REVISTA ELETRÔNICA CIENTÍFICA DA UERGS

Impacto do emprego de aplicações de segurança em aplicativos de comunicação: um estudo experimental sobre o tempo de processamento

Vinicius Gadis Ribeiro
Universidade Federal do Rio Grande do Sul (UFRGS).
E-mail: vinicius.gadis@ufrgs.br, http://lattes.cnpq.br/2937182050702659

Guilherme Martinez Floriano
Centro Universitário Ritter dos Reis (UniRitter).
E-mail: guilhermefloriano@gmail.com, http://lattes.cnpq.br/01953147816498 82

Sidnei Renato Silveira
Universidade Federal de Santa Maria (UFSM).
E-mail: sidneirenato.silveira@gmail.com, http:/ lattes.cnpq.br/0107727024654188

Jorge Rodolfo Silva Zabadal
Universidade Federal do Rio Grande do Sul (UFRGS).
E-mail: jorge.zabadal@ufrgs.br, http://lattes.cnpq.br/0586975941517922

ISSN 2448-0479. Submetido em: 07 ago. 2022. Aceito: 15 set. 2022.
DOI: http://dx.doi.org/10.21674/2448-0479.83.171-177

Resumo

Este trabalho visa mensurar o estudo do impacto do emprego de tecnologias de segurança da informação que buscam prover serviços de privacidade e autenticidade em comunicação segura. Para tanto, foi implementado um protótipo que emprega dois mecanismos de segurança em conjunto - a criptografia e a esteganografia -, fornecendo as funcionalidades necessárias para troca de mensagens confidenciais. Para isso, utiliza-se um esquema de chave pública para cifrar e decifrar a mensagem, um esquema de assinatura digital e verificação dessa mensagem e a técnica de esteganografia LSB para ocultar a assinatura digital em uma imagem – possibilitando posterior verificação de integridade de assinatura. Com a utilização das técnicas de forma adequada pretende-se garantir que os dados não serão corrompidos, dificultando ainda mais o trabalho do atacante - que terá de trabalhar sobre informações resultantes de duas diferentes tecnologias de segurança. Foram levantados dados para a análise do impacto do emprego dessas tecnologias no domínio tempo de processamento.

Palavras-chave: Segurança de sistemas; criptografia de chave pública; assinatura digital; esteganografia.

Abstract

Impact of employing security applications on communication applications: an experimental study on processing time

This work aims to measure the study of the impact of the use of information security technologies that seek to provide privacy and authenticity services in secure communication. To this end, a prototype was implemented that employs two security mechanisms together - cryptography and steganography -, providing the necessary functionalities for exchanging confidential messages. For this, a public key scheme is used to encrypt and decrypt the message, a digital signature scheme and verification of this message, and the LSB steganography technique to hide the digital signature in an image – allowing subsequent verification of signature integrity. By using the techniques properly, it is intended to guarantee that the data will not be corrupted, making the attacker's work even more difficult - who will have to work on information resulting from two different security technologies. Data were collected to analyse the impact of using these technologies in the

processing time domain.

Keywords: Systems security; public key encryption; digital signature; steganography.

Resumen

Impacto del empleo de aplicaciones de seguridad en las aplicaciones de comunicación: un estudio experimental sobre el tiempo de procesamiento

Este trabajo tiene como objetivo medir el estudio del impacto del uso de tecnologías de seguridad de la información que buscan brindar servicios de privacidad y autenticidad en la comunicación segura. Para ello, se implementó un prototipo que emplea dos mecanismos de seguridad en conjunto -criptografía y esteganografía -, brindando las funcionalidades necesarias para el intercambio de mensajes confidenciales. Para ello se utiliza un esquema de clave pública para encriptar y desencriptar el mensaje, un esquema de firma digital y verificación de este mensaje, y la técnica de esteganografía LSB para ocultar la firma digital en una imagen permitiendo la posterior verificación de la integridad de la firma. Usando las técnicas correctamente, se pretende garantizar que los datos no se corrompan, dificultando aún más el trabajo del atacante, que tendrá que trabajar con información resultante de dos tecnologías de seguridad diferentes. Se recopilaron datos para analizar el impacto del uso de estas tecnologías en el dominio del tiempo de procesamiento.

Palavras clave: Seguridad de los sistemas; cifrado de clave pública; firma digital; esteganografía.

Introdução

Com a crescente utilização de meios digitais para troca de informações sensíveis, em que os envolvidos desejam manter sigilo, tornou-se extremamente necessária a criação de novos e eficientes meios de realizar essa comunicação de forma segura. Nesse sentido, busca-se prover os serviços de privacidade e autenticidade do conteúdo das mensagens, a confiabilidade na comunicação, a garantia dos envolvidos na mesma e a integridade da mensagem.

O presente trabalho tem como objetivo o estudo do impacto do emprego de técnicas de criptografia, assinatura digital e esteganografia. Para tanto, foi realizada a implementação de um protótipo que proporcionou, assim, um meio privado para troca de informações que necessitam de segurança. Basicamente, o protótipo desenvolvido emprega algoritmos de criptografia de chave pública - para cifrar e decifrar as informações -, algoritmo de *hash* - para gerar uma assinatura digital dessas informações - e um algoritmo de esteganografia - para ocultar essa assinatura digital em uma imagem digital. Pode-se, assim, dificultar o trabalho do atacante, que terá de trabalhar sobre duas informações - a mensagem cifrada e a imagem com a assinatura digital -, que foram empregadas a diferentes técnicas de segurança. As métricas que foram empregadas foram o tempo de processamento em razão do tamanho do arquivo de dados.

Atualmente, as redes de computadores vêm crescendo de forma considerável; empresas estão se integrando cada vez mais nesta área para conduzir seus negócios de forma mais ágil e lucrativa. Com base nisso, surge a necessidade de melhores mecanismos para garantir a segurança das transações de informações confidenciais - sendo muitas destas informações essenciais para a empresa -, não podendo estar expostas.

A segurança de sistemas baseia-se em diversos conceitos. São os chamados serviços de segurança (STALLINGS, 2015; STALLINGS, 2019), sendo eles: a privacidade, que visa garantir que seus arquivos ou documentos digitais não serão lidos por nenhuma outra pessoa que não a que você autorize; a integridade, que é um mecanismo que informa se/quando algo foi alterado; autenticidade, que é a garantia de que determinada pessoa ou instituição realmente é quem diz ser e o não repúdio - muitas vezes também chamado de irretratabilidade -, é a garantia de que determinada pessoa realmente participou de determinado processo.

Atualmente, existem diversos tipos de ataques a segurança que visam obter informações não autorizadas, desde senhas e dados pessoais até segredos de negócios das grandes organizações. Em razão disto, é necessário que os dados realmente importantes sejam protegidos com eficientes mecanismos de segurança, para não correr o risco de serem roubados, provendo a esses um meio seguro para comunicação digital, podendo suportar ataques de pessoas não autorizadas. Para a experimentação conduzida no presente trabalho, as tecnologias envolvidas são a criptografia de chave pública e privada, assinaturas digitais e esteganografia.

A criptografia, segundo Burnett e Paine (2002), tem como funcionalidade "a capacidade de conversão de dados legíveis em algo sem sentido, com a capacidade de recuperar os dados originais a partir desses dados sem sentido". Para tornar isso possível é utilizado um algoritmo criptográfico, que é "uma função matemática utilizada para cifrar e decifrar uma mensagem", (SCHNEIER,1996; MARTIN, 2020).

A criptografia fornece a pessoas ou instituições devidamente autorizadas, a determinados processos, serviços básicos de: autenticidade, confidencialidade, integridade e não repúdio para os dados. Existem diversos algoritmos de criptografia implementados atualmente; os mais utilizados são o AES, para criptografia simétrica, e o RSA, para criptografia assimétrica. A questão da simetria se refere ao emprego de chaves: se for a mesma chave para cifrar e para decifrar, temos um esquema de criptografia simétrica; se forem distintas, trata-se de criptografia assimétrica. O foco do presente trabalho se dá na criptografia assimétrica, em razão de possibilitar assinatura digital – um processo comumente mais moroso, e com desempenho menor do que os esquemas de criptografia simétrica.

O algoritmo RSA "é o mais comumente utilizado para solucionar o problema de distribuição de chaves e criptografia nos dias de hoje", segundo Burnett e Paine (2002). Foi desenvolvido por Ron Rivest, professor do *Massachusetts Institute of Technology* e seus orientandos, Adi Shamir e Len Adleman. Segundo Margi (2000), "o algoritmo apoia-se na dificuldade de fatorar números primos extensos para determinar as chaves pública e privada".

Já assinaturas digitais consistem basicamente na criação de um código de tamanho fixo resultante de uma mensagem original, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar se a mensagem possa ter sido modificada. Esse código de tamanho fixo, chamado de resumo de mensagem ou assinatura digital, é gerado através de uma função *hashing* - mecanismo utilizado para verificar a integridade de uma mensagem (MARTIN, 2020).

Há diversas implementações de algoritmos de assinatura digital, sendo os mais conhecidos são o MD, SHA-1 e o DSA. "O algoritmo que tem suas partes internas mais fortes que os outros é o SHA-1, ele produz um resumo mais longo - de 160 bits -comparado aos 128 bits do MD5", cita Burnett e Paine (2002). O SHA-1 já resistiu a análises criptográficas e é altamente recomendado pela comunidade de criptografia. Conforme Schneier (1996), "o algoritmo SHA-1 recebe uma mensagem com tamanho máximo menor que 264 bits e gera um resumo de mensagem de 160 bits, trabalhando sobre blocos de mensagem de 512 bits".

Outra tecnologia de segurança é a esteganografia - arte da escrita para comunicações ocultas (STALLINGS, 2015; MUÑOZ, 2016). De acordo com Schneier (1996) e Katz e Lindell (2020), "a esteganografia tem como finalidade esconder mensagens secretas em outras mensagens, de forma que a mensagem secreta esteja bem escondida que o invasor não consiga identificá-la". Uma das técnicas mais simples e utilizadas - e desenvolvida neste trabalho - é a técnica LSB (*Least Significant Bit*). Tal técnica basicamente consiste na utilização do bit menos significativos de cada pixel para ocultar um bit da informação. Para a utilização desta técnica são necessárias imagens que possuam qualidade de 24 bits, pois são imagens grandes que utilizam três bytes para a representação de cada pixel. A imagem possuindo três bytes por pixel - cada um deles representando a quantidade de vermelho, azul e verde de cada pixel (RGB) e contendo oito bits em cada um desses bytes, levando em consideração que cada um desses bits pode assumir valores de 0 a 255, cada pixel terá 256 valores para representar a quantidade da associação de cada uma das três cores que tem um pixel. Se apenas o bit menos significativo de cada byte for alterado, o valor desse byte irá variar somente em uma unidade. Assim sendo, essa alteração fica praticamente impossível de ser identificada a olho nu.

Materiais e Métodos

Nessa seção são apresentados os principais conceitos, requisitos, dificuldades e passos necessários para implementação deste trabalho.

A ferramenta tem como funcionalidade principal a transmissão e recebimento de mensagens que necessitem de segurança, levando em conta a necessidade de garantir os conceitos de autenticidade, integridade, confiabilidade e não repúdio, tratados anteriormente. Para isso, o protótipo de software desenvolvido neste trabalho utiliza em conjunto técnicas de criptografia, assinaturas digitais e esteganografia.

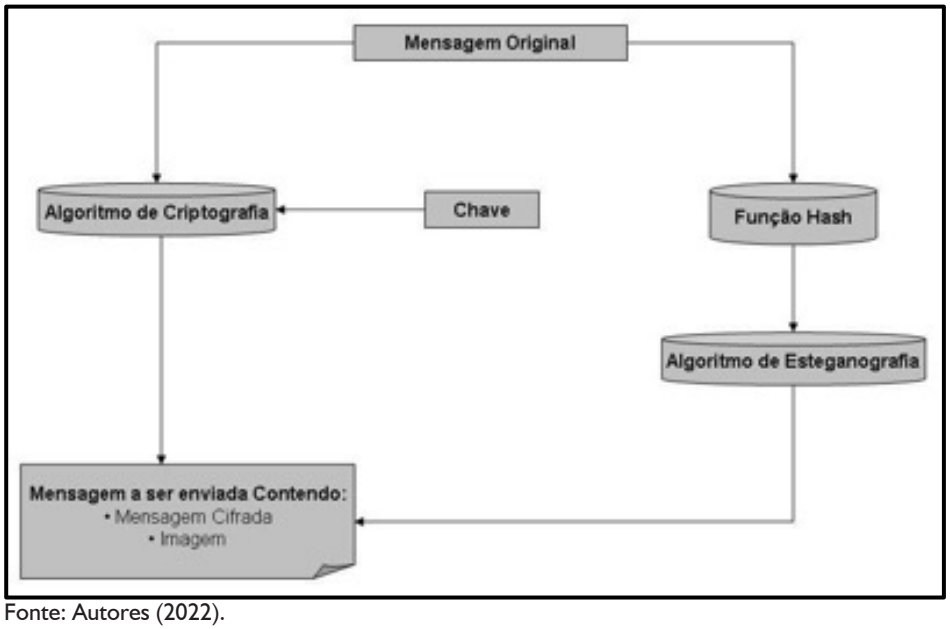
A criptografia é feita através do algoritmo de chave pública RSA, a assinatura digital, por sua vez, utiliza o algoritmo de hash SHA-1 e, por fim, a esteganografia é feita através do método LSB ou inserção no bit me-

nos significativo. Como já citado, criptografia tem como objetivo garantir a autenticidade e a privacidade da comunicação, as assinaturas digitais visam garantir a integridade das informações, sendo esta assinatura digital oculta em uma imagem digital através da técnica de esteganografia visando a não rotulação da transmissão dessa informação.

Com a utilização dessas técnicas em conjunto, atende-se a funcionalidade de dificultar o trabalho de um atacante, que tem de dedicar seu trabalho sobre diferentes informações (mensagem cifrada e imagem), empregadas em diferentes técnicas de segurança (criptografia, assinatura digital e esteganografia).

O protótipo, denominado *Camouflaged Security System*, foi desenvolvido no ambiente de programação Eclipse CDT, em linguagem de programação C. Contempla dois módulos de usuários: emissor e receptor. O emissor tem como dados de entrada uma chave de criptografia, a mensagem a ser enviada e uma imagem no formato bitmap, e tem como saída uma imagem com a assinatura digital da mensagem oculta salva no formato mapa de bits (bitmap) – além da mensagem texto cifrada, no formato texto. Os processos de envio e recepção de uma mensagem são apresentados nas figuras 1 e 2.

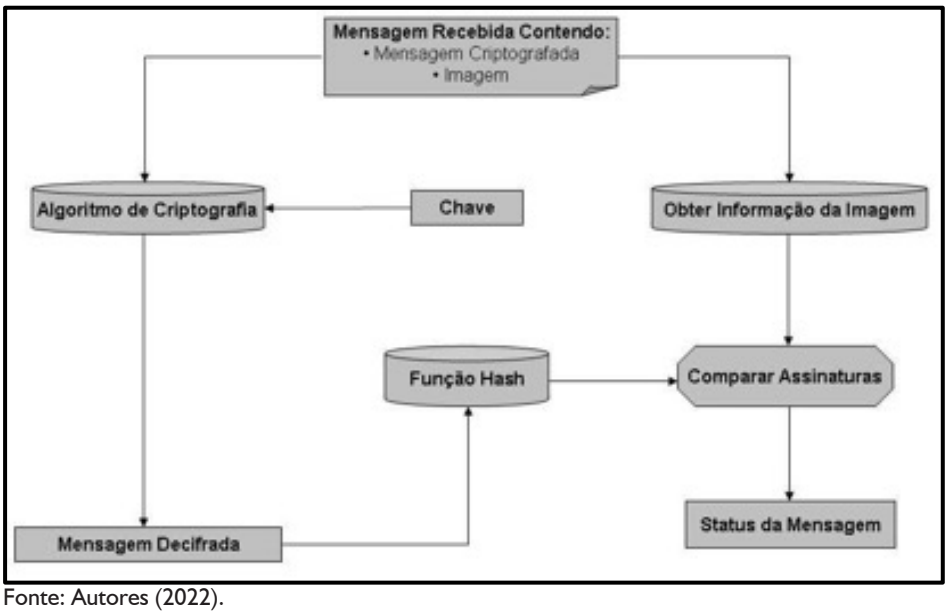
Figura 1 - Diagrama simplificado do processo de envio de mensagem empregando o *Camouflaged Security System*.



Fonte: Autores (2022).

O receptor, por sua vez, tem o arquivo texto com a mensagem criptografada e a imagem com a assinatura digital da mensagem original oculta, e terá como saída a mensagem decifrada, a assinatura digital dessa mensagem e a assinatura digital obtida de dentro da imagem recebida, podendo assim ter acesso a informação recebida e verificar o status desta.

Figura II - Arquitetura simplificada do processo de recepção de mensagem empregando o *Camouflaged Security System*



Fonte: Autores (2022).

Deste modo, é possível realizar a troca de informações sigilosas de forma segura, tendo três diferentes técnicas de segurança de sistemas empregadas em conjunto, aumentando o nível de segurança, validade da transmissão e dificultando o trabalho de um atacante, podendo ao final deste processo de envio e recebimento comparar as informações e verificar a validade da transmissão.

A Criptografia é a funcionalidade do protótipo responsável por cifrar e decifrar as mensagens transmitidas. Esta funcionalidade foi desenvolvida com o auxílio de componentes de terceiros, chamado *TPLockBox* - sendo utilizado o algoritmo RSA implementado neste componente. O *TPLockBox* é um componente *open source* desenvolvido pela empresa Turbo Power. Esse emprega diversas técnicas de criptografia e assinaturas digitais de forma profissional, proporcionando serviços de autenticação e de privacidade. O protótipo trabalha com esse componente informando a mensagem a ser cifrada ou decifrada e a chave secreta de criptografia, tendo como resultado a mensagem cifrada ou decifrada.

As Assinaturas Digitais, por sua vez, são responsáveis por gerar um resumo de mensagem, ou código *hash*, de uma mensagem. Esta funcionalidade foi desenvolvida com a utilização do componente *TPLockBox* também, fazendo o uso do algoritmo SHA -1 implementado no mesmo. O protótipo interage com esse componente, definindo a mensagem original e, tendo como resultado, um resumo de mensagem ou assinatura digital dessa mensagem. Já a esteganografia é responsável por ocultar e extrair as assinaturas digitais da imagem. Esta parte do trabalho necessita da utilização de imagens digitais no formato bitmap. Tem como dados de entrada a assinatura digital da imagem e a imagem, resultando em uma imagem com a informação oculta ou, a partir apenas da imagem, buscar a assinatura digital oculta na mesma. Foi implementada em sua totalidade, necessitando de algoritmos que trabalhem nas tonalidades das cores da imagem, buscando e alterando as mesmas, trabalhem com conversão de valores binário, decimal e ASC II e o algoritmo LSB de esteganografia.

Resultados e Discussões

A seguir, são apresentados os principais resultados dos experimentos realizados. Como a execução de técnicas de esteganografia poderia ser extremamente eficiente, dada a rapidez do algoritmo, foram considerados os tempos de processamento separadamente – ou seja, o tempo para geração de chaves pública e privada, o tempo para cifragem, para decifragem e o de ocultar a informação na mídia.

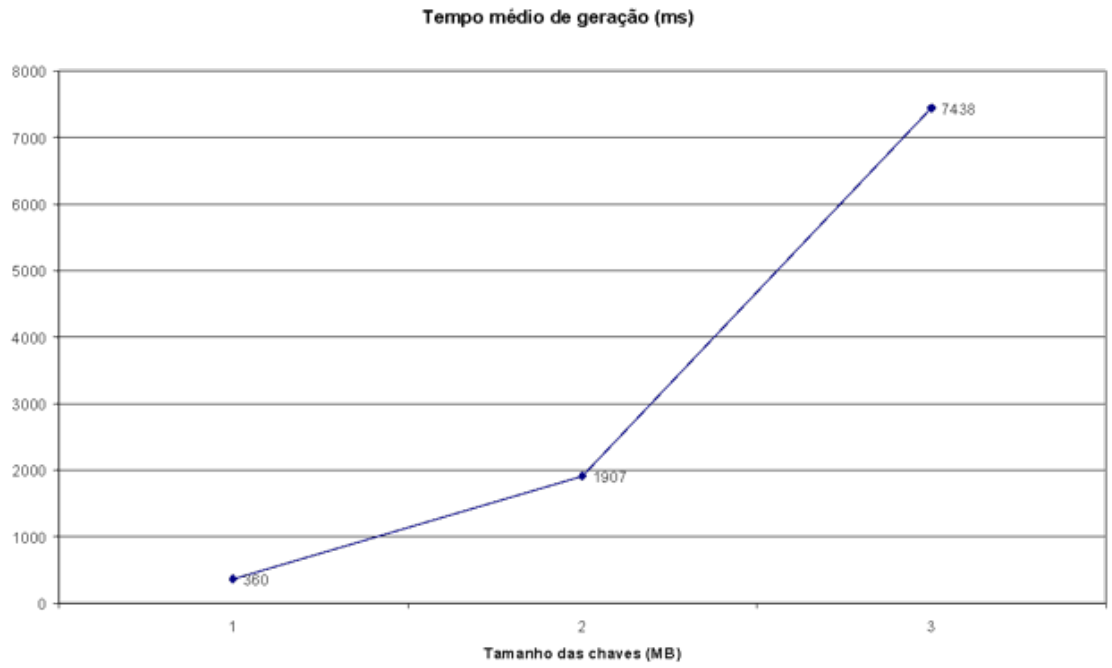
Algumas das preocupações existentes antes da aplicação das técnicas de esteganografia eram identificar se haveria percepção de diferença entre as imagens original de gerada, assim como se o tempo de processamento seria diretamente proporcional ao tamanho do arquivo – ou seja, se para uma mensagem de porte considerável, o emprego da técnica de bit menos significativo indicaria ser o tempo proporcional ao tamanho

do arquivo.

Os dados representam a média de 100 execuções no sistema, sendo utilizada a mesma mensagem e a mesma imagem. A mensagem enviada foi "Testando o Desempenho do Sistema", e a imagem tinha o tamanho de 287 bytes. Como esperado, não ocorreu alteração no tamanho da imagem, e não há percepção de diferenças ao olho humano.

A arquitetura sobre o qual o protótipo foi executado foi, propositadamente, de um *Personal Computer* com arquitetura limitada - empregado processador Celeron, 2 GB DDR2, 500 GB de HD SATA e uma placa de vídeo NVIDIA GeForce 7000 Turbo Cache.

Figura III - Tempo médio para geração de chaves públicas.



Fonte: Autores (2022).

A figura 3 apresenta gráfico gerado do tempo necessário para a geração de um par de chaves, de tamanho
128MB: 360 ms
256MB: 1907 ms
512MB: 7438 ms

Percebe-se uma tendência exponencial – contudo, embora tenham sido realizados experimentos apenas com esses três tamanhos de arquivos. Com relação ao tempo para geração de assinatura digital, essa manteve-se constante em 8 ms – tanto na operação original, quanto na operação inversa. Com relação ao tempo médio de cifrar a mensagem – 31 ms – observa-se crescente emprego de recursos ao se comparar com o tempo para decifrar a mensagem – 381,5 ms. O tempo médio de ocultar a assinatura na imagem foi de 84,5 ms, ao passo que o tempo para extração da assinatura gerada foi, em média, 40 ms.

Considerações Finais

Cabe ressaltar, na conclusão do presente trabalho, que o objetivo dos experimentos foi restrito ao domínio tempo de operações. O tempo de geração de chaves pública e privada tende a se elevar, ao contrário da técnica de esteganografia de bit menos significativo. Esse se manteve constante em 8 ms. Os resultados referentes à geração de chaves públicas eram esperados – o que não acontece com a constância dos tempos de introdução e remoção de informações nos arquivos.

Como limitações, pode-se ressaltar que podem ser analisadas outras métricas além do domínio tempo. Ademais, para as execuções, foram cancelados da memória os processos que não diziam respeito ao experimento – como programas residentes, antivírus, etc., visando o maior controle possível. Provavelmente, em

outros sistemas operacionais - onde se possa interferir em nível mais próximo da arquitetura -, seja possível efetuar melhor controle sobre a memória.

Pode ser observado que o emprego de qualquer tecnologia de segurança impacta no desempenho. Afinal, usuários – sejam organizações sejam indivíduos – não empregam recursos computacionais exclusivamente para questões de segurança. A segurança sempre será considerada overhead nos sistemas computacionais, especialmente por se tratar de requisito não desejado, mas sempre lembrado em situações de perda de privacidade.

Por fim, deve ser considerado que a tecnologia aqui empregada se restringiu tão somente a aspectos de segurança da informação – em especial, ao serviço de privacidade. Um trabalho futuro a ser considerado envolve investigar o impacto pelo emprego de outros serviços de segurança, os quais podem demandar outra estrutura para experimentação, como emprego de rede de computadores e o emprego de protocolos de comunicação.

Referências

BURNETT, Steve & PAINE, Stephen. **Criptografia e segurança: o guia oficial RSA**. 1.ed. Rio de janeiro: Campus Ltda., 2002.

KATZ, Jonathan & LINDELL, Yehuda. **Introduction to Modern Cryptography**. 3rd ed. Boca Raton: CRC Press, 2020.

MARGI, Cíntia Borges. **Um Mecanismo para Distribuição Segura de Vídeo MPEG. 2000.** Dissertação (Mestrado) – Escola politécnica da Universidade de São Paulo, São Paulo, 2000.

MUÑOZ, Alfonso Muñoz. **Privacidad y ocultación de información digital esteganografia.** Madri: RA-MA S.A. Editorial y Publicaciones, 2016.

MARTIN, Keith. **Cryptography:** The Key to Digital Security, How It Works, and Why It Matters. London: W. W. Norton & Company, 2020.

SCHNEIER, Bruce. **Applied Cryptography:** Protocols, Algorithms and Source Code in C. 2. ed. New York: John Wiley & Sons, Inc., 1996.

SCHNEIER, Bruce. **SHA-1 Broken**. Disponível em: http://www.schneier.com/blog/archives/2005/02/ sha1_ broken.html. Acesso em 27 jun.2019.

STALLINGS, William. **Criptografia e Segurança de Redes:** princípios e práticas. 6.ed. New Jersey: Prentice Hall, 2015.

STALLINGS, William. **Information Privacy Engineering and Privacy by Design:** Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices. Hoboken, NJ: Addison-Wesley Professional, 2019.