Criptografia Assimétrica em Documentos de Áudio: uma experiência inicial com o algoritmo RSA

Mariana de Lourdes Godoy da Silva, Cintia Carvalho Oliveira

Instituto Federal do Triângulo Mineiro – Campus Patrocínio.

mariannag_@hotmail.com; cintiacarvalho@iftm.edu.br.

Abstract. *Today, with the advancement of technology security it has become necessary in all aspects and with the exchanging information, it became apparent the need for automated tools to protect files and other information stored on databases. In this research, the RSA asymmetric encryption is adopted that works with two keys, a public and a private, and it generates bades on the multiplication of two numbers primes. The breakdown, however, is complex because it is large enough to factorize this and process which can take years. So today it is widely used for ensuring efficiency and safety as well as besides never have been violated by any algorithm. In the course of developing this study we aimed to develop software using the above techniques to protect personal files.*

Resumo. *Hoje, com o avanço de tecnologias é necessário segurança em todos os aspectos e com a troca constante de informações tornou-se evidente a necessidade de ferramenta para proteger arquivos armazenados em bancos de dados. Nesta pesquisa é adotado o algoritmo RSA de criptografia assimétrica que funciona com um par de chaves, pública e privada, geradas com base na multiplicação de dois números primos. Sua "quebra" é complexa, pois se ele for grande o suficiente a fatoração de tal pode demorar anos. Por isso, hoje é amplamente usado por garantir eficiência e segurança, além de nunca ter sido violada por qualquer algoritmo. Ao decorrer deste trabalho objetivamos o desenvolvimento de um software capaz de criptografar documentos de áudio digital utilizando as técnicas supracitadas para proteger arquivos pessoais.*

1. Introdução

Atualmente, com o crescimento dos meios de comunicação enfatizando o uso da Web, o mundo avança no desenvolvimento e sofisticação de tecnologias que nos permitem mais praticidade no decorrer do dia, como por exemplo, efetuar uma compra através do seu cartão de crédito, aplicativos que controlem sua movimentação bancária, envio de documentos privados e entre outros. Devido a isso faz-se necessário o aprimoramento de ferramentas que tornem seguras tais atividades evitando a decodificação de informações pessoais por pessoas mal-intencionadas. (STALLINGS)

Portanto, a criptografa é usada como um método para assegurar sigilo de qualquer tipo de informação virtual, tornando-as códigos a serem decriptadas apenas pelo receptor da mensagem. O conceito de criptografia de chave pública evoluiu de uma tentativa de atacar dois dos problemas mais difíceis associados à criptografia simétrica. O primeiro problema é o da distribuição de chaves que requer (1) que dois comunicantes já compartilhem uma chave de alguma forma distribuída a eles; ou (2) o uso de um centro de distribuição de chaves. Whitfield Diffie, um dos inventores da criptografia

de chave pública, descobriu que esse segundo requisito anulava a própria essência da criptografia: a capacidade de manter sigilo total sobre sua própria comunicação. Conforme foi dito por Diffie, não há vantagem de desenvolver criptossistemas impenetráveis, se seus usuários forem obrigados a compartilhar suas chaves com um CDC (Centro de Distribuição de Chaves) que pode estar sujeito a roubo ou suborno. (STALLINGS)

2. Fundamentos

Os métodos de criptografia podem ser classificados de acordo com o uso das chaves em duas categorias principais: os criptossistemas simétricos que utilizam apenas uma chave, cuja função é tanto cifrar quanto decifrar; e assimétricos que utilizam duas delas, uma com a função de cifrar, chamada pública, e outra com a função de decifrar, privada. (CAVALCANTE)

A Criptografia RSA trabalha com algoritmos computacionais utilizando um par de chaves que permite a qualquer usuário codificar mensagens usando sua chave pública, entretanto só o destinatário legítimo poderá decodificá-la usando sua chave privada. A segurança desse sistema criptográfico está baseada em um antigo problema matemático: obter os fatores primos de um número dado. (CAVALCANTE)

O RSA explora essa situação ao utilizar um número, que atualmente varia de 512 a 1024 bits, e que é o produto de dois números primos muito grandes sendo impossível a quebra da chave de decodificação pela não existência de algoritmos eficientes para a fatoração de números inteiros em fatores primos. Dessa forma esse trabalho aborda as técnicas supracitadas, aplicadas à manipulação de áudio. (STALLINGS)

3. Desenvolvimento

Este capítulo tem o objetivo de descrever as etapas do desenvolvimento do trabalho, as quais foram elaboradas com base em pesquisas bibliográficas. Um áudio digital é um arquivo binário como qualquer outro, e devido ao processo de evolução tecnológica dos processos de conversão de som analógico para digital, não há mais distinção perceptível ao ouvido humano entre o som analógico e sua representação digital. Contudo, a precisão de um áudio varia de acordo com a taxa de amostragem, frequência e a quantidade de bits para cada amostra. De acordo com o Teorema de Nyquist, uma taxa de amostragem de duas vezes o valor da frequência máxima alcançada pelo sinal analógico é suficiente para uma representação digital sem grandes perdas. (IAZZETTA)

Dessa forma ao termos um áudio como objeto em entrada e o armazenarmos num vetor obtêm-se a quantidade de bits por amostra explicita, onde poderá ser facilmente criptografada. Por conseguinte utilizamos a linguagem de programação JAVA e o NetBeans 8.0.2 como interface de desenvolvimento para implementarmos um código de manipulação de áudio usando a biblioteca AudioFileInputStream e assim reproduzi-lo.

Ao longo do desenvolvimento foram estudados alguns códigos de criptografia RSA provenientes de pesquisas com o objetivo de encontrar a melhor biblioteca de manipulação de arquivos assim como métodos para gerar chaves públicas e privadas. Entretanto, ao usar um método que gere chaves automaticamente, restringimos que o resultado de uma criptografia seja observado em relação a sua velocidade e eficiência versus o tamanho de suas chaves. Dessa forma decidimos optar por gerar os pares de chaves manualmente de forma que tivéssemos o controle de mudar variáveis e comparar

diferentes tamanhos de chaves entre outros algoritmos de criptografia assimétrica para comprovar a eficiência do RSA.

4. Conclusões

Através de árdua pesquisa fizemos uma coleta de dados bibliográficos em trabalhos apresentados em congressos, teses e artigos especializados, em busca de modelos e casos de sucesso no desenvolvimento de algoritmos para criptografia de documentos de áudio. Também estudamos as bibliotecas de processamento e manipulação de áudio e criptografia RSA da linguagem de programação Java, bem como Programação Orientada a Objetos de forma a atribuir tais métodos em nossa pesquisa. Testamos algoritmos de alguns trabalhos finalizados com o intuito de agregarmos os melhores métodos no software, e assim por meio de análises concluímos que o método RSA de criptografia é o mais seguro devido a forma de como é criada seu par de chaves. Medimos também a eficiência do algoritmo em relação ao tempo de resposta para cifrar e decifrar uma mensagem.

Percebemos que a busca pela segurança através do aumento do tamanho das chaves provoca um aumento exponencial no tempo das cifragens e decifragens, o que pode trazer resultados negativos. Em um servidor de Internet por exemplo, onde circula um volume enorme de informações, exigirão alto poder de processamento para utilizar a criptografia RSA de forma rápida. Dessa forma, a escolha do tamanho da chave deverá levar em conta o grau de importância e o tamanho da informação que se queira proteger. Por isso atualmente as cifragens e decifragens são realizadas geralmente pelos algoritmos simétricos, que são mais rápidos, e o transporte das chaves é feito através só sistema assimétrico.

Contudo, o que destruiria o RSA seria a criação de um algoritmo de fatoração eficiente de encontrar d sem utilizar n. Neste caso para Barbosa *et al* (2003), a saída seria utilizar criptografia baseada em curvas elípticas, pois utilizam grupos e polinômios mais complexos. Nesta edição, Silva (2006) afirma que existe uma pesquisa sobre a construção de um computador quântico, capaz de fatorar números e encontrar primos com mais velocidade, o que daria início a Criptografia Quântica.

Referências

BARBOSA, Luis Alberto de Moraes et al. RSA: Criptografia Assimétrica e Assinatura Digital. 2003. 50 p. (Especialização em Redes de Computadores) - Universidade Estadual de Campinas, Campinas, 2003.

SILVA, Elen Viviani Pereira da. Introdução à Criptografia RSA. 2006. 32 p. - Faculdade de Engenharia de Ilha Solteira, Universidade Estadual Paulista „Julio de Mesquita Filho“, Ilha Solteira, 2006.

CAVALCANTE, André LB. “Teoria dos números e criptografia”. Revista Virtual (2005)

DE OLIVEIRA, Ana Karina Dourado Salina; PRETI, João Paulo Delgado. Métodos Criptográficos EM Java. Profiscientia, n. 3, 2013.

STALLINGS, William.Criptografia e segurança de redes: princípios e práticas. Pearson Prentice Hall, 2008.Protocolo Diffie-Hellman Sobre Curvas Elípticas.

IIAZZETTA, Fernando. Disponível em:< http://www2.eca.usp.br/prof/iazzetta/tutor/audio/a_digital/a_digital.html> . Acesso em 9 de Março de 2016.

TRINTA, Fernando. Um Estudo sobre a Criptografia e Assinatura Digital. Setembro, 1998. Disponível em:<http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 22 set. 2015.

OLIVEIRA, Ronielton. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. Disponível em:< http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. Acesso em: 22 set. 2015.