UNIVERSIDADE FEDERAL DE SERGIPE

Iuri Rodrigo Ferreira Alves da silva
Gregory Medeiros Melgaço Pereira
Raul Rodrigo Silva de Andrade
Rafael Castro Nunes
Ruan Robert Bispo dos Santos
Vítor do Bomfim Almeida Carvalho

Encriptação AES

São Cristóvão,SE
19 de abril de 2017

Iuri Rodrigo Ferreira Alves da silva
Gregory Medeiros Melgaço Pereira
Raul Rodrigo Silva de Andrade
Rafael Castro Nunes
Ruan Robert Bispo dos Santos
Vítor do Bomfim Almeida Carvalho

Encriptação AES

Relatório em conformidade com as normas ABNT

Universidade Federal De Sergipe
Faculdade de Engenharia Eletrônica
Redes e Comunicações

São Cristóvão,SE
19 de abril de 2017

Resumo

Palavras-chaves: Grafos, Problema dos Menores Caminhos, Floyd-Warshall, Dijkstra, Iterações

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

No contexto capitalista e competitivo atual é cada vez mais prescindível que os dados enviados e recebidos, principalmente online, sejam protegidos, em que apenas quem envia e quem recebe tenha acesso ao seu conteúdo, garantindo assim o direito de privacidade. Essa ideia de segurança de dados se aplica diretamente à diversas áreas como : troca de mensagens entre usuários de aplicativos, compras e processos financeiros online e troca de informações entre países ou entre organizações de um único país, já que muitos conteúdos são confidenciais e apenas autoridades do governo podem ter acesso. Os fundamentos de segurança (REFERENCIAR) são definidos por disponibilidade, integridade, controle de acesso, autenticidade, não-repudiação e privacidade. Foi pensando-se nisso que a criptografia foi criada. A palavra criptografia que provém dos radicais gregos kriptos (oculto) e grafo (escrita), é o nome dado à ciência de codificar mensagens utilizando algoritmos que serão usados novamente para decodificar essa mensagem. A criptografia apresenta dois tipos básicos: Simétrica (chave fechada) e Assimétrica (chave aberta).

A criptografia assimétrica foi criada na década de 1970. Nesse modelo, cada dispositivo envolvido na comunicação possui dois tipos de chaves diferentes, uma particular e uma pública. Essas chaves são processos digitais complexos que podem eventualmente estar associados a senhas. A chave pública é conhecida por qualquer usuário e é utilizada quando se quer se comunicar com outro usuário de modo seguro. Já a chave particular apenas cada dispositivo conhece e tem a sua. É com essa chave particular que o destinatário pode descriptografar a mensagem que foi criptografada com sua respectiva chave pública. A mensagem pode ser entendido com um bem precioso, a chave pública o cadeado que protege esse bem e a chave particular é chave física capaz de abrir esse cadeado. A vantagem desse método é a segurança, já que não é necessário o compartilhamento das chaves particulares e elas se encontram em poder do destinatário e da fonte, não há risco de intercepção por terceiros para saber essa chave particular, eles apenas podem conhecer a chave pública do destinatário. É importante ressaltar que para um dispositivo enviar uma mensagem a outro, ele já tem que conhecer a chave pública do destino. A desvantagem é que com esse método o tempo de processamento de mensagens fica muito maior que a criptografia simétrica. Vários algoritmos para a criptografia assimétrica já existem, como o RSA e o Elgamal. O algoritmo RSA é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número

A criptografia simétrica é o modelo mais antigo de criptografia. Nesse modelo,

a chave que dá acesso ao conteúdo da mensagem trocada entre dois dispositivos deve permanecer em segredo. Geralmente essa chave é representada por uma senha que é usada pelo remetente para codificar a mensagem e usada pelo destinatário para decodificar a mensagem. A vantagem desse modelo é a sua simplicidade. Caso a chave seja complexa o algoritmo não necessariamente precisa também ser muito complexo, o que é bom, já que quanto mais simples o algoritmo, maior é a sua velocidade de processamento e facilidade de implementação. A principal desvantagem deste modelo é que como é utilizada apenas uma chave para ciframento e desciframento, conhecendo a chave se tem acesso aos dois processos, o que pode ocorrer interceptando o canal utilizado. Com isso, é muito importante a comunicação por um canal seguro evitando assim a ação de intrusos que podem ter acesso a mensagem. Outros problemas desse método é que como cada par necessita de uma chave, em uma rede com 'n' usuários, serão necessárias n^2 chaves, o que dificulta o gerenciamento. Além disso, não é fácil armazenar essas chaves de forma segura. Com isso, esse método não garante os princípios de autenticidade e não-repudiação. Vários algoritmos para a criptografia simétrica já existem, como o AES e o DES. O algoritmo AES é o mais utilizado e é o adotado como padrão pelo governo dos EUA. Esse algoritmo possui um bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, é relativamente fácil de executar e requer pouca memória. Esse algoritmo será o utilizado neste projeto.

2 Referência

3 Objetivos

4 Formulação do problema

5 Resultados Obtidos

6 Conclusão

Referências

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital [Revista online]*, v. 31, p. 11–15, 2012. Nenhuma citação no texto.

SILVA, M. d. L. G. da; OLIVEIRA, C. C. Criptografia assimétrica em documentos de áudio: uma experiência inicial com o algoritmo rsa. Nenhuma citação no texto.