Análise e Comparação de Algoritmos Criptográficos aplicados à IoT

Analysis and Comparison of Cryptographic Algorithms applied to IoT

Valtensir L. Junior, Gabriel A. D. Miranda, Kênia C. Gonçalves, Carlos A. Silva
Instituto Federal de Minas Gerais - Sabará
Sabará, Brasil
{valtensirl, gabriel.alan32}@gmail.com
{kenia.carolina, carlos.silva}@ifmg.edu.br

***Resumo* — Devido aos rápidos avanços tecnológicos relacionados à dispostivos e sensores, a Internet das Coisas ou *Internet of Things* (IoT) vem sendo tema recorrente de pesquisas acadêmicas, devido ao fato da mesma proporcionar vantagens aos usuários como integração de serviços, facilidade de acesso e otimização de processos. Porém, estes avanços também podem viabilizar falhas de segurança, podendo causar prejuízos sociais e econômicos de grande magnitude. Desta forma, faz-se necessário o desenvolvimento de eficientes métodos de segurança da informação a fim de garantir o bom funcionamento das comunicações realizadas no ambiente de IoT. Este trabalho busca comparar clássicos algoritmos criptográficos da literatura utilizando o microcontrolador ESP8266 comumente utilizado em aplicações IoT.**

Palavras Chave - criptografia; IoT; segurança da informação; algoritmos.

***Abstract* — Technology is advancing daily. The use of the internet, devices and sensors are increasingly present in daily life making the Internet of Things (IoT) the subject of recent research. The technologies of the IoT provide many benefits to the world, but it can also provide security breaches and can cause major social and economic losses. In this way it is necessary to develop efficient methods of information security. In this work we implement, analyze and compare classical cryptographic algorithms of the literature using the ESP8266 microcontroller commonly used in IoT applications.**

Keywords - cryptography; IoT; information of security; algorithms.

I. INTRODUÇÃO

A internet das coisas, do inglês "*Internet of things*", comumente conhecida como **IoT** é uma promissora tecnologia na qual deve conectar bilhões de dispositivos. É esperado que, em um futuro bem próximo, as casas estejam equipadas com automação e dispositivos inteligentes, todos conectados via internet. Estima-se que em 2020 haja mais de 50 bilhões de dispositivos conectados à internet [1], ou seja, para cada pessoa na Terra deve haver mais de 6 dispositivos ou objetos online. No planeta, haverão milhões de sensores coletando informações de dispositivos físicos e enviando-as para a internet. As aplicações da **IoT**, apesar de recentes, evoluem muito rapidamente. Em [2] são descritos alguns trabalhos que mostram aplicações diversas de seu uso, como na área de saúde, área de mineração, previsão de desastres, serviços automotivos, sistemas de transporte público, entre outros. Para o uso desta tecnologia é necessário que os usuários se sintam confiantes em relação à privacidade e segurança de seus dados. Devido ao grande número de conexões geradas por esta tecnologia, em virtude de sua própria natureza, um vazamento de informação pode ter graves consequências econômicas e/ou sociais. Com a tendência do *Big Data* e com o aumento do número de comunicações, faz-se necessário desenvolver mecanismos de segurança de informação, a fim de garantir a confidencialidade, integridade e autenticidade dos dados trafegados na rede virtual [3]. Uma alternativa para se obter a segurança mencionada é a codificação e encriptação das informações da rede, por meio de criptografia. Porém, algoritmos criptográficos são, em geral, caros computacionalmente, e a opção por algoritmos menos complexos pode comprometer a integridade desejada das informações. De acordo com [4], estas ameaças podem ser consideradas como um dos principais obstáculos para a utilização da **IoT**. Apesar de toda facilidade que pode ser gerada, sua segurança é frágil em virtude de algumas características como: a conexão sem fio, que possibilita facilmente uma invasão a dispositivos ou captação de informações e a ineficiência com gastos de energia, em virtude de sua capacidade computacional.

Neste trabalho, implementamos cinco algoritmos criptográficos baseados em cifras de blocos ambientados para o

2019 14th Iberian Conference on Information Systems and Technologies (CISTI)
19 – 22 June 2019, Coimbra, Portugal
ISBN: 978-989-98434-9-3

cenário da **IoT,** caracterizado nesta pesquisa pelo microcontrolador *ESP8266*. Os algoritmos pertencem à classe de cifras simétricas. Para a comparação entre as técnicas foram utilizadas como variáveis respostas o consumo de tempo, energia e memória para a encriptação/decriptação das chaves distintas em relação ao seu tamanho, além da vazão de bits envolvida neste processo. Este artigo está organizado da seguinte forma. Na seção I é apresentada uma introdução sobre o problema abordado, a proposta de solução e a motivação do estudo realizado neste trabalho. Na seção II é descrito o cenário da **IoT** no mundo, caracterizando a importância desta tecnologia e discutindo sobre suas fragilidades. Os métodos computacionais utilizados e simulados no cenário da **IoT** são descritos na seção III, bem como os trabalhos correlatos ao desenvolvimento e implementação destes algoritmos criptográficos. A análise dos dados gerados pela simulação dos métodos apresentados na seção anterior estão presentes na seção IV. Por fim, a conclusão deste trabalho é apresentada na seção V.

II. O CENÁRIO DA INTERNET DAS COISAS

A evolução da computação, tanto em relação a softwares quanto a hardwares; a ampliação e disponibilização da conectividade; a redução de custos de dispositivos e sensores; além da crescente utilização de computação em *nuvem* tem proporcionado uma revolução tecnológica mundial. A inserção e utilização de dispositivos conectados à internet tem sido cada vez mais frequente no cotidiano das pessoas. Esses dispositivos, quando conectados à internet e acoplados à análise de dados habilitados para *nuvens*, têm o potencial de revolucionar a vida pessoal e profissional das pessoas, e promover significativos impactos sociais e econômicos. Baseando-se nesta premissa, esta seção apresenta o cenário da **IoT** pelo mundo.

A. A Internet das Coisas no Mundo

A **IoT** permite que dispositivos altamente restritos sejam interconectados e comunicáveis para a realização de tarefas que podem simplificar consideravelmente atividades do nosso cotidiano. Além disso, ela tem trazido o potencial dos softwares e da internet para o mundo físico por meio de sensores, dados, criptografia e *nuvens*.

Apesar do termo **IoT** ser bastante atual, a história da internet das coisas começa no início da década de 90, quando uma torradeira foi conectada à internet para controlá-la remotamente [5]. Desde então, pesquisadores têm investido no estudo sobre conexão de dispositivos à internet para diversas finalidades. Diversos estudos como indicam [5], apontam benefícios proporcionados pela **IoT** como, redução de custos na saúde, diminuição de criminalidade, desobstrução de tráfego, minimização da emissão de gases poluentes, diminuição de mortes no trânsito e melhorias na qualidade de vida.

Conforme [9], em 2010 o número de dispositivos no mundo ligadas à internet ultrapassou o número de pessoas. Atualmente, para cada pessoa dos EUA existem em média 10 dispositivos conectados, sendo que a estimativa para 2022 é de termos 500 dispositivos conectados por domicílio familiar, entre televisores, termostatos, despertadores, torradeiras, cafeteiras, dentre outros. A Fig. 1 ilustra importantes estatísticas a respeito das vantagens da **IoT**.

Figura 1. Impacto Social/Econômico da **IoT** nos EUA (figura adaptada de [9, pp. 8]

O sucesso da comunicação sem fio entre dispositivos que caracteriza a **IoT** dependia da disponibilidade de equipamentos, do ponto de vista da viabilidade econômica e baixo consumo de energia de equipamentos. A adoção de chips RFID de baixo consumo de energia, resolveu parcialmente este problema. Outros avanços contribuíram para a evolução desta comunicação entre os dispositivos, como a adoção do IPv6 que tende a suprimir a demanda de IPs para o crescente número de dispositivos.

De acordo com [7] 8,4 bilhões de dispositivos de **IoT** estavam em uso em 2017, um aumento de 31% em relação a 2016 e deve chegar a 20,4 bilhões em 2020. Informações de [8] indicam que 86% das empresas esperam aumentar seus gastos em **IoT** em 2019. Além disso, as empresas aumentaram seus investimentos nesta tecnologia em 4% em 2018 em relação a 2017, gastando uma média de US$ 4,6 milhões em 2018. Ainda segundo [8], quase metade das empresas entrevistadas globalmente estão buscando fortemente investimentos em **IoT** com o objetivo de transformar digitalmente seus modelos de negócios nesta década. Cerca de 38% das empresas têm implantações de **IoT** e 55% têm uma visão de **IoT**, e estão atualmente executando seus planos nesta direção. Maiores detalhes podem ser obtidos em [9].

ISBN: 978-989-98434-9-3

III. ALGORITMOS CRIPTOGRÁFICOS

Nesta seção são apresentados os algoritmos criptográficos implementados neste artigo para a análise de seus comportamentos em ambiente da **IoT**, caracterizado nesta pesquisa pelo acesso e processamento de informações no microcontrolador *ESP8266*, sendo tal componente popularmente conhecido nos últimos anos pela facilidade e prática integração à redes *Wi-Fi* e conexões TCP/IP de projetos eletrônicos. São apresentados também, trabalhos correlatos à criptografia na **IoT,** baseados nesses algortimos.

B. Advanced Encryption Standard (AES)

O *Advanced Encryption Standard* (AES) [20], ou em português Padrão de Criptografia Avançada, é um algoritmo de chave simétrica, ou seja, a mesma chave é usada para criptografar e descriptografar os dados. O AES é baseado em uma criptografia de blocos, sendo uma das criptografias simétricas mais usadas no mundo, com alto grau de confiabilidade e com compatibilidade com diversos sistemas operacionais.

C. Simon e Speck

Os algoritmos de Simon e Speck [21] são algoritmos de cifras de bloco leve que se adequam a diversas aplicações em **IoT**, sistemas embarcados, computação pervasiva ou ubíqua, além de cenários onde o hardware disponível é limitado quanto ao processamento, consumo de energia e memória. A cifra de bloco é uma função que mapeia blocos de *n*-bits de texto não cifrado para blocos de *n*-bits de texto cifrado, sendo *n* o comprimento do bloco. Existem, na literatura, diversos algoritmos criptográficos baseados em cifras de bloco leve, especialmente entre os anos de 1985 e 2015, como é descrito em [22]. Os algoritmos de Simon e Speck são baseados na função de Feistel e em redes de substituição-permutação. O algoritmo de Speck foi otimizado para o desempenho em implementações de software, enquanto o algoritmo de Simon foi otimizado para desempenho em implementações de hardware.

D. Curupira

Projetado para plataformas com restrições de memória, energia e capacidade de processamento, o algoritmo de Curupira [23] tem sido aplicado em redes móveis, redes de sensores ou sistemas dependentes de *tokens* e *smart cards*. Seu funcionamento baseia-se em blocos de 96 bits e aceita chaves de 96, 144 ou 192 bits, com um número variado de *rounds*. Esta cifra possui uma estrutura involutiva e possibilidade de escalonamento de chaves facilmente inversíveis. O Curupira segue a Estratégia de Trilha Larga como o próprio AES, porém, uma das diferenças entre Curupira e AES é que o AES não possui estrutura involutiva, o que minimiza a segurança quanto a encriptação e decriptação. Existem duas versões deste algoritmo, o Curupira1 e o Curupira2. Ambos utilizam a mesma estrutura da função de *round*, porém o Curupira2 adota um algoritmo de escalonamento de chaves menos conservador.

*E. Trabalhos Correlatos à Criptografia na **IoT***

Existe, na literatura, uma grande variedade de artigos envolvendo criptografia na **IoT** aplicada a diversas áreas como segurança, saúde, lazer, entre outros. Para trabalhos no estilo de *survey* destaca-se [10, pp.286-291] onde os autores listam algoritmos de criptografia leve, ou seja, algoritmos adaptados para implementação em ambientes restritos, e apresentam comparações entre os mesmos, desenvolvidos em diferentes plataformas. Em [11] são apresentados problemas de segurança em um ambiente restrito onde algoritmos criptográficos tradicionais não podem ser usados, sendo feita uma comparação de algoritmos de criptografia leve, além de discutir os desafios da pesquisa nesta área, bem como os problemas e propostas de soluções associadas a este tema. Em [12] os autores propõem o *EXPer*, um novo algoritmo de criptografia leve para multimídia em **IoT**, sendo este método baseado em uma cifra de fluxo simétrico envolvendo operações *XOR* com chaves de 128 bits. O algoritmo proposto foi comparado com o AES e obteve melhor resultado em termos de segurança quando aplicado em aplicativos de vídeo em tempo real. Ainda relatando trabalhos recém publicados em 2018-2019, faz-se menção à [13] no qual, motivados pela evolução dos dispositivos eletrônicos integrados à *nuvens*, os autores propõem um algoritmo criptográfico em FGPA, considerando como parâmetros de eficiência: velocidade, área e potência. Dentre a comparação com algoritmos conhecidos como Simon e AES, o algoritmo proposto foi mais rápido e apresentou menor consumo de memória.

Para os algoritmos abordados neste artigo, pode-se citar o trabalho de [14], o qual apresenta uma alternativa à autenticação e re-autenticação durante a conexão e transferência de dados em redes *Wi-Fi* com protocolos de segurança *WPA*/*WPA2*. O algoritmo proposto é baseado em Criptografia de Curva Elíptica (CCE), apresentando imunidade às vulnerabilidades existentes no *WPA2*. O algoritmo de Curupira é usado em [15] para a construção de um *benchmark* em função do tempo e consumo de energia levando em consideração diferentes plataformas e sistemas operacionais. Segundo os autores, estes são os primeiros resultados de *benchmark* de criptografia simétrica para a plataforma Edison de **IoT**. Nos resultados apresentados, o algoritmo de Curupira não apresenta uma boa performance em relação aos demais algoritmos presentes nos testes realizados. O artigo [16] aborda a comunicação multimídia na **IoT,** destacando seu crescimento exponencial em diversas áreas como sensoriamento, saúde e indústria, porém adverte sobre a insegurança das redes onde estes dados trafegam. Desta forma, é apresentado um estudo sobre um algoritmo desenvolvido pelos autores baseado no algoritmo criptográfico Simon para uso acionado pela **IoT**, especialmente na área de saúde. Os autores compararam o algoritmo desenvolvido ao AES e demais algoritmos de codificação em bloco, levando em consideração o tempo de execução e consumo de memória. Os resultados mostraram adequação do algoritmo quanto à proteção de dados em configurações próprias da tecnologia abordada. Um interessante estudo sobre o algoritmo AES e o algoritmo Simon é apresentado em [17]. A base de comparação entre os

ISBN: 978-989-98434-9-3

algoritmos leva em consideração a área, a potência e tempos de atraso no compilador RTL (Cadence) usando CMOS de 180nm e 90nm. Os resultados mostram superioridade do algoritmo de Simon quando aplicado em cenários com recursos limitados. Uma nova microarquitetura AES de 32-bit é apresentado em [18] para aplicativos de **IoT**. Os resultados indicam economia de 20% da área ou de energia por bit na mesma área quando comparado com outras arquiteturas 32-bit. Um fato interessante sobre o algoritmo Speck é sua relação com o Linux. Ele foi incluído no Kernel 4.17 como uma estratégia do Google para o *dm-crypt* e o *fscrypt* do Android. O propósito seria fornecer criptografia no Android Go, uma versão do Android para smartphones de nível básico, pois o AES não é considerado rápido o suficiente para operar em baixo nível. No entanto, a *International Standards Organization* (ISO) considera a Speck uma criptografia insegura, sendo noticiado que esta criptografia está sendo removida a partir do Kernel 4.20 [19].

IV. Simulação e Análise dos Resultados

As metodologias criptográficas abordadas neste artigo são baseadas em cifras de bloco leve cujas implementações lógicas são realizadas nos níveis de software e hardware. As métricas utilizadas para analisar o comportamento dos algoritmos levam em consideração a velocidade de encriptação/ decriptação das chaves, sendo caracterizada pelo tempo de execução dos algoritmos em milissegundos; consumo de memória RAM utilizada durante a execução dos métodos medida em bytes; vazão do algoritmo medida em megabits por segundos (Mb/s); além do gasto energético para as simulações no microcontrolador *ESP8266*. As simulações dos testes ocorrem em dois cenários, conforme apresentado na Tabela 1:

Tabela 1. Ambientes para as simulações computacionais

	Hardware	Especificação do Hardware
Cenário 1 (simulando **IoT**)	*ESP8266*	microcontrolador do fabricante chinês *Espressif*, que inclui capacidade de comunicação por *Wi-Fi* e possui as seguintes características: • CPU 32-bit RISC: Tensilica Xtensa LX106 rodando a 80 MHz; • 64 KB de memória RAM de instruções, 96KB de dados; • Flash QSPI Externo – de 512 KB a 4 MB; • IEEE 802.11 b/g/n Wi-Fi; • 16 pinos de GPIO; SPI, I²C.
Cenário 2	Personal Computer Desktop	processador Intel Core i5 – 3330 CPU @ 3.00GHz, memória RAM de 8 GB e sistema operacional Windows 10 de 64 bits

Para o cálculo da vazão foi utilizada uma fórmula, que consiste da divisão do tempo base (1000 milissegundos), pelo período de execução do algoritmo, multiplicado pelo número de iterações necessárias para cada implementação, que é multiplicado pelo tamanho do texto em bits, conforme descrito na Eq. 1:

$$V = (1000/(p \times n)) \times m, \quad (1)$$

onde,

- V: vazão do algoritmo;
- p: período de execução do algoritmo;
- n: número de iterações necessária para a implementação;
- m: tamanho do texto em bits.

Para o microcontrolador *ESP8266*, também foi medido o gasto energético, em Microwatts, com o objetivo de se identificar o impacto da utilização da criptografia no consumo de energia em uma troca de informações entre dispositivos que compõem um sistema de **IoT**, como uma casa inteligente, por exemplo. Esse gasto resulta do cálculo da potência multiplicada pelo tempo de execução do algoritmo, onde tal potência resulta da multiplicação da tensão pela corrente, que são fornecidos pelo fabricante do microcontrolador. O cálculo do gasto energético é representado pela Eq. 2:

$$G = v \times i \times t, \quad (2)$$

onde,

- G: Gasto energético associado à execução do algoritmo;
- v: tensão consumida na placa;
- i: corrente consumida na placa;
- t: tempo de execução do algoritmo.

Foram implementados os seguintes algoritmos criptográficos: AES (128/128), Simon (32/64), Speck (32/64), Curupira1 (96/96) e Curupira2 (96/96), sendo a nomenclatura *x*/*y* dentro dos parêntesis significando: tamanho de bloco de *x* bits e comprimento de chaves de *y* bits.

Para as instâncias utilizadas na encriptação/decriptação, utilizou-se cinco tamanhos (bits) distintos de textos sendo categorizados em: pequeno porte (PP), médio porte (MP) e grande porte (GP). A base de dados para o *benchmark* constituiu-se de duas instâncias PP sendo uma de 384 bits e a outra de 786 bits; uma instância MP sendo de 9600 bits; e duas instâncias GP sendo uma de 15360 bits e a outra de 19200 bits.

O processo de encriptação/decriptação foi mensurado de acordo com as métricas apresentadas nos dois cenários descritos. A variação no tamanho das instâncias objetiva-se a representar situações de ocorrência de transmissão de informações em um cenário **IoT**. Os resultados obtidos com os testes são apresentados nos gráficos abaixo, inicialmente, são apresentados os resultados do Cenário 1 (Simulando **IoT**):

ISBN: 978-989-98434-9-3

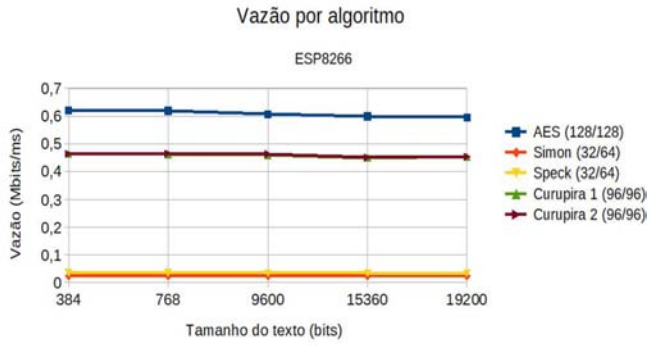

Figura 2. Comparação entre a vazão dos algortimos (Cenário 1)

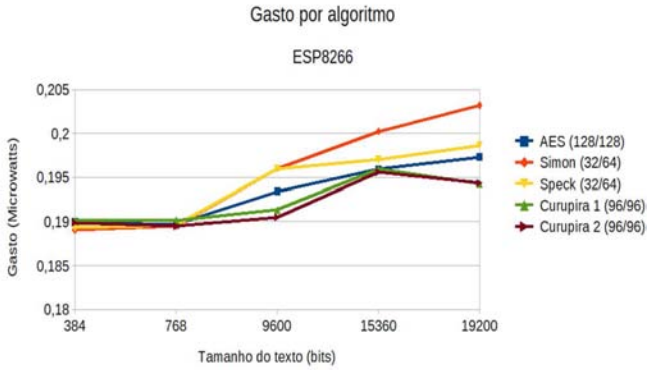

Figura 3. Comparação entre o gasto (microwatts) dos algoritmos (Cenário 1)

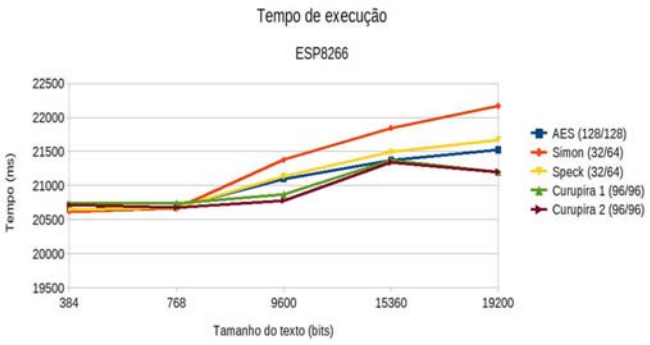

Figura 4. Tempo de execução dos algoritmos (Cenário 1)

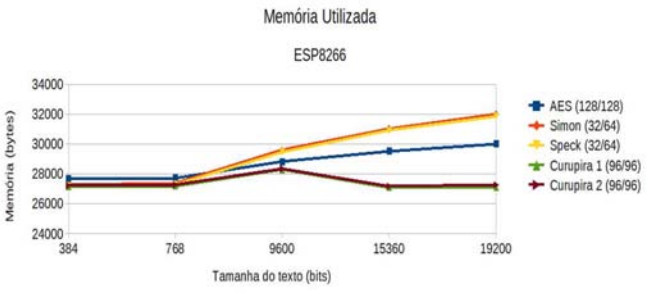

Figura 5. Memória utilizada pelos algoritmos (Cenário 1)

Percebe-se que, para as instâncias PP, o algoritmo Simon apresenta melhor desempenho em relação aos demais em quase todas as métricas. O algoritmo de Speck apresentou leve vantagem em relação ao consumo de memória e o AES apresentou a melhor vazão. Já para a instância de médio porte, de 9600 bits, o algoritmo mais rápido, com menor dispêndio energético e consumo de memória no ambiente da **IoT** (Cenário 1), foi o algoritmo Curupira2. Entretanto, em ambos os cenários o algoritmo de Simon apresentou a menor vazão.

Como pode ser observado nas figuras anteriores, o algoritmo AES foi o que apresentou maior vazão em todas as instâncias utilizadas, demonstrando sua eficiência na encriptação/decriptação em diferentes tamanhos de texto. De maneira oposta, o algoritmo Simon apresentou a menor vazão. Quanto ao consumo de energia despendido durante a execução dos algoritmos, as duas versões do Curupira, são as que produziram o menor gasto energético no microcontrolador, na maior parte das instâncias. Em se tratando de velocidade no ambiente de **IoT,** os algoritmos de Curupira, em ambas as versões, são os mais rápidos.

A seguir, são apresentados os resultados referentes ao Cenário 2:

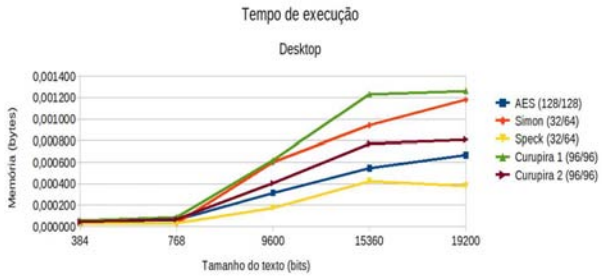

Figura 6. Tempo de execução dos algoritmos (Cenário 2)

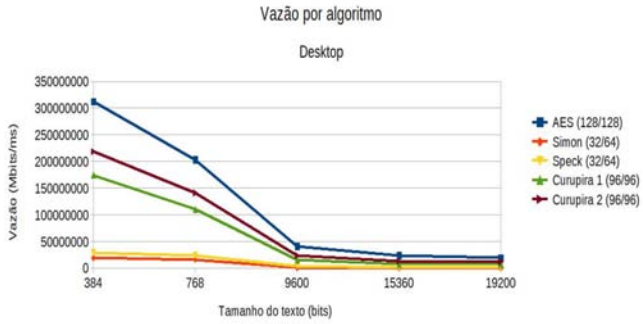

Figura 7. Comparação entre a vazão dos algoritmos (Cenário 2)

Para o Cenário 2, foram considerados o tempo de execução e a vazão dos algortimos, como mostrado nas Fig. 6 e Fig. 7, pois foram as métricas que apresentaram resultados mais relevantes. Assim, observa-se que, para as instâncias PP, os algortimos apresentaram resultados semelhantes em seu tempo de execução, com uma pequena vantagem para o Simon e para o Speck, sendo que, este cenário muda à medida em que se aumenta o tamanho do texto. Com relação a vazão, o processo

ISBN: 978-989-98434-9-3

se inverte, onde o AES se destaca, assim como no Cenário 1, mas, com o aumento do tamanho do texto, as vazões dos algoritmos apresentam resultados bem próximos, mas ainda com destaque para o AES.

Para as instâncias de grande porte na **IoT** (Cenário 1), os algoritmos Curupira apresentam os melhores desempenhos, exceto quanto à vazão, sendo o algoritmo de Simon com melhor performance. No Cenário 2 o algoritmo mais rápido é o algoritmo de Speck.

V. CONCLUSÕES

Neste trabalho foram propostos cinco algoritmos criptográficos de cifra leve destinados à utilização em ambiente **IoT**. O cenário desta tecnologia foi representado pelo microcontrolador *ESP8266* e o desempenho dos métodos basearam no tempo de execução, consumo energético e vazão. Constatou-se que os algoritmos de Curupira foram os mais econômicos em relação ao consumo de energia e mais rápidos no processo de encriptação/decriptação.

Como pode-se perceber nos resultados apresentados na seção anterior, o algoritmo AES apresentou a maior vazão, tendo maior capacidade de cifrar dados e informações computacionais. Além disso, apresentou também uma maior estabilidade em relação ao tempo de execução, a memória utilizada e o gasto, o que proporciona uma maior segurança pela criptografia aplicada, devido ao fato de que, mesmo sendo o algoritmo que possui o maior tamanho de bloco (128 bits) e a chave de maior tamanho (128 bits), pode se sobressair à outros algortimos que atuam em ambientes em que a capacidade de processamento do dispositivo que irá utilizá-lo seja reduzida.

Como trabalho futuro, pretende-se analisar em específico o algoritmo AES, devido ao seu desempenho, com o objetivo de se fortalecer a segurança na **IoT**, propondo estratégias criptográficas. Também é almejado a proposição de estratégias criptográficas hibridizadas para o cenário da **IoT**.

REFERÊNCIAS BIBLIOGRÁFICA

[1] D. Airehrour, J. Gutierrez, and S. K. Ray,"Secure Routing for Internet of Things: A Survey", Journal of Network and Computer Applications, vol. 66, pp. 198-213, **doi**: 10.1016/j.jnca.2016.03.006, May 2016.

[2] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", International Journal of Advanced Computer Science and Applications, vol. 8, **doi**: 10.14569/IJACSA.2017.080151, April 2017.

[3] H. Sou, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: a Review", In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on, vol. 3, pp. 648-651, **doi**: 10.1109/ICCSEE.2012.373, March 2012.

[4] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view", Internet Research, vol. 26, n. 2, pp. 337-359, **doi**: 10.1108/IntR-07-2014-0173, April 2016.

[5] LIVINGINTERNET, "John Romkey and Simon Hackett created the world's first connected device (other than a computer): a toaster powered through the Internet". Disponível em: http://www.livinginternet.com/i/ia_myths_toast.htm, Acesso em: 29 de janeiro de 2019.

[6] SOFTWARE.ORG, "Sensor Sensibility – Getting the Most from the Internet of Things". Disponível em: https://software.org/wp-content/uploads/iot-sensor-sensibility.pdf, Acesso: 29 de janeiro de 2019.

[7] S. Ranger, "What is the IoT? Everything you need to know about the Internet of Things right now". Disponível em: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/, Acesso: 29 de janeiro de 2019.

[8] L. Columbus, "86% Of Enterprises Increasing IoT Spending In 2019". Disponível em: https://www.forbes.com/sites/louiscolumbus/2018/11/23/86-of-enterprises-increasing-iot-spending-in-2019/#3f6c7808384d, Acesso: 29 de janeiro de 2019.

[9] ZEBRA, "The Intelligent Enterprise Index". Disponível em: https://www.zebra.com/content/dam/zebra_new_ia/en-us/campaigns/brand-campaign/harvard-symposium/how-intelligent-enterprise-survey-index-en-us.pdf, Acesso em: 29 de janeiro de 2019.

[10] A. Shah, and M. Engineer, "A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications", In Tiwari S., Trivedi M., Mishra K., Misra A., Kumar K. (eds) Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing, vol 851, Springer, Singapore, **doi**: 10.1007/978-981-13-2414-7_27, January 2019.

[11] I. S. Masoode, B. Javid, "A Review of Cryptographic Algorithms for the Internet of Things", In Cryptographic Security Solutions for the Internet of Things. IGI Global, pp. 67-93, **doi**: 10.4018/978-1-5225-5742-5.ch003, 2019.

[12] A. Shifa, M. Asghar, and M. Fleury, "Efficient Lightweight Encryption Algorithm for Smart Video Applications", In Conference: 2018 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, **arxiv**: 1901.08344v1, January 2019.

[13] V. G. K. Kumar, C. S. Shantharama, "Implementation and Analysis of Cryptographic Ciphers in FPGA", In Emerging Technologies in Data Mining and Information Security. Springer, Singapore, pp. 653-666, **doi**: 10.1007/978-981-13-1951-8_59, December 2019.

[14] P. K. Singh et al., "Elliptic Curve Cryptography Based Mechanism for Secure Wi-Fi Connectivity", In International Conference on Distributed Computing and Internet Technology. Springer, Cham, pp. 422-439, **doi**: 10.1007/978-3-030-05366-6_35, January 2019.

[15] G. C. C. F. Pereira et al., "Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems", Security and Communication Networks, vol. 2017, pp. 1-16, **doi**: 10.1155/2017/2046735, August 2017.

[16] N. Alassaf, A. Gutub, S. A. Parah, and M. A. Ghamdi, "Enhancing speed of SIMON: A lightweight-cryptographic algorithm for IoT applications", Multimedia Tools and Applications, pp. 1-25, **doi**: 10.1007/s11042-018-6801-z, November 2018.

[17] R. Nithya, D. S. Kumar, "Where AES is for Internet, Simon could be for IoT", Procedia Technology, vol. 25, pp. 302-309, **doi**: 10.1016/j.protcy.2016.08.111, December 2016.

[18] D. H. Bui, D. Puschini, S. B. Min, and E. Beigné, "Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications", In 2016 International Conference on IC Design and Technology (ICICDT). IEEE, pp. 1-4, **doi**: 10.1109/ICICDT.2016.7542076, August 2016.

[19] L. Armasu, "NSA-Designed Speck Algorithm to Be Removed From Linux 4.20". Disponível em: https://www.tomshardware.co.uk/nsa-speck-removed-linux-4-20,news-59110.html, Acesso em: 30 de janeiro de 2019.

[20] N. F. Standard, "Announcing the advanced encryption standard (AES)", Federal Information Processing Standards Publication, vol. 197, pp. 1-51, 2001.

[21] R. Beaulieu, D. Shors, J. Smith, S. T. Clark, B. Weeks, and L. Wingers, "The Simon and Speck Families of Lightweight Block Ciphers", Cryptology ePrint Archive, Report 2013/2014, June 2013.

[22] R. Beaulieu, D. Shors, J. Smith, S. T. Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Block Ciphers on AVR 8-bit Microcontrollers", Cryptology ePrint Archive, Report 2014/947, November 2014.

[23] P. S. L. M. Barreto, and M. A. Simplício, "Curupira, a block cipher for constrained platforms", In 25th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC), vol. 2017, pp. 61-74, 2017.

ISBN: 978-989-98434-9-3