabalho apresentado à Universidade de Brasília, como pré-requisito para obtenção de nota parcial, referente à avaliação do semestre, na disciplina de Segurança Computacional, relativo ao primeiro semestre de 2023.

ECL0014
Professor: João José Costa Gondim.
Discente: Vinícius Giovani Moreira Nascimento – 170115437 (Turma 2)
Adriano Ulrich do Prado Wiedmann – 202014824 (Turma 1)

1. CRIPTOGRAFIA SIMÉTRICA

A criptografia de chave simétrica é uma das técnicas mais antigas de criptografias utilizadas. Este método baseia-se no uso de uma mesma chave para criptografar e descriptografar uma mensagem ou dado. Para que o procedimento tenha êxito, é necessária a troca prévia de chaves entre os envolvidos na comunicação.

As principais vantagens da criptografia simétrica são: facilidade de implementação, velocidade na criptografia dos dados; uso de menos recursos computacionais; e menor comprimento das chaves. É possível compreender como a principal desvantagem deste método é necessidade de troca de chaves, que se forem comprometidas, todos os dados se tornam vulneráveis, sendo necessário o estabelecimento de uma nova chave. Além disso, este método não permite autenticar a identidade do emissor da mensagem.

No passado, esse método foi utilizado por diversos padrões de criptografia, como a Cifra de Cesar e a Máquina Enigma. Atualmente, é utilizado pelo *Data Encryption Standard* (DES), 3DES e o *Advanced Encryption Standard* (AES).

1.1 *Advanced Encryption Standard* (AES)

O AES surgiu como um método de criptografia de chave simétrica substituta do DES, após a descoberta de inúmeras vulnerabilidades encontradas e publicadas a respeito do processo de criptografia. O AES trabalha com blocos de dados de 128 bits com uso de chaves de 128, 192 ou 256 bits, é implementado de acordo com o seguinte algoritmo:

Chave de Criptografia: Primeiro, é necessário ter uma chave de criptografia adequada. O AES do trabalho utiliza o tamanho de 128 bits de chave.

Divisão em Blocos: Os dados que precisam ser criptografados são divididos em blocos de 128 bits (16 bytes).

Chaves de Rodadas: O AES usa várias "chaves de rodadas" derivadas da chave de criptografia original. O número de chaves de rondadas depende do tamanho da chave (10 rodadas para uma chave de 128 bits).

SubBytes: Nesta etapa, cada byte do bloco é substituído por um byte correspondente na "Tabela de Substituição". Isso é feito para confundir os dados e dificultar o processo de descriptografia.

ShiftRows: Os bytes do bloco são rearranjados de acordo com um padrão específico. Isso ajuda a dispersar os dados e tornar a criptografia mais forte.

MixColumns: Os bytes de cada coluna do bloco são misturados uns com os outros usando operações matemáticas. Isso oferece uma maior difusão dos dados e ajuda a aumentar a segurança da criptografia.

AddRoundKey: Cada bloco é combinado com uma chave de rodada específica usando uma operação de "OU exclusivo" (XOR). Isso adiciona outra camada de complexidade aos dados.

Repetição: Os passos de SubBytes, ShiftRows e MixColumns são repetidos várias vezes, dependendo do número de chaves de rondas necessárias.

Última Rodada: Na última rodada, a etapa MixColumns não é realizada. Apenas as etapas SubBytes, ShiftRows e AddRoundKey são aplicadas.

Cifra Final: Após as rodadas finais, o bloco de dados criptografados é gerado. Esse bloco é o resultado final da criptografia AES.

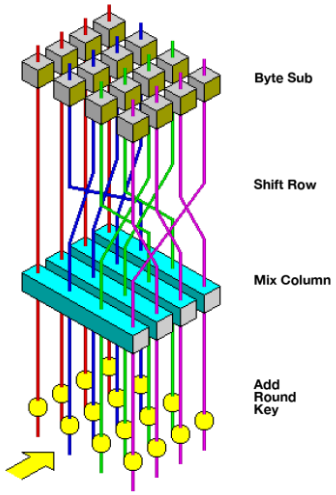

Figura 1 – Processo de criptografia AES

2. CRIPTOGRAFIA ASSIMÉTRICA

A criptografia de chave assimétrica, também conhecida por criptografia de chave pública, é um método criptográfico baseado no uso de chaves distintas, mas que estão correlacionadas. As chaves são denominadas por:

a) Chave pública: a chave divulgada pelo emissor para toda a rede, de conhecimento público; e
b) Chave privada: a chave que é mantida em sigilo pelo emissor, de conhecimento privado.

Apesar de resolverem o problema da troca de chaves em uma comunicação, as chaves assimétricas são de comprimento longo (em geral, 2048 bits), o que requerem maior uso computacional e um maior tempo de processamento. Alguns processos computacionais usam chaves assimétricas para realizar a troca de chaves simétricas que serão utilizadas durante toda a comunicação.

Alguns exemplos de algoritmos que implementam chaves assimétricas são: o *Rivest-Shamir-Adleman* (RSA), *Digital Signature Algorithm* (DAS) e o *Elliptic Curve Cryptography* (ECC). Estes algoritmos também são utilizados nos processos de certificado digital e assinatura digital.

2.1 Rivest-Shamir-Adleman (RSA)

O RSA é um dos primeiros e mais amplamente utilizados algoritmos de criptografia assimétrica, inventado por Ron Rivest, Adi Shamir e Leonard Adleman em 1977, o algoritmo RSA se baseia em um problema matemático conhecido como "fatoração de inteiros", que envolve a decomposição de números grandes em seus fatores primos, fator que leva a segurança do RSA, baseada na dificuldade prática de fatorar números grandes em seus fatores primos. O processo é implementado de acordo com o seguinte algoritmo:

Geração de Chaves: São escolhidos dois números primos grandes de forma aleatória (*random* 1024 bits), p e q, e validados através do teste de Miller-Rabin. Calculamos o produto n = p * q, que será o módulo para as operações de criptografia e descriptografia. Calculamos a função totiente de Euler φ(n) = (p-1) * (q-1). É escolhido um número inteiro e relativamente primo a φ(n) (coprimo), que será a chave pública, geralmente chamada de "e". Calculamos a chave privada, "d", que é o inverso multiplicativo de "e" módulo φ(n).

Criptografia: Converta a mensagem em um valor numérico. Realizamos o *padding* através do algoritmo *Optimal Asymmetric Encryption Padding* (OAEP), que consiste em gerar dois valores aleatórios “r” e “s”, realizar o preenchimendo dos dados com um valor b“ ”, a aplicação de uma função *Mask Generation Function* (MGF) e de *hash* (SHA3-256), por fim é realizado a combinação dos valores e feito a criptografia utilizando a chave pública "e" para elevar o valor da mensagem à potência "e" módulo n. Esse resultado é a mensagem criptografada.

Descriptografia: Usamos a chave privada "d" para elevar a mensagem criptografada à potência "d" módulo n. Isso resultará no valor original da mensagem criptografada, levando em consideração que o algoritmo deve desfazer o processo de *padding* realizado no OAEP (*decode*).

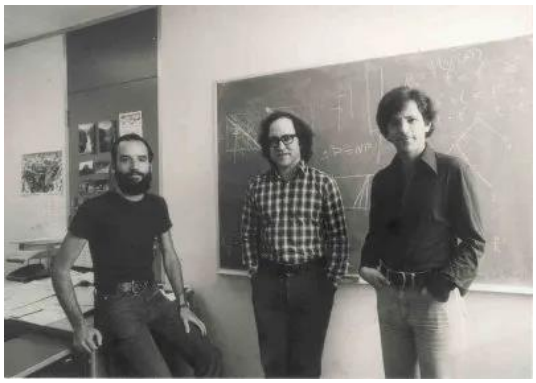

Figura 2 – Rivest, Shamir e Adleman, criadores do processo de criptografia RSA.

3. ASSINATURA DIGITAL

Assinatura Digital é um procedimento que utiliza o processo de criptografia por chave assimétrica que permite a verificação da autenticidade de uma informação, ou seja, confirmar o autor (assinante) do documento. Além disto, a assinatura digital garante a integridade do documento, já que é realizada a criptografia do *hash* do documento.

O destinatário pode realizar a descriptografia da assinatura e obter o *hash* do documento. Como o *hash* foi criptografado com a chave privada do assinante, algo que somente ele possui, é possível atestar a origem ao realizar a descriptografia com o uso da chave pública.

O processo de assinatura digital é amplamente utilizado no mercado financeiro, contratos eletrônicos, e-mails e certificados digitais. Atualmente os Governos de diversos países passaram a aceitar a assinatura digital como uma assinatura válida juridicamente e administrativamente.

3.1 Verificação e Assinatura RSA

A assinatura digital RSA fornece uma maneira confiável de verificar a autenticidade do remetente e garantir que a mensagem não tenha sido modificada durante a transmissão. Ao usar a chave privada para assinar a mensagem, o remetente fornece uma prova criptográfica de que é o autor legítimo. A verificação da assinatura usando a chave pública do remetente garante que apenas o remetente possa ter gerado essa assinatura específica.

A assinatura digital RSA é amplamente aplicada em áreas como assinaturas eletrônicas, autenticação de identidade, integridade de dados e certificação digital, fornecendo confiança e segurança em comunicações eletrônicas.

Neste trabalho, o processo de assinatura consiste em gerar o *Hash* da mensagem criptografada com a chave AES, em seguida assinamos com a chave privada RSA do emissor, por fim enviamos a mensagem criptografada M com AES, a assinatura e a chave pública RSA do emissor (A). A verificação consiste no processo inverso e a comparação com o Hash da mensagem criptografada com AES.

Sign = (AES_k(M) , RSA_KA_s(H(AES_k(M))), KA_p); e
RSA_KA_s (RSA_KA_s(H(AES_k(M)))) = H(AES_k(M)) ?