IMPLEMENTAÇÃO DE CRIPTOGRAFIA ASSIMÉTRICA E SIMÉTRICA

PIETRO FERRAZZO DANIEL

VICTORIA FERNANDES GALVÃO

TATIANA SAKUMA

06 de setembro de 2024, Florianópolis (SC)

1. Qual algoritmo é mais rápido? Teste o desempenho ao criptografar/descriptografar grandes mensagens.

O algoritmo simétrico é consideravelmente mais rápido do que o assimétrico quando se trata de criptografar e descriptografar grandes volumes de dados. Isso ocorre porque o AES utiliza uma única chave para as operações de criptografia e descriptografia, o que o torna menos complexo computacionalmente. Em contrapartida, o RSA requer o uso de pares de chaves (pública e privada), e sua operação envolve cálculos matemáticos mais pesados, o que aumenta o tempo de processamento.

Portanto, o AES é muito mais eficiente para grandes quantidades de dados, enquanto o RSA é mais utilizado para criptografar pequenas quantidades de dados ou chaves.

2. Em que situação você utilizaria criptografia assimétrica?

A criptografia assimétrica é ideal em situações que envolvem troca de chaves ou comunicação segura entre duas partes que não compartilham uma chave previamente. Um exemplo comum é o envio seguro de dados através da internet, como em transações de e-commerce ou trocas de e-mails, onde o remetente usa a chave pública do destinatário para criptografar a mensagem, e o destinatário a descriptografa com sua chave privada.

Outro uso significativo é na autenticação e assinatura digital, onde a criptografia assimétrica assegura a identidade de uma pessoa ou sistema e garante que os dados não foram alterados.

3. Quando a criptografia simétrica é mais adequada?

A criptografia simétrica é mais adequada quando existe uma necessidade de criptografar grandes volumes de dados de forma rápida e quando há uma maneira segura de compartilhar a chave secreta entre as partes envolvidas. Um exemplo típico é a criptografia de discos rígidos ou de dados armazenados em um servidor, onde o mesmo sistema ou entidade possui tanto a chave de criptografia quanto a chave de descriptografia.

Também é amplamente utilizada em comunicações de redes seguras internas, como VPNs, onde o desempenho é crucial e o compartilhamento da chave pode ser gerenciado com segurança.

4. Explique como os dois algoritmos podem ser combinados (modelo híbrido) para maximizar a segurança e o desempenho:

Um modelo híbrido combina a criptografia assimétrica e simétrica para garantir tanto segurança quanto eficiência. O cenário mais comum é o seguinte:

- O algoritmo RSA é utilizado para criptografar uma pequena chave simétrica (chave AES), garantindo que apenas o destinatário, com sua chave privada, consiga acessá-la.

- Em seguida, o AES é utilizado para criptografar os dados reais (geralmente grandes), garantindo uma criptografia rápida e eficiente.

Esse modelo é amplamente utilizado em protocolos como o SSL/TLS, que protege as comunicações na web. A criptografia assimétrica RSA assegura a troca segura da chave de sessão, e o AES é usado para criptografar os dados da sessão em si, maximizando o desempenho sem comprometer a segurança.