Trabalho 03

Pedro Trajano - 190055251

Dezembro 2023

1 Introdução

O algoritmo RSA, é um dos algoritmos de criptografia assimétrica mais amplamente utilizados e conhecidos. Introduzido em 1977, o RSA desempenhou um papel fundamental na segurança da comunicação digital e ainda é amplamente empregado em aplicações como criptografia de dados, autenticação e assinatura digital. Neste será trabalho foi implementado o algoritmo RSA. Desde a geração das chaves p e q, a cifração e decifração assimétrica RSA usando OAEP, até o cálculo de hashes da mensagem SHA-3, para assinar a mensagem, fazendo também a verificação e validação da assinatura.

2 Geração de chave

Para a geração das chaves são gerados dois números primos p e q, sendo eles primos de tamanho 1024 bits, para conseguir primos grandes dessa tamanho, em primeiro local é gerado um número aleatório com o bit mais significativo sendo '1'. Em seguida fazia uma checagem se o número análisado era dividido por um primo relativamente pequeno menor que 1000, foi testado para primos de diversos tamanhos, chegando a chegar para primos de até 100000, mas o ganho não era suficiente para baleancear a quantidade de checagem que fazia. Se o número fosse divisivel por um primo pequeno, outro número era escolhido, mas se ele não fosse divisivel esse número então seguia para um teste de Miller Rabin, que é um teste estatistico para dizer se o número é possívelmente primo, esse método é iterativo e foi escolhido o número de iterações igual a 20, pois dessa forma a precisão do número primo era grande o suficiente para uma criptografia RSA. Obviamente utilizar um teste iterativo que não traz um resultado exato pode causar problemas, mas com um número de iterações grande o suficiente é possivel minimizar a chance de acontecer problemas de com tanta intensidade que ele possa ser ignorado. Fazia-se esse processo duas vezes para p e q, mas caso esses dois valores, por algum milagre estatistico, fosesm iguais, um novo valor de q seria gerado. Para gerar as chaves em si foi utilizado os parâmetros gerados em cima de p e q como n que é seu produto e ϕ_n que é o produto entre os números anteriores a p e q, esse número ϕ_n é utilizado para calcular e que é um número de 1024 bits coprimo a phi_n. Com esses parâmetros é calculado d que

é o inverso multiplicativo modular de e em relação a ϕ_n. Com isso conseguimos gerar nossa chave pública e privada.

3 Cifra

O processo de cifração RSA é fundamentalmente baseado em operações matemáticas envolvendo números inteiros grandes. O algoritmo utiliza um par de chaves, composto por uma chave pública e uma chave privada. A chave pública consiste em dois elementos: n e e. A chave privada inclui o mesmo módulo n e um d. A segurança do RSA reside na complexidade de fatorar o produto de dois números primos grandes para determinar as chaves privadas a partir das chaves públicas. No contexto da cifração de uma mensagem M usando a chave pública, a operação básica é aplicar a função de exponenciação modular. A mensagem cifrada C é obtida como $C \equiv M^e mod n$. Esse resultado cifrado pode então ser enviado com segurança pelo canal de comunicação, pois a dedução da mensagem original sem a chave privada é computacionalmente inviável. Neste trabalho foi implementado uma cifração por caractere, que simboliza à aplicação da operação de cifração a cada caractere individual da mensagem. Embora essa abordagem simplificada seja intuitiva, ela pode ter algumas implicações de segurança. A principal preocupação é que padrões ou características da linguagem natural original podem persistir, tornando a mensagem cifrada potencialmente mais suscetível a quebras, como ataques de frequência. Para trabalhos futuros é sugerido mitigar essa vunerabilidade. O processo de decifração RSA é realizado por meio da aplicação da operação de exponenciação modular. Seja C a mensagem cifrada, a mensagem original M pode ser recuperada através da seguinte equação: $M \equiv C^d mod n$. Aqui, d e n são parte da chave privada.

4 Assinatura

O algoritmo utilizado para realizar a assinatura e a validação foi uma função Hash de mensagem em claro SHA-3. O objetivo principal de uma assinatura é garantir a autenticidade de quem está enviando a mensagem. O SHA-3 (Secure Hash Algorithm 3) é uma função de hash criptográfica que produz um valor de hash fixo, independentemente do tamanho ou conteúdo da entrada. Em primeiro passo gera uma hash SHA-3 em cima da mensagem origal M, é criado uma assinatura digital utilizando a chave privada do remetente. Dessa forma gera a assinatura, já o receptor recebe a mensagem e a assinatura e então ele verifica a assinatura digital utilizando a chave pública, se a assinatura for válida indica que a mensagem está correta. Esse método garante garantias significativas de autenticidade e integridade da mensagem. É primordial que haja assinaturas no processo criptográfico para zelar pela segurança.