# O USO DA CRIPTOGRAFIA EM ÁUDIO

**SILVA, Mariana de Lourdes Godoy da[1]; OLIVEIRA, Cintia Carvalho[2];**

**RESUMO:** Atualmente, a criptografia é o que norteia toda a segurança da informação nos canais web de comunicação. Sendo assim, esse estudo aborda a relação existente entre a busca pela segurança de dados e a velocidade de codificação e decodificação do algoritmo RSA aplicado a mensagens de áudio, considerando o tamanho das chaves como requisito de segurança devido à dificuldade computacional de fatorar números inteiros extensos, levando a conclusão de que o aumento do tamanho das chaves leva a um crescimento exponencial do tempo de cifragem e decifragem. Abordou-se também a matemática utilizada no algoritmo que possui a Teoria dos Números como base de sua implementação, e discutiu-se sobre a experiência na aplicação do RSA a documentos de áudio avaliando as suas possibilidades de quebra por ataques matemáticos e por força bruta.

**Palavras-chave:** Segurança; Autenticidade; Chaves simétricas; Chaves assimétricas; RSA.

## INTRODUÇÃO

A necessidade de guardar segredos pelo homem trouxe o avanço de métodos eficazes de segurança de acordo com o conhecimento que estava ao seu alcance. Júlio César, imperador romano no século V a.C. criou a primeira técnica que chamamos de criptografia, conhecida hoje como Cifra de César e que consiste na simples substituição das letras do alfabeto. Por exemplo, com uma troca de quatro posições, a letra A seria substituído por E, B se tornaria F e assim por diante.

Com o passar dos séculos e o aprimoramento de novas técnicas, a segurança, tornou-se um aspecto bastante amplo e pesquisado, e assim novas invenções surgiram de acordo com a necessidade do momento. Na atualidade, com o crescimento constante da comunicação através de meios audiovisuais, e enfatizando o uso da Web como canal de transmissão, o mundo avança na evolução e sofisticação de tecnologias que nos permitem mais praticidade no decorrer do dia, tornando indispensável o aprimoramento de ferramentas que tornem seguras tais atividades evitando a decodificação de

[1] Aluna, Instituto Federal do Triângulo Mineiro – Campus Patrocínio, Patrocínio-MG; E-mail: mariannag_@hotmail.com; PIBIC-EM, CNPq.
[2] Orientadora, Instituto Federal do Triângulo Mineiro – Campus Patrocínio, Patrocínio-MG; E-mail: cintiaoliveira@iftm.edu.br

informações por pessoas mal-intencionadas. Portanto, esse trabalho se relaciona com a importância de certificar sigilo, autenticidade, integridade e confidencialidade em mensagens de áudio circuladas pela internet.

## MATERIAIS E MÉTODOS

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, chamada privada (CAVALCANTE, 2005).

O conceito de cifra de chave pública evoluiu de uma tentativa de atacar dois dos problemas mais difíceis associados à criptografia simétrica. O primeiro 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 cifra de chave pública, descobriu que esse segundo requisito anulava a 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 partilhar suas chaves com um CDC (Centro de Distribuição de Chaves) que pode estar sujeito a roubo ou suborno (DIFFIE, HELLMAN, 1979).

### *Descrição do algoritmo RSA*

O algoritmo RSA foi criado em 1978 por Rom Rivest, Adi Shamir e Leonard Adleman no Massachussets Institute of Techonology (MIT) e batizado com as iniciais de seus sobrenomes. Atualmente é o método de criptografia assimétrica mais utilizado no mundo principalmente em protocolos de serviços como o SSH e SSL, que gerenciam um canal de comunicação seguro entre o cliente e o servidor, os quais dependem a internet (STALLINGS, 2008).

O RSA foi construído sobre uma das áreas mais clássicas da matemática, a Teoria dos Números. Ele se baseia na dificuldade de fatorar um número em seus componentes primos.

Como o algoritmo criptografa apenas números o primeiro passo ao implementa-lo é definir valores para os caracteres e logo em seguida definir os números primos (*p* e *q*) e calcular seu produto (n = p x q). Quanto maior o tamanho dos primos escolhidos, melhor é a sua segurança. A RSA Data Security responsável pela padronização do protocolo, recomenda que se utilize chaves de 2048 bits, equivalente a 617 dígitos. O próximo passo é calcular a função totiente, ou φ(n) = (p-1)*(q-1), que determina a quantidade de co-primos de um número que são menores que ele mesmo.

Para o cálculo da chave pública, devemos escolher um número *e* em que $1 < e < \varphi(n)$, de forma que *e* seja co-primo de φ(n). Com a chave pública em mãos basta aplicar a seguinte equação a cada letra da mensagem:

$$c = m \wedge e \bmod n$$

Em que *e* é a chave pública e *m* é o valor numérico da letra (STALLINGS, 2008).

Durante o desenvolvimento dessa pesquisa implementamos o algoritmo RSA para criptografar um áudio que é gravado a partir do microfone do computador no qual o programa está sendo interpretado. A cada execução do programa foi gerado um par de chaves pública e privada de 2048 bytes usado para criptografar e decriptografar respectivamente.

## RESULTADOS E DISCUSSÃO

Sabe-se que digitalmente o som não é representado por uma onda, mas sim por uma sequência de valores na linguagem do computador (código binário), para cada período de tempo. O processo de conversão do som analógico acarreta numa perda e devido a isso sua representação digital nunca será exata. Todavia, a evolução tecnológica dos processos de conversão atingiu um grau elevado de precisão ao ponto de ser imperceptível ao ouvido humano. 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 (FERNANDES; PANAZIO, 2009).

## CONSIDERAÇÕES FINAIS

Por meio da pesquisa, concluímos que a ampliação do tamanho das chaves públicas e privadas provocam um aumento exponencial no tempo das cifragens e decifragens, o que ocasiona resultados negativos. Em um servidor de internet, por exemplo, onde circula um volume enorme de informações, exige-se alto poder de processamento para utilizar a criptografia RSA de forma rápida. Portanto, a escolha do tamanho das chaves deve 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 por meio do sistema assimétrico.

Para ter-se ideia do poder computacional necessário para violar o segredo de uma informação cifrada com a técnica de criptografia assimétrica por meio da fatoração, suponha-se uma unidade de medida chamada MIPS-ano, sendo que um MIPS-ano equivale a um computador executando um milhão de instruções por segundo durante um ano inteiro, sem intervalos e com todos os processos desnecessários do Windows desativados. Assim se tivermos uma chave assimétrica de 1024 bits necessitaria de 30.000 MIPS-ano para ser quebrada.

Contudo, o que destruiria o RSA seria a criação de um algoritmo de fatoração eficiente de encontrar *e* sem utilizar a fatoração de *n*. Desta forma, para Barbosa et al., (2003), a saída seria utilizar criptografia baseada em curvas elípticas, pois utilizam grupos e polinômios mais complexos. Realidade não muito distante e que foi abordada na *RSA Conference 2017*, ampliando não só a quebra do RSA como propondo uma criptografia baseada nas curvas elípticas (RSA CONFERENCE, 2017).

## REFERÊNCIAS

CAVALCANTE, A. L.B. “Teoria dos números e criptografia”. **Revista Virtual,** 2005.

DIFFIE, Whitfield; HELLMAN, Martin E. Privacy and authentication: An introduction to cryptography. **Proceedings of the IEEE**, v. 67, n. 3, p. 397-427, 1979.

FERNANDES, T. G.; PANAZIO, A. N. Do analógico ao digital: amostragem, quantização e codificação. **II Simpósio de Iniciação Científica da Universidade Federal do ABC - SIC-UFABC 2009.** Disponível em: < http://ic.ufabc.edu.br/II_SIC_UFABC/resumos/paper_5_74.pdf. 2009.

**RSA CONFERENCE**; Disponível em: < https://www.rsaconference.com/>. Acesso em: 15 de Março de 2017.

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