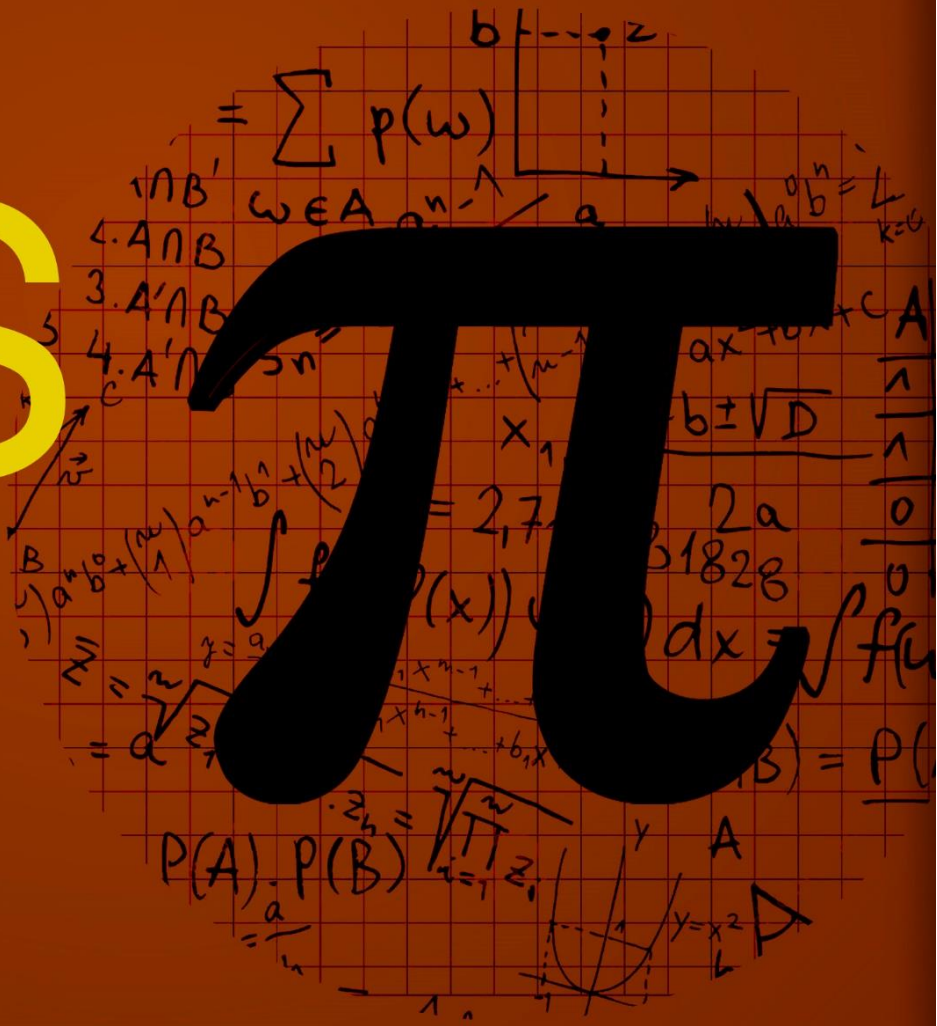
Journal of Exact Sciences

FEITEP
FACULDADE DE ENGENHARIAS

Online ISSN 2358-0348

JES



14(1)

Julho / Setembro
July / September

2017

MASTER EDITORA
Publicações Científicas

Online ISSN 2358-0348

JES Ficha Técnica Technical Specification

Título / *Title:* Journal of Exact Sciences
Título abreviado/ *Short title:* J. Ex. Sci.
Sigla/ *Acronym:* JES
Editora / *Publisher:* Master Editora
Periodicidade / *Periodicity:* Trimestral / Quarterly
Indexação / *Indexed:* Latindex, Google Acadêmico
Início / *Start:* Abril, 2014/ April, 2014

O periódico **Journal of Exact Sciences – JES** é uma publicação da **Master Editora** para divulgação de artigos científicos apenas em mídia eletrônica, indexada à base de dados **Latindex** e **Google Escolar.** Todos os artigos publicados foram formalmente autorizados por seus autores e são de sua exclusiva responsabilidade. As opiniões emitidas pelos autores dos artigos publicados não correspondem necessariamente, às opiniões da Master Editora, do periódico **JES** e/ou de seu conselho editorial.

*The **Journal of Exact Sciences - JES** is an editorial product of **Master Publisher** aimed at disseminating scientific articles only in electronic media, indexed in **Latindex** and **Google Scholar** databases.*
All articles published were formally authorized by the authors and are your sole responsibility.
*The opinions expressed by the authors of the published articles do not necessarily correspond to the opinions of Master Publisher, the **JES** and/or its editorial board.*

Master Editora
Publicações Científicas

Online ISSN 2358-0348

JES Editorial

Prezado leitor,

Temos a imensa satisfação de lançar a décima quarta edição do ***Journal of Exact Sciences - JES***

A ***Master Editora*** *e o periódico* ***JES*** *agradecem publicamente aos Autores dos artigos que abrilhantam esta sexta edição pela colaboração e pela confiança depositada neste projeto. O periódico* ***JES*** *é um dos primeiros "open access journal" do Brasil, representando a materialização dos elevados ideais da* ***Master Editora*** *acerca da divulgação ampla e irrestrita do conhecimento científico produzido pelas diversas áreas das Ciências Exatas.*

Aos autores de artigos científicos que se enquadram em nosso escopo, envie seus manuscritos para análise de nosso conselho editorial!

Nossa décima quinta edição estará disponível a partir do mês de outubro de 2017!

Boa leitura!

Mário dos Anjos Neto Filho
Editor-Chefe JES

Dear reader,

We have the great pleasure to launch the Fourteenth Edition of the ***Journal of Exact Sciences - JES.***

The ***Master Publisher*** *and the* ***JES*** *are very grateful to the authors of the articles that brighten this third edition by the trust placed in this project. The* ***JES*** *is one of the early open access journal in Brazil, representing the materialization of the lofty ideals of* ***Master Publisher*** *about the broad and unrestricted dissemination of scientific knowledge produced by the Exact Sciences.*

Authors of scientific articles that are interested in the scope of ***JES****, send their manuscripts for consideration of our editorial board!*

Our Fifteenth edition will be available in October, 2017!

Happy reading!

Mário dos Anjos Neto Filho
Editor-in-Chief JES

Master Editora
Publicações Científicas

Online ISSN 2358-0348

JES Sumário summary

CRIPTOGRAFIA APLICADA À SEGURANÇA DA INTERNET DAS COISAS

CRYPTOGRAPHY APPLIED TO THE SECURITY OF INTERNET OF THINGS

GABRIEL **KRÜGER**[1*], SIMONE VIEIRA **PEREIRA**[2], VINÍCIUS VAULEI GONÇALVES **MARIUCCI**[3], GILBERTO APARECIDO **TENANI**[4], AFONSO GENTA **PALANDRI**[5]

1. Acadêmico do curso de graduação em Engenharia Elétrica – FEITEP; **2.** Mestre em Informática (UFPR), e docente do curso de Engenharia Elétrica e Computação – FEITEP; **3.** Doutor em Física (UEM), docente do curso de Engenharia Elétrica e coordenador de Pesquisa e Extensão – FEITEP; **4.** Mestre em Matemática (UEM), e docente efetivo de ensino básico, técnico e tecnológico – IFMS; **5.** Especialista em Engenharia de Segurança no Trabalho (UEM), e docente do curso de Engenharia Elétrica – FEITEP.

* Rua Professor Valter Biazin, 36, Maringá, Paraná, Brasil. CEP: 87043-616. grk.82.gabriel@gmail.com

Recebido em 04/09/2017. **Aceito** para publicação em 12/09/2017

RESUMO

O presente artigo visa expor de maneira geral o que é a Internet das Coisas e também o que é Criptografia de forma que os dois conceitos possam ser correlacionados afim de solucionar um dos principais problemas que se tem na atualidade quando se fala não apenas de Internet das Coisas, mas do mundo digital como um todo, a segurança da informação. Tendo a segurança dos objetos conectados em mente, é apresentado um modelo de Criptografia Simétrica Clássica, objetivando a sua aplicação em uma plataforma de IoT (Internet of Things). Para o desenvolvimento do projeto, utilizou-se a linguagem de programação Python com o ambiente PyCharm, juntamente com as bibliotecas Numpy e Math. Os resultados obtidos foram satisfatórios, pois o algoritmo se manteve estável em grande parte dos testes realizados. É possível concluir que a segurança é um fator primordial para qualquer objeto conectado à internet e que a aplicação da Criptografia em plataformas inteligentes é indispensável para que a privacidade, integridade e segurança do usuário sejam preservados.

PALAVRAS-CHAVE: Internet das coisas, criptografia, segurança cibernética, privacidade, IoT.

ABSTRACT

The present article aims to expose in a general way what is the Internet of Things and also what is Cryptography so that the two concepts can be correlated in order to solve one of the main problems that one has at the present time when speaking not only of Internet of the Things, but the digital world as a whole, information security. Having the security of the connected objects in mind, a Classic Symmetric Encryption model is presented, aiming its application in an IoT platform. For the development of the project, the Python programming language was used with the PyCharm environment, along with the Numpy and Math libraries. The results were satisfactory, because the algorithm remained stable in most of the tests performed. It is possible to conclude that security is a key factor for any object connected to the Internet and that the application of cryptography in smart platforms is essential for privacy, integrity and user safety are preserved.

KEYWORDS: Internet of things, cryptography, cybersecurity, privacy, IoT.

1. INTRODUÇÃO

Com a constante evolução tecnológica e a internet cada vez mais presente no cotidiano pessoal e profissional das pessoas, estar conectado tem se tornado uma necessidade. Baseado nisso, fica evidente a utilidade da internet para tornar tarefas cotidianas mais fáceis, simples e autônomas. Visto que estamos expostos a milhares de informações todos os dias, deve existir algum meio de coletar tais informações que estão ao nosso redor, processá-las e realizar alguma tarefa ou ação a partir delas. Dessa forma atribuiu-se um nome a essa facilidade, Internet das Coisas.

Internet das Coisas

Segundo Pires, o termo Internet das Coisas (IoT, do inglês “Internet Of Things”) surgiu por volta de 1999 em uma apresentação ministrada por Kevin Ashton na Procter & Gamble (P&G). Desde então o conceito de IoT vem sido descrito de uma maneira mais genérica como a Internet de Tudo, a Internet que tudo se conecta dos mais irrisórios objetos (para alguns) até os mais complexos objetos mais substanciais da tecnologia atual. Dentre eles, sensores, atuadores, dispositivos inteligentes, *smartphones*, eletrodomésticos, carros, móveis, *wearables* (dispositivos vestíveis), entre uma infinidade de “coisas” ao

nosso redor com potencialidade para serem conectados à rede. Dentre suas principais características, destacam-se a sua ubiquidade e dinamismo, ou seja, a possibilidade de estar concomitantemente em vários lugares. Com essa característica a IoT se torna um princípio intangível e volúvel, diante da possibilidade de interação com diferentes objetos de forma autônoma através da internet, podendo ser uma interação com um objeto inanimado ou um ser humano[1]. Basicamente a IoT é a integração de objetos físicos e virtuais em rede conectados à internet, essas "coisas" tem o objetivo de coletar, trocar e armazenar informações de dados, em que serão processados e analisados para tomar decisões e ações executando serviços em uma escala proporcionalmente grande e em tempo real. A IoT gera impacto em todas as áreas mundiais, como econômica, educacional, política, social, industrial, eletrônica de consumo, saúde, segurança, e a forma como a sociedade consome informação. Estima-se que até 2020 serão 50 bilhões de dispositivos conectados[2] pelo mundo. O mercado de computação em nuvem deve alcançar mais de 120 bilhões de dólares em 2018[2], o que se torna perceptível ao se pensar em 44 zettabytes (trilhões de gigabytes) de tráfego de dados diariamente no mundo em 2020[2]. A informação estará presente em qualquer ambiente, em qualquer situação, a qualquer momento, de forma integrada a atividades corriqueiras. Por outro lado segurança e privacidade, são questões que passam a ser vistas com mais rigor, atenção e preocupação, ao passo que objetos inteligentes se tornam onipresentes, conectados, acessíveis, observados. A segurança passa a ser um princípio vital para a evolução da IoT.

Até o desenvolvimento "maduro" na tecnologia da IoT, é preciso se atentar à segurança dos objetos que serão ou são conectados à internet, pois tais dispositivos têm o poder de transmitir as informações armazenadas sobre seus usuários, como hábitos, locais, horários de rotinas, entre outras informações circunstanciais e sensíveis ao usuário. Por mais que os desenvolvedores se atentem à segurança, ainda se pode perceber alguns descasos que passam despercebidos. Aplicações de engenharia reversa se tornam práticas altamente relevantes quanto ao teste de integridade e segurança do próprio produto de um determinado desenvolvedor. Estudos recentes têm focado em comunicação segura no nível de redes digitais das coisas e enfatizando a proteção de ataques de negação de serviço. Também se faz necessário abordar aplicações de segurança específicas como garantir que um objeto só possua acesso por outro objeto ou pessoa mediante a autorização prévia e controle total por seus legítimos responsáveis. Um objeto conectado deve ser capaz de detectar ataques contra si e se isolar de outros objetos (podendo se desconectar), para que se mantenha a integridade do sistema e as informações sejam inacessíveis[3]. Mas como proteger o futuro da IoT, as *Smart Things, Smart Home, Smart Cities, Smart World?* Uma opção seria o uso de Criptografia aplicada na segurança da IoT, ainda que sendo uma área com vastas aplicações de segurança de redes e computadores, porém rudimentar quanto a aplicação a IoT.

Criptografia

Pode-se definir Criptografia do grego *kryptós*, "escondido", e *gráphein*, "escrita", ou seja, "Escrita Escondida". Essa escrita escondida tem como objetivo impossibilitar a legibilidade da mensagem para terceiros que não deveriam ter acesso a ela, isto é, a Criptografia não impossibilita a captura ou interceptação da mensagem, mas sim o seu entendimento. Não existe algo ou alguém a que é possível atribuir o conceito de Criptografia propriamente dito, porém existem relatos históricos de povos antigos que dizem respeito a utilização de técnicas de ocultamento ou formas de manter o sigilo de mensagens que necessitavam de segurança e privacidade. Posteriormente, surgiram técnicas de utilização da Criptografia mais elaborados como o método dos egípcios e romanos que se utilizavam de alguns procedimentos de ocultação de mensagens, principalmente para comunicar planos de batalha para soldados em guerra (a Cifra de César é um exemplo)[4]. Em 1918 Arthur Scherbius havia patenteado e criado a Enigma, uma máquina de Criptografia baseada em rotores que entre 1933 e 1945 foi aprimorada e utilizada como "arma" militar se tornando a mais importante ferramenta da Alemanha Nazista na Segunda Guerra Mundial[4]. A partir daí a história e o desenvolvimento da Criptografia vem ganhando proporções significativas.

Com a invenção do computador a Criptologia (estudo que reúne conhecimentos na área de Criptoanálise e Criptografia) teve suas implementações mais acessíveis e facilitadas, possibilitando a criação de algoritmos criptográficos de diversos tipos, dentre eles algoritmos simétricos (chave única, privada) e assimétricos (duas chaves, privada e pública). Basicamente a Criptografia nada mais é do que impossibilitar o acesso de pessoas mal-intencionadas a informação transmitida por um dado meio de comunicação (internet, por exemplo), mesmo que a mensagem seja interceptada, não seria possível lê-la a menos que a pessoa tivesse a posse da chave de decriptação da mensagem. Com o avanço da tecnologia, desde a Criptografia Clássica até a Criptografia Moderna pode-se perceber a sua consolidação em nosso cotidiano passando até despercebido por alguns. Alguns exemplos de sua utilização são e-mails, sites de compra online, servidores, *Cloud Computing, Apps* para comunicação como *Whatsapp, Telegram* e *Signal, Apps* para bancos utilizados em desktop e agora de forma mais acessível e em qualquer lugar utilizada em *Smartphones* que se utiliza de Autenticação e Assinatura Digital, ambos conceitos modernos da Criptografia. Pode-se notar a necessidade e a indispensável utilização da Criptografia na era Digital atual, e cada vez mais avanços em sua utilização

como *Smartphones* com leitor biométrico, outros dispositivos com leitor de retina, funções de *Hash*, segurança de IP e redes *Wireless*, criação de protocolos e certificações e *Firewalls* cada vez mais sofisticados[5].

Por conseguinte, o presente projeto tem como objetivo analisar a IoT e a Criptografia e integrar os dois conceitos de alguma forma plausível para tentar resolver problemas e questionamentos atuais que impedem ou retardam o desenvolvimento da IoT e sua segurança. Visto que a análise e correlação dos fatores é de âmbito descritivo e teórico serão exploradas possibilidades de integração dos dois elementos de forma hipotética, partindo do pressuposto de que nem sempre serão obtidas respostas exatas e completas para a solução de todos os questionamentos e desígnios.

2. MATERIAL E MÉTODOS

A pesquisa envolveu o método qualitativo, no intuito de comparar e partir de abordagens quantitativas para a melhor compreensão do método de pesquisa utilizado para apresentar o pré-projeto, pela análise minuciosa e comparativa de pequenas amostras dos fatos e das variáveis de pesquisa. O tipo de pesquisa utilizado será a pesquisa descritiva que visa análises, observações e registros de fatos e fenômenos correlacionando-os, porém, não interferindo ou controlando as variáveis do objeto estudado. O objetivo principal da pesquisa descritiva é o de estudar, levantar informações sobre um tema específico e desta forma auxiliar na formulação do problema de pesquisa[6].

A partir de várias pesquisas e estudos, pode-se perceber diversos algoritmos ou técnicas de Criptografia que já foram ou ainda são utilizados com o objetivo de ocultar mensagens ou dados que contenham informações sigilosas ou de âmbito privativo ao indivíduo. Conforme Stallings, algumas dessas técnicas são apresentadas a seguir[7].

Técnicas Clássicas de Criptografia

Em meio as técnicas de Criptografia Clássica existem dois métodos abordados que são o método de substituição e o método de transposição. A seguir são destacados alguns dos principais métodos seguidos de suas cifras.

A primeira técnica e provavelmente a mais popular é a Cifra de César. A Cifra de César detém como técnica o método de substituição. Na prática, a sua utilização original consistia no deslocamento alfabético a partir de uma chave K com o intervalo do tamanho do alfabeto (de 0 a 25 posições, monoalfabético). Matematicamente:

$$C = E(k,p) = (p + k)\ mod\ 26 \quad (1)$$

Onde,

C = texto criptografado;
E = função de encriptação da mensagem;
K = chave de deslocamento alfabético;
P = texto claro ou texto plano inteiro ou particionado;
mod = operador que obtém o resto de uma divisão.

Pode-se descrever o método de decriptação da mensagem de César matematicamente por:

$$p = D(k,C) = (C - k)\ mod\ 26 \quad (2)$$

Onde D é a função de decriptação da mensagem.

Atualmente, a utilização da Cifra de César não é viável. Algumas das vulnerabilidades que o algoritmo possui é não ter um método que oculte a frequência das letras no texto, tanto claro quando codificado, bem como, a sua permutação permite apenas 26 possibilidades de chave, tornando o método de criptoanálise (estudo de decodificação de criptogramas) ou quebra de código por força bruta (operação feita por computador que verifica todas as chaves possíveis para tentar decodificar a mensagem) muito simples e rápida.

A segunda técnica é a Cifra de Hill. Essa cifra se baseia em princípios da álgebra linear como método de encriptação e decriptação. O seu funcionamento consiste na utilização de *m* letras de texto claro sucessivas substituindo-as por *m* letras do texto cifrado. A substituição é determinada por *m* equações lineares, em que cada caractere recebe um valor numérico correspondente a sua posição alfabética (a = 0, b = 1, ..., z = 25). Supondo *m* = 3, o sistema pode ser descrito matematicamente da seguinte forma:

$$c1 = (k11p1 + k21p2 + k31p3)\ mod 26 \quad (3)$$
$$c2 = (k12p1 + k22p2 + k32p3)\ mod 26 \quad (4)$$
$$c3 = (k13p1 + k23p2 + k33p3)\ mod 26 \quad (5)$$

Esse sistema pode ser impresso em termos de vetores de linhas e matrizes:

$$(c1\ c2\ c3) = (p1\ p2\ p3)\begin{pmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{pmatrix} mod 26 \quad (6)$$

Ou

$$C = PK\ mod\ 26 \quad (7)$$

Com C e P sendo vetores de coluna de tamanho 3, em que K é uma matriz 3 x 3 correspondente a chave para encriptação. De modo geral a Cifra de Hill pode ser expressa matematicamente por:

$$C = E(K,P) = PK\ mod\ 26 \quad (8)$$

Onde,

C = texto criptografado;
E = função de encriptação da mensagem;

K = uma matriz de chave correspondente as atribuições alfabéticas de deslocamento;
P = pares de texto claro ou texto cifrado;
mod = operador que obtém o resto de uma divisão.

Para decriptação da mensagem de Hill, podemos descrever seu algoritmo da seguinte forma:

$$P = D(K, C) = CK^{-1} \, mod \, 26 = PKK^{-1} = P \quad (9)$$

Em que,

D = função de decriptação da mensagem;
K^{-1} = inversa da matriz original de chaves K.

A Cifra de Hill em contraste com a Cifra de César, se mostra bem eficiente contra vulnerabilidades de frequência de única letra, ou seja, a Cifra de Hill permite ocultar completamente as frequências de única letra e quanto maior a matriz, mais letras serão ocultadas de suas frequências. Entretanto, essa cifra é quebrada facilmente com um ataque de texto claro conhecido.

A terceira técnica é a Cifra de Vigenère. A Cifra de Vigenère é uma das mais populares e simples cifra polialfabética. Essa técnica consiste na utilização de 26 cifras de César para a encriptação e decriptação das mensagens. Basicamente seu funcionamento consiste em encriptar cada caractere do texto claro com uma Cifra de César diferente, dependendo do caractere de chave correspondente, essa chave deve ser exatamente de tamanho igual ao do texto claro. A equação geral que define a encriptação pode ser obtida da seguinte maneira:

$$C_i = (p_i + k_{i \, mod \, m}) \, mod \, 26 \quad (10)$$

Onde,

C_i = texto criptografado na posição *i* de cada Cifra de César correspondente;
P_i = texto claro para cada posição *i* de cada Cifra de César correspondente;
$K_{i \, mod \, m}$ = chave aplicada a cada posição *i* resto de *m* letras correspondente de cada Cifra de César;
mod = operador que obtém o resto de uma divisão.

Para decriptação da mensagem de Vigenère podemos denotar os termos:

$$p_i = (C_i - k_{i \, mod \, m}) \, mod \, 26 \quad (11)$$

A vantagem da Cifra de Vigenère também é a sua desvantagem. Para cada letra do texto claro, existem múltiplas letras de texto cifrado, ou seja, uma para cada letra exclusiva da palavra-chave. Dessa forma a Cifra de Vigenère consegue minimizar muito bem os fatores referentes à frequência das letras, porém quanto maior o texto cifrado, maiores são as chances de se ocasionar convergências quanto ao uso repetido das chaves.

A quarta técnica é a Cifra de Vernam. A Cifra de Vernam é uma cifra polialfabética de substituição e foi criada em 1918 por Gilbert Vernam. Sua ideia foi propor uma palavra-chave tão longa quanto o texto claro de forma que não exista nenhuma forma de relacionamento estatístico com ele. Seu funcionamento consiste sobre dados binários (bits), ao invés de letras, dessa forma o texto cifrado é gerado a partir de uma operação lógica XOR (ou-exclusivo) bit a bit entre texto claro e a chave. Seu algoritmo pode ser descrito da seguinte forma:

$$c_i = p_i \oplus k_i \quad (12)$$

Onde,

C_i = dígito binário na posição *i* do texto cifrado;
P_i = dígito binário na posição *i* do texto claro;
K_i = dígito binário na posição *i* da chave;
$\oplus$ = operação lógica ou-exclusivo (XOR).

Para decriptação da mensagem de Vernam, por motivos obtidos nas propriedades da operação lógica XOR é usada a mesma forma de comparação bit a bit:

$$p_i = c_i \oplus k_i \quad (13)$$

A Cifra de Vernam propõe um grande desafio para métodos de Criptoanálise, porém levando em conta o tamanho da palavra-chave adotada, usualmente ocasionaria diversas repetições no texto cifrado.

A quinta e última cifra abordada no presente artigo que utiliza o método de substituição é a Cifra One Time Pad. A Cifra de One Time Pad foi criada por um oficial do exército chamado Joseph Mauborgne[7]. Ele propôs uma melhoria a partir da Cifra de Vernam de forma que a chave fosse aplicada de forma aleatória e que fosse tão grande quanto o texto claro, de maneira que a chave não fosse repetida. Além disso, uma única chave deveria ser usada para encriptação e decriptação de uma única mensagem e depois descartada. Para cada novo texto claro de entrada deveria ser produzido uma nova chave aleatória de tamanho igual à mensagem. Sendo assim, o One Time Pad é conhecido por ser inquebrável porque não produz nenhuma relação estatística com a saída criptografada. Se a chave for verdadeiramente aleatória, o texto cifrado será gerado de forma verdadeiramente aleatória, dessa forma não existe padrões para decodificar o código, sendo assim, não existe um meio de quebrá-lo. Em teoria essa cifra seria um método perfeito de segurança, todavia existem duas objeções que se opõe contra a Cifra One Time Pad. São elas:

1. Para se obter chaves aleatórias a partir do tamanho dos textos claros é necessária uma quantidade de processamento significativa, tendo em vista que para cada texto claro, independentemente do tamanho, deveria ser gerada uma nova chave aleatória diferente de tamanho igual ao da mensagem, o que se torna inviável.
2. Para cada texto criptografado, é necessário que o emissor e o receptor utilizem a mesma chave gerada

para fazer o processo inverso, logo ocasionaria um problema relativamente absurdo em relação a distribuição segura das chaves.

Partindo para técnicas de transposição, o exposto artigo irá apresentar apenas uma, que é a técnica de Cerca de Trilho (ou *Rail Fence*, em inglês). Essencialmente essa técnica se detém de um método de permutação nas letras do texto claro, que consiste basicamente em trocar o posicionamento das letras em uma determinada mensagem. Existem diversas aplicações para se utilizar esse método, uma delas é dispor o texto claro em uma matriz e enumerar as suas colunas. Com base na ordem das colunas, pode-se dispor cada coluna como uma linha seguida da sua próxima ordem, assim obtemos o texto cifrado. Por exemplo,
Texto claro: ataque adiado até as duas da manhã.

4	3	1	2	5	6	7
A	T	A	Q	U	E	A
D	I	A	D	O	A	T
E	A	S	D	U	A	S
D	A	M	A	N	H	A
B	O	A	N	O	I	T
E	W	X	Y	Z	A	B

Chave:
Texto claro:

Texto cifrado:
AASMAXQDDANYTIAAOWADEDBEUOUNO-ZEAAHIAATSATB.

No exemplo acima é visto que a matriz deve ser totalmente preenchida, mesmo que não seja com a mensagem. Por esse motivo, foram colocadas as letras "WXYZAB". Os números de cada coluna são selecionados aleatoriamente e correspondem à chave. Para se obter a mensagem cifrada, as colunas são dispostas em ordem crescente conforme as chaves e em linha. A cifra de transposição pode se tornar muito mais segura realizando mais de um estágio de transposição utilizando o mesmo algoritmo, o que gera um resultado bem menos estruturado com ocultação de frequência de letras ocasionando em uma difícil quebra do código. Entretanto, a decriptação da mensagem por esse método se torna um tanto quanto inviável, pois fica difícil saber qual a ordem das colunas e se torna impossível correlacioná-las caso seja uma mensagem muito longa.

Com a ideia proposta anteriormente de que a segurança de um algoritmo pode ser relativamente aumentada a partir da segmentação de várias etapas de encriptação surgem a partir daí as Máquinas de Rotor. Essas máquinas consistem basicamente de cilindros rotativos independentes. Por meio dos mesmos, pulsos elétricos são conduzidos através de conexões por fios internos em cada pino de entrada, correspondendo a um pino de saída. Cada cilindro tem 26 pinos de entrada e 26 pinos de saída. Associando ao alfabeto, obtem-se uma letra para cada pino. Após o pressionamento de cada tecla contida no cilindro, este gira uma posição, fazendo com que as conexões internas sejam deslocadas de acordo. Sendo assim, se define uma cifra de substituição monoalfabético diferente. Após as 26 letras do texto claro serem pressionadas, o cilindro volta à posição inicial, formando um único cilindro em uma cifra de substituição polialfabética com um período de 26. A grande ideia das Máquinas de Rotor é acoplar outros rotores de forma que a saída do primeiro seja a entrada do segundo e assim por diante. Sendo assim, em uma máquina com 3 rotores por exemplo, haveriam $26^3 = 17.576$ alfabetos de substituição diferentes, utilizáveis antes que esse sistema se repita, acrescentando o quarto e o quinto rotor obtém-se resultados de períodos de 456.976 e 11.881.376 letras, respectivamente. Assim, uma máquina com 5 rotores seria o equivalente a uma cifra de Vigenère com um tamanho de chave de 11.881.376[7].

Técnicas Modernas de Criptografia

Uma das primeiras técnicas modernas que foi utilizada durante muito tempo foi o *Data Encryption Standard* (DES). O DES foi adotado em 1977 e se manteve seguro até 2001[7]. Nessa técnica os dados são encriptados em blocos de 64 bits que utilizam uma chave de 56 bits. Esse algoritmo realiza uma série de operações e etapas a partir da entrada de 64 bits para gerar uma saída de 64 bits idênticos. As mesmas operações e a mesma chave são utilizadas para realizar o processo de decriptação. Para uma chave de 56 bits o DES possui um número de chaves alternativas igual a $2^{56} \approx 7{,}2 \times 10^{16}$. Utilizando a técnica de força bruta que testa todas as chaves possíveis de decriptação, com um tempo exigido de 10^{13} decriptações por segundo o DES seria quebrado em 1 hora (lembrando que é um alto nível de processamento). O Triple DES que consiste basicamente em aplicar o algoritmo DES 3 vezes (aumentando seu nível de segurança) ao mesmo texto com 3 chaves diferentes gerando um tamanho de chave de 168 bits possui um número de chaves alternativas igual a $2^{168} \approx 3{,}7 \times 10^{50}$. No mesmo tempo exigido de 10^{13} decriptações por segundo, corresponde a $5{,}8 \times 10^{29}$ anos para ser quebrado. A partir desse algoritmo, se instituiu o conceito de Criptografia Simétrica e/ou Criptografia de Chave Privada, que consiste em um modelo de algoritmo criptográfico que se utiliza a mesma chave tanto para codificar quanto para decodificar a mensagem[7].

Na atualidade, o DES e o Triple DES não são mais utilizados e em 2001 surgiu um substituto para a criptografia simétrica, sendo utilizado até os dias atuais, o AES (*Advanced Encryption Standard*), o qual foi a segunda técnica abordada neste trabalho[7]. Esse algoritmo é

basicamente uma melhoria alarmante para as técnicas de criptografia simétrica. Nesta técnica, o algoritmo recebe como entrada um único bloco de texto com tamanho de 128 bits ou 16 bytes e o tamanho da chave varia em 128/192/256 bits, por isso a denominação AES-128, AES-192 e AES-256, correspondendo ao tamanho da chave[7]. Esse bloco é indicado como uma matriz quadrada de bytes 4 × 4 e copiado para um *array* estado que é modificado a cada etapa de encriptação/decriptação. Após a última etapa do processo, o *array* estado é copiado para uma matriz de saída. A chave também é apresentada como uma matriz de bytes, essa chave se expande para um conjunto de palavras chave durante o processo. Cada palavra tem 4 bytes, e o conjunto total é de 44 palavras, para a chave de 128 bits. A cifra consiste basicamente de *N* rodadas que dependem do tamanho da chave, então: são 10 rodadas para uma chave de 128 bits, 12 para 192 bits e 14 para 256 bits. Para uma chave de 128 bits o AES possui um número alternativo de chaves igual a $2^{128} \approx 3{,}4 \times 10^{38}$. Levando em consideração as mesmas condições impostas ao DES, isto é, um tempo exigido de 10^{13} decriptações por segundo, o tempo para se quebrar o algoritmo é de $5{,}3 \times 10^{17}$ anos. Já com uma chave de 192 bits, o AES possui um número alternativo de chaves igual a $2^{192} \approx 6{,}3 \times 10^{57}$. Para ser quebrado, levaria um tempo aproximado de $9{,}8 \times 10^{36}$ anos. E com uma chave de 256 bits, o AES possui $2^{256} \approx 1{,}2 \times 10^{77}$ possíveis alternativas de chave e para ser quebrado levaria aproximadamente $1{,}8 \times 10^{56}$ anos[7]. Essa foi uma descrição geral do algoritmo e a descrição do funcionamento detalhado das operações e transformações contidas no algoritmo AES estão além do escopo desse artigo.

Conforme o avanço em estudos e tecnologia ainda na década de 80, surgiu uma nova técnica de Criptografia, a Criptografia de Chave Pública e/ou Criptografia Assimétrica, que consiste na utilização de duas chaves, uma para encriptação e outra para a decriptação. Esse tipo de técnica é baseado em funções matemáticas complexas (teoria dos números e fatoração de números primos são alguns exemplos) que vão além de substituições e permutações apenas[7]. Esse conceito surgiu a partir da necessidade de solucionar dois problemas relacionados à Criptografia Simétrica. O primeiro é a distribuição de chaves e o segundo é a assinatura digital. Para exemplificar, na Criptografia de Chave Privada existe apenas uma chave para encriptar e decriptar a mensagem, sendo assim o emissor da mensagem precisa compartilhar a mesma com o receptor da mensagem, então nesse momento é gerado uma vulnerabilidade, que é a distribuição de forma segura das chaves. Quanto à assinatura digital, na Criptografia Simétrica é possível apenas autenticar a mensagem, ou seja, é possível verificar a integridade dos dados. Dessa forma se houver uma interceptação no seu envio e alteração, será perceptível quando a mensagem chegar ao receptor. Porém, os autores da técnica de Chave Pública viram a necessidade de formular um método que comprovasse que determinado arquivo foi assinado por determinada pessoa, empresa ou entidade. A geração das duas chaves é feita a partir de algoritmos matemáticos e então são obtidos uma chave privada que é utilizada para a decriptação da mensagem e uma chave pública que é utilizada para encriptação da mensagem. Dessa forma, se A quer enviar uma mensagem encriptada para B, então A precisa utilizar a chave pública de B que estará disponível a todos, encriptar a mensagem e enviar para B. Então B irá usar sua chave privada que foi gerada juntamente com a chave pública para decriptar a mensagem[7]. Sendo assim, o problema de geração de chaves é solucionado visto que não é possível obter a chave privada a partir da pública. Atualmente o algoritmo de chave Pública mais utilizado é o RSA (*Rivest-Shamir-Adleman*). Visto que essa técnica não é o objetivo do exposto artigo, sua descrição detalhada está além do escopo do mesmo. Para saber mais sobre o RSA pode-se consultar as respectivas bibliografias especificadas no final do trabalho[8,9,10,11].

3. DESENVOLVIMENTO

Para a implementação do modelo, foi adotado a linguagem de programação Python para a elaboração dos métodos de Criptografia. O ambiente de desenvolvimento que foi utilizado é o PyCharm Community Edition e também o editor SublimeText 3. As bibliotecas adicionais que foram necessárias ao projeto foram o Numpy que é uma biblioteca específica para computação numérica e também a biblioteca Math que é uma biblioteca nativa do Python utilizada para auxiliar nos cálculos matemáticos.

A ideia proposta inicialmente foi de elaborar um método criptográfico de cunho próprio partindo de técnicas já existentes e unindo conceitos de Criptografia Clássica Simétrica para a implementação em plataformas de Internet das Coisas. Logo, o código fonte dispõe de alguns conceitos Criptográficos, o primeiro deles é o conceito ou método da Cifra de César que consiste na permutação do alfabeto. Aplicando ao código fonte, a Cifra de César é utilizada a partir de 52 listas de chaves configuradas com 26 números aleatórios de 0 a 25. Dessa forma o usuário insere apenas o texto para ser criptografado. Logo o respectivo texto é encriptado com todas as 52 listas de chaves com seus respectivos 26 números contidos. O segundo conceito utilizado é o da Transposição que consiste basicamente em trocar as letras de lugar. Aplicando ao código, o texto inserido pelo usuário entra em um bloco de função, que por sua vez, preenche uma matriz quadrada automaticamente, ou seja, são feitos cálculos que permitem o programa decidir qual a matriz quadrada será mais efetiva, logo, se faltar espaços para completar a matriz, o programa à preenche com zeros, apenas para que fique completa. Isso é necessário

pois para encriptar a mensagem é preciso permutar a matriz utilizando sua transposta, ou seja, mudando linhas por colunas, logo para decriptar a matriz utilizamos o processo inverso (isto é, novamente a transposta e não a operação matricial inversa), que no caso de uma matriz quadrada será exatamente igual a sua forma original. Logo caso a matriz não seja quadrada, a operação de transposição de sua transposta não será exatamente igual à matriz original. O terceiro conceito utilizado é o conceito da Máquina de Rotor, que nesse caso, consistiu em utilizar apenas a reentrada de funções, ou seja, após o programa executar todos os passos e técnicas anteriores e obter um resultado, o programa utiliza essa saída para ser criptografada novamente. O número de repetições ou loops configurados foi de 51 rodadas.

4. RESULTADOS

Os resultados obtidos, após diversos testes realizados no código apontam que todos os métodos e conceitos utilizados foram aplicados de forma conjunta e que seu desempenho obteve êxito, visto que as técnicas utilizadas são de aspecto clássico. Pode-se observar o funcionamento nas figuras a seguir:

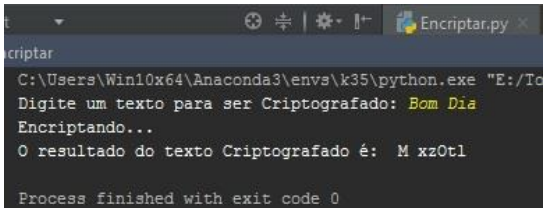


Figura 1. Exemplo de Criptografia do texto 1.

Na figura 1, é possível ver o processo de criptografia do código. Após executar o programa "Encriptar.py" na IDLE PyCharm, o software aguarda um texto de entrada. Esse texto pode ter até 5625 caracteres, ou seja, uma matriz quadrada de 75x75. Após a inserção do texto "Bom Dia", o programa executa suas respectivas operações e cálculos e então retorna como saída o texto criptografado "M xzOtl".

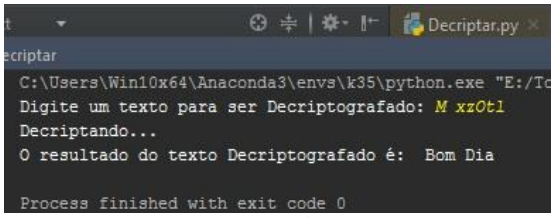


Figura 2. Exemplo de Decriptografia do texto 1.

Na figura 2, pode-se ver o processo de decriptação da mensagem obtida anteriormente. É preciso executar o código "Decriptar.py" e então inserir o texto criptografado "M zxOtl" para o programa retornar o texto original "Bom Dia" como saída.

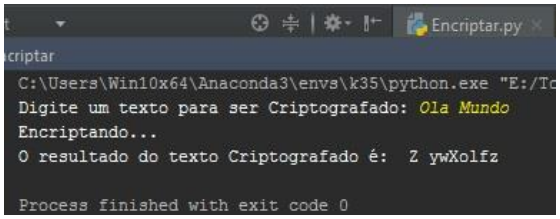


Figura 3. Exemplo de Criptografia do texto 2.

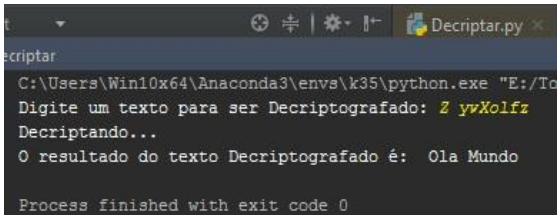


Figura 4. Exemplo de Decriptografia do texto 2.

Os seguintes processos mostrados nas figuras acima (figura 3 e figura 4) foram executados da mesma forma que os exemplos das figuras anteriores 1 e 2. Como é possível ver, foram obtidos os mesmos resultados, ou seja, o programa foi capaz de Encriptar e Decriptar qualquer texto que lhe foi dado como argumento de entrada e saída.

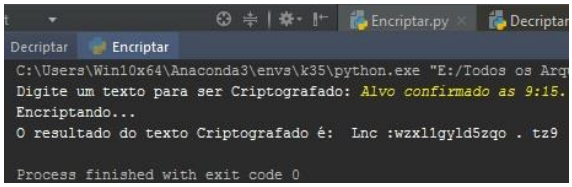


Figura 5. Exemplo de Criptografia do texto 3.

Na figura 5 foi solicitado ao programa que criptografasse um texto contendo números, "Alvo confirmado as 9:15.". Então é visto que o programa retorna uma saída mais ilegível do que nos exemplos anteriores, pois o tamanho do texto sendo maior, a ilegibilidade também aumenta.

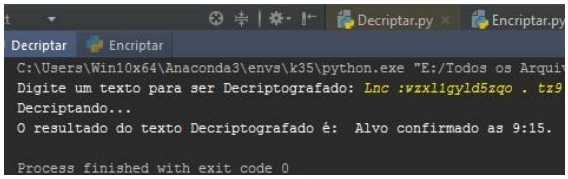


Figura 6. Exemplo de Decriptografia do texto 3.

Na figura 6 é solicitado ao código que decodifique o texto criptografado "Lnc :wzxl1gyld5zqo . tz9". É possível notar que o programa realiza a execução de decriptar a mensagem corretamente.

5. DISCUSSÃO

Dado que nos dias atuais a segurança se torna cada vez mais primordial para toda e qualquer tipo de entidade (isto é, pessoa, máquinas, corporações e/ou empresas), é imprescindível o uso da Criptografia para a segu-

rança nas mais diversas áreas. Hoje, é pouca ou quase nula a utilização de métodos clássicos para criptografia, porém os métodos simétricos ainda são evidentes e muito eficientes.

A aplicação da Criptografia no universo dos objetos inteligentes e conectados (IoT) tem aumentado gradativamente e em ritmo acelerado. É notável que nesse ritmo, as aplicações de segurança terão que acompanhar e se atualizar ainda mais rápido contra Ciberataques e outros tipos de ameaças à segurança dos objetos conectados à rede.

6. CONCLUSÃO

Conforme a análise dos resultados obtidos, percebe-se que o programa cumpriu com os objetivos inicialmente propostos, bem como na conscientização de como a segurança aplicada ao desenvolvimento de novos softwares e plataformas inteligentes, não é um dos principais fatores que são abordados pelos desenvolvedores.

Existem melhorias significativas que podem proporcionar a elaboração de trabalhos futuros. Alguns exemplos são: a aplicação prática do software em um dispositivo conectado na rede, melhorias para Cifra de Substituição e Transposição, como aprimorar o alfabeto expandindo sua gama de caracteres, dessa forma viabilizando a utilização de textos com acentuações, substituir o alfabeto comum por um alfabeto hexadecimal (melhorando assim de modo significativo o tempo de processamento) e aprimorar a transposição das matrizes quadradas. Em estudos futuros, pretende-se abordar a distribuição de chaves pela técnica Assimétrica (RSA) e a Criptografia em si pela técnica Simétrica, tendo em vista a expressiva utilização destas técnicas atualmente, uma vez que o avanço e o desenvolvimento de sistemas eletrônicos inteligentes apresentam novos desafios para a segurança e integridade das informações armazenadas e manipuladas pelos mesmos[12,13].

REFERÊNCIAS

[1] Oliveira Neto IR. Síntese de Requisitos de Segurança para Internet das Coisas Baseada em Modelos em Tempo de Execução. 2015. 116 f. Dissertação (Mestrado em Ciências da Computação) - Instituto de Informática, Universidade Federal de Goiás, Goiânia. 2015.

[2] Congresso da Sociedade Brasileira de Computação, XXXVI, 2015. Recife (PE). Anais... Recife (PE): Sociedade Brasileira de Computação, 2015. 58 p.

[3] Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, XIII, 2013. Manaus (AM). Anais... Manaus (AM): Simpósio Brasileiro Em Segurança Da Informação E De Sistemas Computacionais, 2013. p. 156-215.

[4] Cruz EF. A Criptografia e seu Papel na Segurança da Informação e das Comunicações (SIC) – Retrospectiva, Atualidade e Perspectiva. Brasília, 2009. 84 p.

[5] Terada R. Segurança de Dados: Criptografia em Rede de Computador. 2ª edição. São Paulo: Blucher, 2008. 305 p.

[6] SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B. Metodologia de pesquisa. 5. ed. Porto Alegre: AMGH, 2013. 624p. (Série Métodos de Pesquisa).

[7] Stallings W. Criptografia e Segurança de Redes: Princípios e Práticas. 6ª edição. São Paulo: Pearson, 2015. 558 p.

[8] Boneh D. "Twenty Years of Attacks on the RSA Cryptosystem". Notices of the American Mathematical Society, fev.1999.

[9] Cormen T, et al. Introduction to Algorithms. Cambridge, MA: MIT Press, 2009.

[10] DIFFIE, W. "Thr First Tem Years of Public-Key Cryptography". Proceedings of the IEEE, maio 1988.

[11] Shamir A, Tromer E. "On the Cost of Factoring RSA-1024". CryptoBytes, Verão 2003. Disponível em: <http://www.rsasecutiry.com/rsalabs>.

[12] Moreno ED, Pereira FD, Chiaramonte RB. Criptografia em Software e Hardware. São Paulo: Novatec, 2005. 288 p.

[13] PIRES, P. F. et al. Plataformas para Internet das Coisas, Rio de Janeiro, 60 p.

[14] GitHub. Código utilizado e desenvolvido no artigo. Disponível em: https://github.com/MrKruger/CRYPTOGRAPHY-APPLIED-TO-THE-SECURITY-OF-INTERNET-OF-THINGS#cryptography-applied-to-the-security-of-internet-of-things