Revista Brasileira de Computação Aplicada, Julho, 2020

DOI: 10.5335/rbca.v12i2.10455
Vol. 12, Nº 2, pp. 46–53
Homepage: seer.upf.br/index.php/rbca/index

ISSN 2176-6649

ARTIGO ORIGINAL

O estado da arte das criptografias modernas: uma revisão sistemática da literatura

The state of the art of modern cryptography: a systematic literature review

Lara Ludwig[1], Miguel Grando Rebelatto[2], Sandro José Ribeiro da Silva[3]

[1]Instituto Federal do Rio Grande do Sul - Campus Canoas (IFRS), 92.412-240, Canoas, RS, Brasil

*laraludwig18@gmail.com; miguelgrandorebelatto@gmail.com; sandro.silva@canoas.ifrs.edu.br

Recebido: 18/12/2019. **Revisado:** 02/06/2020. **Aceito:** 30/06/2020.

Resumo

Neste artigo realizamos uma análise sobre as principais características dos algoritmos criptográficos modernos, a fim de obter o estado da arte das principais criptografias modernas. Utilizamos uma revisão sistemática da literatura contida em artigos publicados nas bases Science Direct e Springer Link entre os anos de 2016 à 2019. Os objetivos do estudo foram mostrar quais criptografias estavam sendo usadas em diversas áreas, tais como internet das coisas, códigos QR e redes 3G e 4G, além de analisar a melhor criptografia para cada tipo de sistema, com base nas características dos algoritmos e dos requisitos das aplicações.

Palavras-Chave: AES; Código QR; Criptografia Moderna; Internet das Coisas; RSA

Abstract

In this article, we have analyzed the key features of modern cryptography algorithms to get a state-of-the-art of main encryptions. We used a systematic review of the literature contained in articles published in the Science Direct and Springer Link databases from 2016 to 2019. The objectives of the study were to show which encryptions were used in various areas, such as Internet of Things, QR codes, 3G and 4G networks and analyze the best encryption for each type of system based on the characteristics of the algorithms and application requirements.

Keywords: AES; IoT; Modern Encryption; QR Code; RSA

1 Introdução

A criptografia tem como princípio permitir a comunicação entre um remetente e um destinatário de modo que terceiros não tenham acesso ao conteúdo compartilhado. A troca de mensagens secretas e proteção de informação não é uma necessidade exclusiva deste século. A "cifra de César", um dos métodos mais famosos de sistemas criptográficos da antiguidade, existe desde o império romano, no período de 100 a.C. a 44 a.C. O imperador Júlio César a utilizava para a comunicação com os membros do seu exército. Ela consiste em uma substituição simples das letras de uma mensagens de acordo com a posição do alfabeto (Silva, 2016).

A criptografia é necessária para proteção e segurança dos equipamentos eletrônicos e softwares conectados a internet e redes. Segundo Kouicem et al. (2018), esta consiste em fornecer os seguintes objetivos: Disponibilidade, garantir que a informação esteja sempre disponível no momento de acesso; Integridade, garantir que o conteúdo não seja alterado; Controle de acesso, somente pessoas autorizadas possuem acesso; Não-

repudiação, prevenir que uma pessoa negue o envio e/ou recebimento de uma mensagem; e, Privacidade, apenas origem e destino têm acesso.

A constante evolução tecnológica tornou a era dos computadores e da internet uma grande troca e armazenamento de dados, transformando estes como fundamentais para a população mundial. Logo, para algo tão relevante para a sociedade atual, também é necessário a proteção destas informações. Partindo desta necessidade, a criptografia moderna passou a entrar em vigor, possuindo como características a base em algoritmos matemáticos, a operação em sequência de bits binários e a existência de chaves, simétricas ou assimétricas.

Para Oliveira (2012), a chave simétrica utiliza a mesma chave para criptografar e para descriptografar dados. Com isso, este tipo de chave possibilita algoritmos mais simples e, pelo fato de possuir a mesma chave em ambas as pontas da comunicação, mais rápidos. Enquanto isso, as criptografias com chave assimétrica são compostas por duas chaves diferentes para o envio e recebimento das informações, matematicamente relacionadas. Por possuir chaves diferentes, se torna uma chave mais segura, mas para tal precisa de operações complexas para sua operação, tornando-se mais lenta.

Com a diversidade de produtos online utilizados pela população, a encriptação e proteção dos dados passou a ser fundamental em diferentes áreas, tanto em hardware como software. Este artigo analisou trabalhos que falassem sobre as criptografias aplicadas a internet das coisas, setor muito crescente na área da tecnologia, redes 3G e 4G e códigos QR (Quick Response, traduzido para português, resposta rápida), muito utilizados para facilitar a abertura de páginas web e realizar o controle de acesso, de identificação e logística (Focardi et al., 2019).

A autenticação de arquivos e mensagens e a assinatura digital são outros pontos que exigem segurança, pois é necessário garantir a integridade dos conteúdos (Yu et al., 2016). Para tal, é utilizado funções Hash, que são cálculos realizados sobre um conjunto de dados que resultam em um valor. Em troca de mensagens, por exemplo, pode-se realizar a função na mensagem de envio e, ao receber a mensagem, calcular novamente e comparar os valores, podendo assim, verificar se houve alguma alteração no conteúdo.

Com todos os diferentes equipamentos, aplicações e setores que a técnica de encriptação é utilizada, foi desenvolvido diferentes tipos de criptografia computacional. Busca-se neste artigo apresentar o estado da arte dos principais algoritmos de criptografia moderna utilizados em diferentes aplicações.

2 Referencial Teórico

Nesta seção serão apresentados as definições de alguns termos que serão vistas ao longo desta revisão, sendo dividas em criptografias simétricas (Seção 2.1), criptografias assimétricas (Seção 2.2) e funções de hash (Seção 2.3).

2.1 Criptografias Simétricas

De acordo com [Kouicem, Bouabdallah and Lakhlef 2018], nas criptografias de chaves simétricas, cada entidade no sistema deve compartilhar chaves criptográficas com todas as outras entidades no sistema.

Para Oliveira (2012), a chave simétrica utiliza a mesma chave para criptografar e para descriptografar dados. Com isso, este tipo de chave possibilita algoritmos mais simples e, pelo fato de possuir a mesma chave em ambas as pontas da comunicação, mais rápidos. São exemplos de algoritmos de chave simétrica:

- AES: O algoritmo Advance Encryption Standard (AES) foi desenvolvido em 1998 por Joan Daemen e Vincent Rijmen, que é uma cifra simétrica de bloco de chaves. O algoritmo AES suporta qualquer combinação de dados e comprimento de chave de 128, 192 e 256 bits (Patil et al., 2016);
- AES S-box: É uma matriz usada no algoritmo criptográfico AES, que é um caixa de substituição e atua como uma tabela de pesquisa (Kaul et al., 2016);
- DES: O padrão de criptografia de dados (DES) é uma cifra de bloco de chave simétrica. O comprimento da chave é 56 bits e o tamanho do bloco é 64 comprimento de bit. (Patil et al., 2016);
- 3DES: O Padrão de Criptografia de Dados foi publicado pela primeira vez em 1998, que recebe esse nome porque aplica a cifra DES três vezes para cada bloco de dados. O comprimento da chave é de 112 bits ou 168 bits e o tamanho do bloco é de 64 bits (Patil et al., 2016);
- Blowfish: É uma cifra de bloco publicada em 1993 por Bruce Schneier, com comprimento de chave variável de 32 a 448 bits e tamanho de bloco de 64 bits (Patil et al., 2016);
- RC4: É uma cifra de fluxo com tamanho de chave de até 2048 bits. Seu principal problema é o comprimento da chave ser limitada, tornando a cifra não segura (Partheeban and Kavitha, 2016).

2.2 Criptografias Assimétricas

De acordo com Pavanati et al. (2017), as abordagens assimétricas tradicionais agrupam todos os métodos com base em chaves públicas e requer autoridade para emitir certificados para diferentes usuários do sistema.

Para Oliveira (2012), as criptografias com chave assimétrica são compostas por duas chaves diferentes para o envio e recebimento das informações, matematicamente relacionadas. Por possuir chaves diferentes, se torna uma chave mais segura, mas para tal precisa de operações complexas para sua operação, tornando-se mais lenta. São exemplos de algoritmos de chave assimétrica:

- RSA: É um algoritmo criptográfico assimétrico criado por Ron Rivest, Adi Shamir e Leonard Adleman. Ele gera duas chaves: chave pública para criptografia e chave privada para descriptografar a mensagem. O tamanho da chave é de 1024 a 4096 bits (Patil et al., 2016).

2.3 Funções Hash

De acordo com Oliveira (2012), funções hash servem para garantir a integridade do conteúdo da mensagem, sendo que após feito o cálculo de hash, qualquer modificação em seu conteúdo será detectada, pois um novo cálculo sobre o conteúdo modificado resultará em um valor bastante distinto.

Para Yu et al. (2016), funções de hash desempenham um papel significativo na criptografia moderna. São indispensáveis na obtenção de sistemas seguros, como assinaturas digitais, códigos de autenticação de mensagens e assim por diante. Em 2005, muitas funções famosas de hash, incluindo MD5 e SHA-1, foram quebradas, levando o National Institute of Standards and Technology propor a transição do SHA-1 para a família SHA-2.

- MD5: É uma função de espalhamento unidirecional, um hash md5 não pode ser transformado novamente no texto original, que foi inventada por Ron Rivest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário (Oliveira, 2012);
- SHA-2: O Secure Hash Algorithm foi desenhado pela agência nacional de segurança dos Estados Unidos, para ser uma família de duas funções hash similares, com diferentes tamanhos de bloco, conhecido como SHA-256 e SHA-512. Eles diferem no tamanho, o SHA-256 utiliza 256 bits e o SHA-512 utiliza 512 bits (Oliveira, 2012);

3 Revisão Sistemática da Literatura

Nesta seção, será apresentado o planejamento da revisão sistemática da literatura (subseção 2.1) e a fase de execução desta pesquisa (subseção 2.2). Esta revisão sistemática foi feita a partir de artigos publicados entre Janeiro de 2016 a Outubro de 2019.

3.1 Planejamento da Revisão Sistemática

Para realização da revisão sistemática, é fundamental, especificar as perguntas que serão respondidas no processo de escrita dos resultados, pois são elas que vão conduzir toda a metodologia de revisão. Dessa forma, foram escolhidas as seguintes perguntas:

- Q01: Qual o "estado da arte" das criptografias modernas?
- Q02: Onde as criptografias modernas estão sendo aplicadas?

Para realização desta revisão, foram selecionadas as bases Science Direct e Springer Link.

A construção da string de busca foi baseada nas questões Q01 e Q02, só que traduzidas para o inglês, pois a maior parte dos artigos, das bases de pesquisa escolhidas, estavam em inglês. Assim, gerando o seguinte protocolo de pesquisa:

- P01: (Modern cryptography techniques in information security) AND (rsa OR aes OR md5)

Após a construção do protocolo de pesquisa, iniciou-se a elaboração dos critérios para aceitação ou rejeição dos artigos encontrados na revisão, onde estes podem ser vistos na Tabela 1.

Tabela 1: Critérios de inclusão e exclusão utilizados na revisão sistemática

Critérios de Inclusão	Critérios de Exclusão
a) Artigos em Inglês e Português (Brasil)	a) Artigos não relacionados a aplicação de técnicas de segurança na computação
b) Artigos publicados entre 2016 e 2019	b) Artigos duplicados
c) Artigos que abordam o "estado da arte" das criptografias modernas e/ou suas aplicações	c) Artigos que não sejam publicados em periódicos

Fonte: autoria própria, 2019.

3.2 Execução da Pesquisa

Por meio da execução do protocolo P01, identificou-se artigos que versavam sobre o "estado da arte" das criptografias modernas, suas principais características e onde estas estão sendo utilizadas atualmente. Foram encontrados 1374 artigos, em língua inglesa, no período determinado por esta pesquisa que foi de Janeiro de 2016 a Outubro de 2019, como pode ser visto na Tabela 2.

Tabela 2: Resultado da busca

Bases	Total	Seleção Primária	
		Excluídos	Incluídos
Science Direct	452	446	6
Springer Link	992	918	4
Total	**1474**		

No repositório da Science Direct, foram encontrados 452 artigos na busca. Aplicando-se os critérios de inclusão e exclusão o número de artigos que atendiam os mesmos resultou em 6.

Já no repositório da Springer Link foram encontrados 922 artigos na busca. Aplicando-se os critérios de inclusão e exclusão o número artigos que atendiam os mesmos resultou em 4.

Os critérios foram aplicados para direcionar a pesquisa para artigos que desenvolveram estudos e testes específicos relacionados às criptografias modernas, suprimindo-se capítulos de livros ou artigos de eventos e palestras.

3.3 Resultados e Discussões

Nesta seção, será discutido as questões Q01 e Q02, com base nos artigos encontrados através da revisão sistemática.

Tabela 3: Apresentação dos estudos quanto ao objetivo e conteúdo

Número	Autor/ano	Título	Objetivo	Conteúdo
1	Patil, P.; Narayankar, P.; Narayan, D.G.; S.M. Meena. (2016)	A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish	Analisar o desempenho dos algoritmos 3DES, AES, Blowfish e RSA	• 3DES • AES • Blowfish • RSA
2	Focardi, R.; Luccio, F.L.; Wahsheh, H.A.M. (2019)	Usable security for QR code	Analisar os esquemas criptográficos populares para proteção de códigos QR	• RSA • AES • ECDSA
3	Ravi, P.; Najm, Z.; Brasin, S.; Khairallah, M.; Gupta, S.S.; Chattopadhyay, A. (2019)	Security is an architectural design constraint	Mostrar as vulnerabilidades de segurança existentes nos algoritmos criptográficos	• RSA • AES
4	Samarasinghe, N.; Mannan, M.; (2019)	Another look at TLS ecosystems in networked devices vs. Web servers	Mostrar as criptografias utilizadas atualmente por dispositivos, tais como roteadores, modems e impressoras	• RC4 • MD5 • RSA • SHA-256
5	Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. (2018)	Internet of things security: A top-down survey	Análise das soluções de segurança propostas recentemente na internet das coisas	• AES • RSA
6	Kaul, V.; Nemade, B.; Bharadi, V. Dr.; khedkar, S.K.N. Dr. (2016)	Next Generation Encryption Using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks	Aprimoramento do AES para uso em redes atuais e de próxima geração	• AES
7	Dinu, D.; Corre, Y.L.; Khovratovich, D. (2019)	Triathlon of lightweight block ciphers for the Internet of things	Comparar as implementações de cifras leves, para obter resultados do quão bem elas são adequadas para proteger a Internet das coisas	• AES
8	Yu, H.; Hao, Y.; Bai, D. (2016)	Evaluate the security margins of SHA-512, SHA-256 and DHA-256 against the boomerang attack	Avaliar as margens de segurança das funções hash: SHA-512, SHA-256 e DHA-256, contra o ataque do bumerangue	• SHA-512 • SHA-256 • DHA-256
9	Partheeban, P.; Kavitha, V. (2018)	Dynamic key dependent AES S-box generation with optimized quality analysis	Análise do algoritmo AES com uma caixa S-box dinâmica	• AES
10	Patel, K. (2019)	Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files	Analisar a performance dos algoritmos AES e Blowfish em pequenos e grandes arquivos de dados	• AES • RSA

Fonte: autoria própria, 2019.

Na Tabela 3, estão organizados os trabalhos analisados, com os autores, título, objetivo da pesquisa e a qual algoritmo criptográfico aquele trabalho está relacionado.

Por meio da análise dos artigos encontrados na revisão, identificamos que as criptografias modernas estão

sendo aplicadas em diversos lugares, tais como, internet das coisas, redes 3G e 4G e códigos QR.

Para Kouicem et al. (2018), a internet das coisas sofre de vários problemas de segurança. questões que são mais desafiadoras do que as de outras áreas em relação ao seu ambiente complexo e dispositivos com recursos limitados. Assim, os autores realizaram a pesquisa com base em duas perspectivas, as criptografias tradicionais, RSA e AES, e as outras abordagens baseadas em novas tecnologias emergentes como SDN, que permite controlar a rede de maneira central usando aplicativos de software, e Blockchain, tecnologia de registro distribuído que visa a descentralização como medida de segurança.

De acordo com a pesquisa realizada por Kouicem et al. (2018), soluções tradicionais são, geralmente, eficientes em termos de armazenamento e computação, mas limitados em termos de escalabilidade e heterogeneidade. Quando utilizadas para soluções baseadas em blockchain lidam muito bem com problemas de escalabilidade e heterogeneidade, graças à arquitetura distribuída oferecida por essa tecnologia, tendo como desvantagens o consumo de energia e a latência. Já as abordagens SDN otimizam de maneira muito eficiente os custos de computação, consumo de energia e recursos de rede, pois todas as tarefas de controle são dedicadas a servidores de alto desempenho. Sendo uma abordagem centralizada, a SDN não lida com eficiência com problemas de escalabilidade na internet das coisas.

Ainda na área de internet das coisas, Dinu et al. (2019) realizaram uma pesquisa com 19 cifras de blocos leves em 3 plataformas comumente usadas nesta área, para avaliar o tempo de execução, tamanho do código binário e uso da memória RAM de cada uma para provar que essas cifras são adequadas para proteger a internet das coisas.

O resultado da pesquisa foi que as cifras Chaskey e Speck tem um desempenho consistente nos cenários de uso e nas três plataformas, o que os torna forte candidatos a serem usados na internet das coisas.

Na área de proteção de códigos QR, para Focardi et al. (2019), as pessoas tendem a escanear códigos QR e confiar em seu conteúdo, ficando expostas a ataques, como o redirecionamento para um site mal-intencionado ou a infecção de um smartphone por um malware. Embora não exista um mecanismo padrão para fornecer autenticidade e confidencialidade do conteúdo do código, os autores fizeram a comparação entre algoritmos criptográficos populares com base em desempenho, segurança e o quanto eles afetam a usabilidade.

De acordo com a pesquisa de Focardi et al. (2019), o HMAC (Hash-based Message Authentication Code), código de autenticação de mensagens baseado em funções hash, é altamente utilizável e seguro e pode fornecer uma alternativa às assinaturas digitais para autenticação e integridade. O AES é altamente utilizável e seguro, com qualquer tamanho de chave, no entanto, é recomendado o uso do GCM (Galois/Counter Mode), modo de operação para algoritmos de chave simétrica, pois fornece confidencialidade e autenticação \ integridade. Os resultados mostram, também, que o ECDSA (Elliptic Curve Digital Signature Algorithm), algoritmo de assinatura digital de curvas elípticas, e RSA com chaves pequenas são utilizáveis em códigos QR, mesmo quando impressos em tamanhos pequenos, por exemplo, em produtos de supermercado. Outro ponto observado é que a inclusão de certificado nos códigos QR apresentou problemas de usabilidade, sugerindo que o uso de certificados on-line pode ser uma alternativa, podendo ser baixados via protocolo HTTPS (Hyper Text Transfer Protocol Secure). Este protocolo possibilita a transmissão dos dados por uma conexão criptografada, que verifica a autenticidade do servidor e do cliente por meio de certificados digitais.

Nas redes de próxima geração, tecnologias como LTE (Long Term Evolution) fornecerão velocidades onde será possível oferecer aplicativos e serviços, como videoconferência, jogos e downloads de filmes, que trazem experiência de desktop para os dispositivos sem fio dos usuários. Essas novas tecnologias exigem que as funções de segurança sejam de maneira ideal e eficiente incorporada ao sistema geral (Kaul et al., 2016).

Para alcançar um nível de segurança e velocidade adequado para as redes de próxima geração, Kaul et al. (2016) fazem a comparação de desempenho e segurança do algoritmo AES tradicional e de modificações do AES.

Os resultados foram que o AES round structure, etapas de encriptação e desencriptação do algoritmo, com S-BOX dinâmico tem a velocidade de cerca de 2 Mbps, sendo compatível com a rede LTE, além de ser mais resistente a ataques.

Em relação ao estado da arte das criptografias modernas, Patil et al. (2016) realizaram implementação e análise dos algoritmos criptográficos RSA, AES, Blowfish e 3DES em relação ao desempenho, analisando os seguintes critérios: tempo de criptografia e descriptografia, uso de memória, tempo de avalanche (força do algoritmo criptográfico), entropia(medida da aleatoriedade da informação) e o número de bits necessários na codificação de caracteres.

Os resultados foram que em aplicações que necessitem menor uso de memória, maior segurança contra ataques de adivinhação e menor tempo de criptografia e descriptografia, o algoritmo Blowfish é a melhor opção. Já se a aplicação necessitar de confidencialidade, integridade e força criptográfica, a opção ideal seria o algoritmo AES, embora ele exija maior largura de banda para transmissão. Se a aplicação necessitar de menor largura de banda, o algoritmo 3DES é o mais adequado. A Fig. 1 apresenta os resultados da análise dos algoritmos em relação ao tamanho do arquivo por seu tempo de encriptação, mostrando que o RSA leva mais tempo para realizar o processo de encriptação, enquanto o Blowfish é o mais rápido. A Fig. 2 apresenta o tempo do processo de descriptografia dos algoritmos relacionado ao tamanho do arquivo, mostrando que os mesmos necessitam de menos tempo para descriptografar um arquivo do que para criptografar.

Outro trabalho que deu enfoque a questão de performance foi Patel (2019), que realizou uma análise do desempenho dos algoritmos AES e Blowfish na encriptação de grandes e pequenos arquivos de dados, onde os parâmetros medidos foram o tempo de execução e o uso de memória.

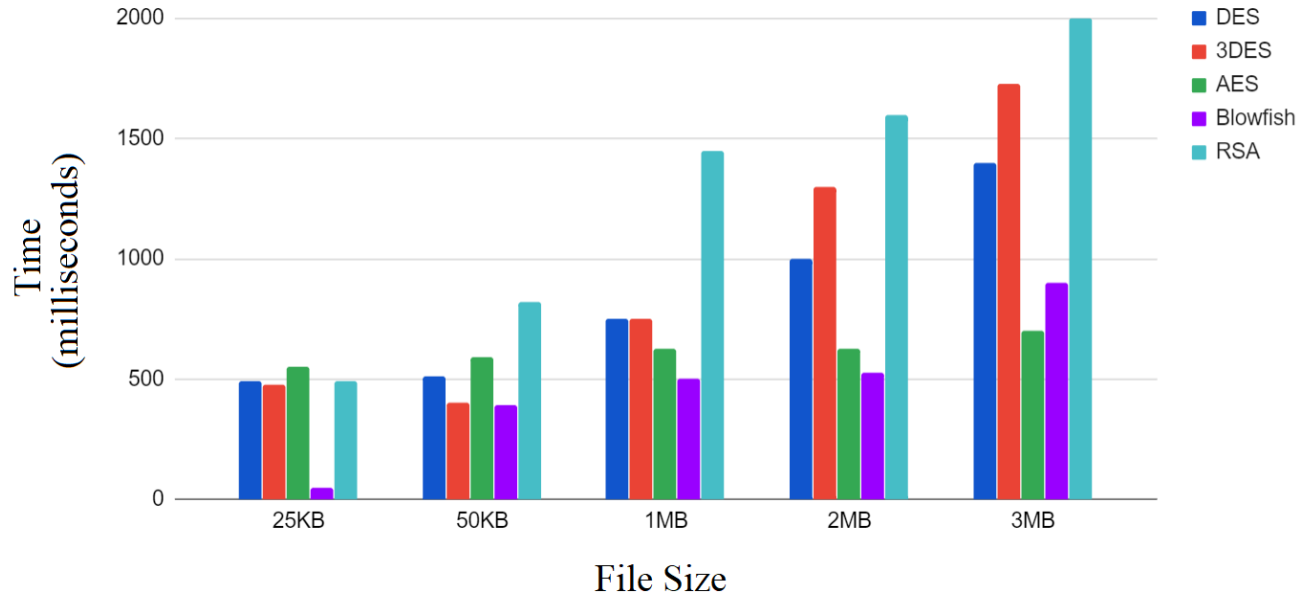

Figura 1: tempo de encriptação

Fonte: Adaptado de Patil et al. (2016).

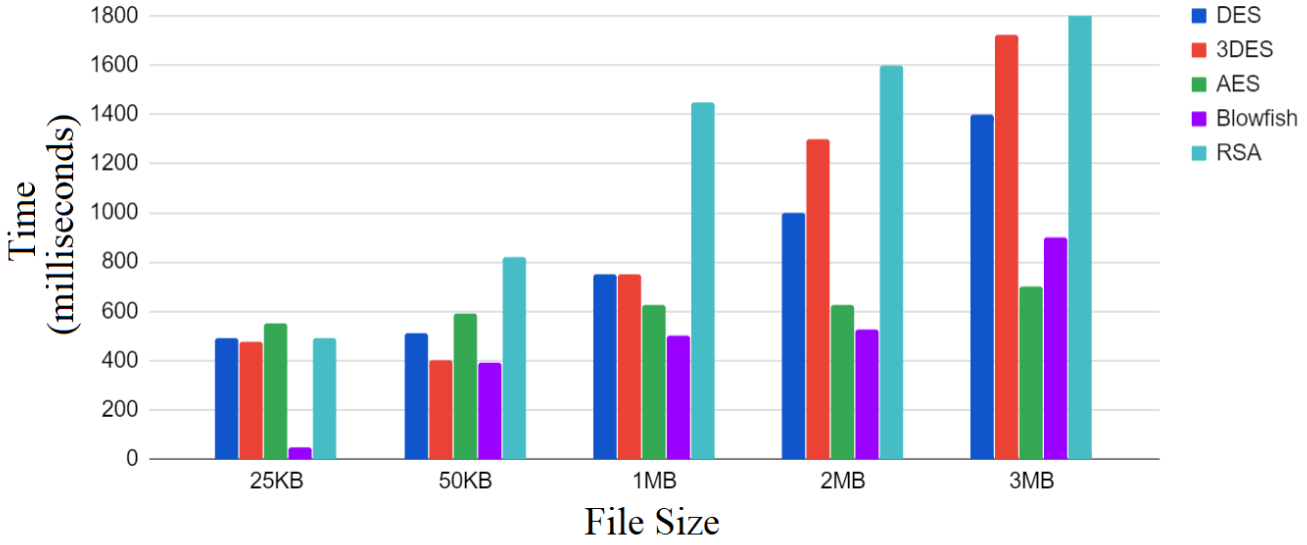

Figura 2: tempo de desencriptação

Fonte: Adaptado de Patil et al. (2016).

O estudo mostrou que o desempenho do algoritmo Blowfish é melhor que o do AES, com base no tempo de execução em pequenos arquivos de dados de texto (tamanho menor que 1000 bytes) e em arquivos grandes (tamanho maior que 10.000 bytes) o desempenho dos algoritmos é quase igual. Outro ponto observado, foi que para aplicativos com restrição de memória, o uso do Blowfish deve ser aconselhável para implementação de segurança.

Em um dos artigos analisados (Samarasinghe and Mannan, 2019), é feita uma pesquisa em dispositivos, tais como roteadores, modems e impressoras, para analisar os algoritmos criptográficos utilizados. Os resultados foram que, embora haja um crescimento no uso de criptografias mais seguras, como SHA-256 e RSA com tamanho de 2048 ou 4096, alguns fabricantes parecem ainda produzirem um número maior de dispositivos com RC4, MD5 e comprimentos de chave de 1024 bits (RSA) e abaixo, que são considerados algoritmos inseguros, além de ter sido encontrado um número considerável de chaves privadas conhecidas em dispositivos.

Ainda sobre a temática de segurança, de acordo com Ravi et al. (2019), alguns dos problemas que afetam a segurança do algoritmo criptográfico RSA é o ataque conhecido como "LogJam", que é causado pela reutilização de valores, por exemplo os números primos, do cálculo para geração de chaves do algoritmo RSA, além do ataque "Hastad Broadcast", que acontece quando é usado um pequeno expoente de chave secreta para geração de assinaturas.

Ainda, segundo Ravi et al. (2019), todos esses problemas poderiam ser evitados caso fosse dado tanta importância a segurança do sistema, quanto se dá a outras questões, como o desempenho.

Por fim, Partheeban and Kavitha (2016) propõem uma caixa S-BOX dinâmica para o algoritmo AES, como forma de proteção contra ataques de força bruta.

4 Conclusões

Este artigo apresentou uma revisão sistemática da literatura sobre as principais características e onde estão sendo aplicados os algoritmos criptográficos modernos. A pesquisa utilizou as bases Science Direct e Springer Link, pesquisando por artigos publicados entre os anos de 2016 à 2019. Foram encontrados 1374 artigos e, após a aplicação dos critérios de inclusão e exclusão, o número resultou em 10.

Os resultados obtidos após a leitura dos artigos selecionados, foi que não existe o melhor algoritmo criptográfico, e sim, o que melhor se encaixa nas especificações do dispositivo e requisitos do cliente, sendo necessária a análise caso a caso para a escolha do algoritmo.

Assim, na área da internet das coisas, com seu ambiente complexo e dispositivos com recursos limitados, se a necessidade for armazenamento e computação, os algoritmos AES e RSA serão uma boa escolha, já se a necessidade for por escalabilidade e heterogeneidade, soluções baseadas em blockchain serão melhores. Ainda, se a demanda for por baixo custo computacional, menor consumo de energia e recursos de rede, a melhor escolha será pelo uso da abordagem SDN.

Na área de proteção de códigos QR, o uso do HMAC, como alternativa às assinaturas digitais, AES no modo GCM, ECDSA e RSA, com chaves pequenas, mostraram resultados positivos, com base na comparação de desempenho, segurança e o quanto eles afetam a usabilidade. Porém, a inclusão de certificado nos códigos QR apresentou problemas de usabilidade, sugerindo que o uso de certificados on-line pode ser uma alternativa.

De maneira geral, o algoritmo Blowfish é mais adequado para aplicações que necessitem de menor uso de memória, maior segurança contra ataques de adivinhação e menor tempo de criptografia e descriptografia. Já se a aplicação necessitar de confidencialidade, integridade e força criptográfica, a opção ideal seria o algoritmo AES. Por fim, se a aplicação necessitar de menor largura de banda, o algoritmo 3DES é a melhor opção.

Um último ponto a ser comentado, é a importância de se pensar na segurança das aplicações, antes mesmo de desenvolvê-las, além de não abdicar dela para conseguir melhores resultados em outras áreas, como performance.

Referências

Dinu, D., Corre, Y. L., Khovratovich, D., Perrin, L., Großschädl, J. and Biryukov, A. (2019). Triathlon of lightweight block ciphers for the internet of things, **9**: 283–302. https://doi.org/10.1007/s13389-018-0193-x.

Focardi, R., Luccio, F. L. and Heider, A. (2019). Usable security for qr code, **48**(102369). https://doi.org/10.1016/j.jisa.2019.102369.

Kaul, V., Nemade, B., Bharadi, D. V. and Khedkar, S. K. N. (2016). Next generation encryption using security enhancement algorithms for end to end data transmission in 3g/4g networks, **79**: 1051–1059. https://doi.org/10.1016/j.procs.2016.03.133.

Kouicem, D. E., Bouabdallah, A. and Lakhlef, H. (2018). Internet of things security: A top-down survey, **141**: 199–221. https://doi.org/10.1016/j.comnet.2018.03.012.

Oliveira, R. (2012). Criptografia simétrica e assimétrica: os principais algoritmos de cifragem, *Revista Segurança Digital* **5**: 11–24. https://www.researchgate.net/publication/303367222_Criptografia_simetrica_e_assimetrica_os_principais_algoritmos_de_cifragem.

Partheeban, P. and Kavitha, V. (2016). Dynamic key dependent aes s-box generation with optimized quality analysis, **22**: 14731––14741. https://doi.org/10.1007/s10586-018-2386-6.

Patel, K. (2019). Performance analysis of aes, des and blowfish cryptographic algorithms on small and large data files, **11**: 813––819. https://doi.org/10.1007/s41870-018-0271-4.

Patil, P., Narayankar, P., D.G., N. and S.M., M. (2016). A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish, **78**: 617–624. https://doi.org/10.1016/j.procs.2016.02.108.

Pavanati, A., Souza, J. M. B. d., Nunes, H. and Coelho, A. (2017). Documentos digitais na gestão universitária: O certificado digital como garantia de segurança, origem e integridade. https://repositorio.ufsc.br/xmlui/handle/123456789/181080.

Ravi, P., Najm, Z., Brasin, S., Khairallah, M., Gupta, S. S. and Chattopadhyay, A. (2019). Security is an architectural design constraint, **68**: 17–27. https://doi.org/10.1016/j.micpro.2019.03.003.

Samarasinghe, N. and Mannan, M. (2019). Another look at tls ecosystems in networked devices vs. web servers, **80**: 1–13. https://doi.org/10.1016/j.cose.2018.09.001.

Silva, J. d. S. (2016). Alguns métodos de criptografia. http://tede.bc.uepb.edu.br/jspui/handle/tede/2619.

Yu, H., Hao, Y. and Bai, D. (2016). Evaluate the security margins of sha-512, sha-256 and dha-256 against the boomerang attack. https://doi.org/10.1007/s11432-015-5389-4.