

Helenton Carlos da Silva  
(Organizador)

The background is a dark purple gradient with a pattern of white and light blue mathematical and engineering icons. These include gears, a compass, a pencil and ruler, a scale, a network diagram, a calculator, a chemical structure, a magnifying glass, a graph of a bell curve, a graph of a sine wave, a graph of an absolute value function, a graph of a hyperbola, a book, and various geometric shapes and symbols.

Estudos (Inter)  
Multidisciplinares  
nas Engenharias

Helenton Carlos da Silva  
(Organizador)

# Estudos (Inter) Multidisciplinares nas Engenharias

Atena Editora  
2019

2019 by Atena Editora  
Copyright © Atena Editora  
Copyright do Texto © 2019 Os Autores  
Copyright da Edição © 2019 Atena Editora  
Editora Chefe: Profª Drª Antonella Carvalho de Oliveira  
Diagramação: Geraldo Alves  
Edição de Arte: Lorena Prestes  
Revisão: Os Autores



Todo o conteúdo deste livro está licenciado sob uma Licença de Atribuição Creative Commons. Atribuição 4.0 Internacional (CC BY 4.0).

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

### **Conselho Editorial**

#### **Ciências Humanas e Sociais Aplicadas**

Profª Drª Adriana Demite Stephani – Universidade Federal do Tocantins  
Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas  
Prof. Dr. Alexandre Jose Schumacher – Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso  
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília  
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa  
Profª Drª Cristina Gaio – Universidade de Lisboa  
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia  
Prof. Dr. Edvaldo Antunes de Faria – Universidade Estácio de Sá  
Prof. Dr. Eloi Martins Senhora – Universidade Federal de Roraima  
Prof. Dr. Fabiano Tadeu Grazioli – Universidade Regional Integrada do Alto Uruguai e das Missões  
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná  
Profª Drª Ivone Goulart Lopes – Istituto Internazionele delle Figlie de Maria Ausiliatrice  
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense  
Profª Drª Keyla Christina Almeida Portela – Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso  
Profª Drª Lina Maria Gonçalves – Universidade Federal do Tocantins  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof. Dr. Marcelo Pereira da Silva – Universidade Federal do Maranhão  
Profª Drª Miranilde Oliveira Neves – Instituto de Educação, Ciência e Tecnologia do Pará  
Profª Drª Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa  
Profª Drª Rita de Cássia da Silva Oliveira – Universidade Estadual de Ponta Grossa  
Profª Drª Sandra Regina Gardacho Pietrobon – Universidade Estadual do Centro-Oeste  
Profª Drª Sheila Marta Carregosa Rocha – Universidade do Estado da Bahia  
Prof. Dr. Rui Maia Diamantino – Universidade Salvador  
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará  
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande  
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

#### **Ciências Agrárias e Multidisciplinar**

Prof. Dr. Alan Mario Zuffo – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano  
Profª Drª Daiane Garabeli Trojan – Universidade Norte do Paraná  
Prof. Dr. Darllan Collins da Cunha e Silva – Universidade Estadual Paulista  
Profª Drª Diocléa Almeida Seabra Silva – Universidade Federal Rural da Amazônia  
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul  
Profª Drª Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia  
Prof. Dr. Jorge González Aguilera – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Júlio César Ribeiro – Universidade Federal Rural do Rio de Janeiro  
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão  
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará  
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

### **Ciências Biológicas e da Saúde**

Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás  
Prof. Dr. Edson da Silva – Universidade Federal dos Vales do Jequitinhonha e Mucuri  
Profª Drª Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina  
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria  
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará  
Profª Drª Magnólia de Araújo Campos – Universidade Federal de Campina Grande  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa  
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

### **Ciências Exatas e da Terra e Engenharias**

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto  
Prof. Dr. Alexandre Leite dos Santos Silva – Universidade Federal do Piauí  
Profª Drª Carmen Lúcia Voigt – Universidade Norte do Paraná  
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará  
Prof. Dr. Juliano Carlo Rufino de Freitas – Universidade Federal de Campina Grande  
Profª Drª Neiva Maria de Almeida – Universidade Federal da Paraíba  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

<b>Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)</b>	
E82	Estudos (inter) multidisciplinares nas engenharias 1 [recurso eletrônico] / Organizador Helenton Carlos da Silva. – Ponta Grossa, PR: Atena Editora, 2019.  Formato: PDF Requisitos de sistema: Adobe Acrobat Reader Modo de acesso: World Wide Web Inclui bibliografia ISBN 978-85-7247-697-3 DOI 10.22533/at.ed.973190910  1. Engenharia – Pesquisa – Brasil. I. Silva, Helenton Carlos da.  CDD 658.5
<b>Elaborado por Maurício Amormino Júnior – CRB6/2422</b>	

Atena Editora  
Ponta Grossa – Paraná - Brasil  
[www.atenaeditora.com.br](http://www.atenaeditora.com.br)  
contato@atenaeditora.com.br

## APRESENTAÇÃO

A obra “*Estudos (Inter) Multidisciplinares nas Engenharias*” aborda uma série de livros de publicação da Atena Editora, em seu I volume, apresenta, em seus 25 capítulos, discussões de diversas abordagens acerca da importância da (inter) multidisciplinaridade nas engenharias.

O processo de aprendizagem, hoje em dia, é baseado em um dinamismo de ações condizentes com a dinâmica do mundo em que vivemos, pois a rapidez com que o mundo vem evoluindo tem como chave mestra a velocidade de transmissão das informações.

A engenharia praticada nos dias de hoje é formada por conceitos amplos e as situações a que os profissionais são submetidos mostram que esta onda crescente de tecnologia não denota a necessidade apenas dos conceitos técnicos aprendidos nas escolas.

Desta forma, os engenheiros devem, além de possuir um bom domínio técnico da sua área de formação, possuir domínio também dos conhecimentos multidisciplinares, além de serem portadores de uma visão globalizada.

Este perfil é essencial para o engenheiro atual, e deve ser construído na etapa de sua formação com o desafio de melhorar tais características.

Dentro deste contexto podemos destacar que uma equipe multidisciplinar pode ser definida como um conjunto de profissionais de diferentes disciplinas que trabalham para um objetivo comum.

Neste sentido, este livro é dedicado aos trabalhos relacionados aos estudos da (inter) multidisciplinaridade nas engenharias, com destaque mais diversas engenharias e seus temas de estudos.

Os organizadores da Atena Editora agradecem especialmente os autores dos diversos capítulos apresentados, parabenizam a dedicação e esforço de cada um, os quais viabilizaram a construção dessa obra no viés da temática apresentada.

Por fim, desejamos que esta obra, fruto do esforço de muitos, seja seminal para todos que vierem a utilizá-la.

Helenton Carlos da Silva

## SUMÁRIO

<b>CAPÍTULO 1</b> .....	<b>1</b>
A IMPORTÂNCIA DA (INTER) MULTIDISCIPLINARIDADE NAS ENGENHARIAS PARA O DESENVOLVIMENTO E OPERAÇÃO DAS CIDADES INTELIGENTES	
Roberto Righi Roberta Betania Ferreira Squaiella	
<b>DOI 10.22533/at.ed.9731909101</b>	
<b>CAPÍTULO 2</b> .....	<b>13</b>
ANÁLISE DOS MÉTODOS DE ENSINO E AVALIAÇÕES UTILIZADOS NA GRADUAÇÃO DE ENGENHARIA FLORESTAL	
Elaine Cristina Lengowski Carla Cristina Cassiano	
<b>DOI 10.22533/at.ed.9731909102</b>	
<b>CAPÍTULO 3</b> .....	<b>26</b>
AVALIAÇÃO ERGONÔMICA DE POSTO DE TRABALHO EM UM ATELIÊ DE SOUVENIRS COM USO DOS MÉTODOS OWAS E DE SUZANNE RODGERS	
Jordy Felipe de Jesus Rocha Maria Vanessa Souza Oliveira Leila Medeiros Santos Bento Francisco dos Santos Júnior	
<b>DOI 10.22533/at.ed.9731909103</b>	
<b>CAPÍTULO 4</b> .....	<b>40</b>
AVALIAÇÃO ERGONÔMICA: ESTUDO DE CASO DE VIGILANTES	
Gustavo Francesco de Moraes Dias Diego Raniere Nunes Lima Renato Araújo da Costa Roberto Pereira de Paiva e Silva Filho Fernanda da Silva de Andrade Moreira Hugo Marcel Flexa Farias Jessica Cristina Conte da Silva	
<b>DOI 10.22533/at.ed.9731909104</b>	
<b>CAPÍTULO 5</b> .....	<b>53</b>
ESTILO DE LIDERANÇA QUE O ENGENHEIRO DE PRODUÇÃO DEVE POSSUIR NA ÓTICA DOS ENGENHEIROS DE PRODUÇÃO DA FACULDADE PARAÍSO DO CEARÁ	
Emmanuela Suzy Medeiros José Valmir Bezerra e Silva Júnior	
<b>DOI 10.22533/at.ed.9731909105</b>	
<b>CAPÍTULO 6</b> .....	<b>66</b>
EVOLUÇÃO DAS POLÍTICAS PÚBLICAS PARA A INDÚSTRIA NO BRASIL	
Lídia Silveira Arantes Thales de Oliveira Costa Viegas	
<b>DOI 10.22533/at.ed.9731909106</b>	



**CAPÍTULO 7 ..... 80**

**GOVERNANÇA, RESPONSABILIDADE SOCIAL E SUSTENTABILIDADE:  
ENTENDENDO OS FENÔMENOS DE GESTÃO ORGANIZACIONAL**

Leonardo Petrilli  
Denize Valéria dos Santos Baia  
Juliana Fernanda Monteiro de Souza

**DOI 10.22533/at.ed.9731909107**

**CAPÍTULO 8 ..... 93**

**PERCEPÇÃO AMBIENTAL DOS ALUNOS DO ENSINO FUNDAMENTAL DE UMA  
ESCOLA DA REDE PÚBLICA MUNICIPAL DE PARAUAPEBAS**

Diego Raniere Nunes Lima  
Renato Araújo da Costa  
Gustavo Francesco de Moraes Dias  
Roberto Pereira de Paiva e Silva Filho

**DOI 10.22533/at.ed.9731909108**

**CAPÍTULO 9 ..... 105**

**ANÁLISE DO RISCO DE ACIDENTE CAUSADO PELA ALTA TEMPERATURA EM  
ALTO-FORNO SIDERÚRGICO NO MUNICÍPIO DE MARABÁ – PA**

Diego Raniere Nunes Lima  
Roberto Pereira de Paiva e Silva Filho  
Gustavo Francesco de Moraes Dias  
Renato Araújo da Costa

**DOI 10.22533/at.ed.9731909109**

**CAPÍTULO 10 ..... 120**

**CONFECÇÃO DE BANCADA DIDÁTICA PARA SIMULAÇÃO DE SISTEMAS  
HIDRELÉTRICOS COM PERSPECTIVA À INTEGRAÇÃO DA INDÚSTRIA 4.0**

Kariston Dias Alves  
Gustavo Catusso Balbinot  
Artur Vitório Andrade Santos

**DOI 10.22533/at.ed.97319091010**

**CAPÍTULO 11 ..... 131**

**DESENVOLVIMENTO DE METODOLOGIA PARA ESTUDO DE VIABILIDADE  
TÉCNICA DE TERMELÉTRICAS A BIOMASSA NO BRASIL**

Beatriz Gabrielle de Carvalho Pinheiro  
Josiane do Socorro Aguiar de Souza Oliveira Campos  
Luciano Gonçalves Noleto  
Maria Vitória Duarte Ferrari  
Tallita Karolline Nunes

**DOI 10.22533/at.ed.97319091011**

**CAPÍTULO 12 ..... 143**

**DESENVOLVIMENTO DE UM REGULADOR AUTOMÁTICO DE TENSÃO  
MICROCONTROLADO UTILIZADO EM GERADORES SÍNCRONOS ISOLADOS**

Guilherme Henrique Alves  
Lúcio Rogério Júnior  
Antônio Manoel Batista da Silva  
Wellington Mrad Joaquim

**CAPÍTULO 13 ..... 157**

**DESPACHO ÓTIMO DAS UNIDADES GERADORAS DA USINA HIDRELÉTRICA  
LUIS EDUARDO MAGALHÃES**

Henderson Gomes e Souza  
Brunno Henrique Brito  
Vailton Alves de Faria  
Jabson da Cunha Silva

**DOI 10.22533/at.ed.97319091013**

**CAPÍTULO 14 ..... 170**

**DIMENSIONAMENTO E ANÁLISE ÓPTICA E TÉRMICA DE UM COLETOR  
PARABÓLICO COMPOSTO COM E SEM EFEITO ESTUFA**

Joaquim Teixeira Lopes  
Ricardo Fortes de Miranda  
Keyll Carlos Ribeiro Martins  
Camila Correia Soares

**DOI 10.22533/at.ed.97319091014**

**CAPÍTULO 15 ..... 177**

**EFEITOS DO TRATAMENTO TÉRMICO DE ENDURECIMENTO POR  
PRECIPITAÇÃO NA MICROESTRUTURA E PROPRIEDADES MECÂNICAS EM  
LIGAS DE AL-SI-MG FUNDIDAS**

Albino Moura Guterres  
Daniel Beck  
Cláudio André Lopes de Oliveira  
Juliano Poleze

**DOI 10.22533/at.ed.97319091015**

**CAPÍTULO 16 ..... 186**

**ESTUDO DA VIABILIDADE ECONÔMICA DE IMPLANTAÇÃO DE SISTEMAS  
FOTOVOLTAICOS CONECTADOS A REDE PARA CONSUMIDORES DO GRUPO A**

Roberto Pereira de Paiva e Silva Filho  
Murilo Miceno Frigo  
Gustavo Francesco de Moraes Dias  
Diego Raniere Nunes Lima  
Renato Araújo da Costa  
Timóteo Gonçalves Braga

**DOI 10.22533/at.ed.97319091016**

**CAPÍTULO 17 ..... 199**

**GESTÃO AMBIENTAL: ESTUDO DE CASO DA GESTÃO DOS RESÍDUOS  
ELETRÔNICOS NA IMAGEM SOM ELETRÔNICA LTDA**

Carla Ruanita Pedroza Maia  
Leila Medeiros Santos  
Maria Vanessa Souza Oliveira  
Bento Francisco dos Santos Júnior

**DOI 10.22533/at.ed.97319091017**



<b>CAPÍTULO 18</b> .....	<b>212</b>
INDICADOR DE CONSUMO DE ENERGIA ELÉTRICA	
Jean Carlos da Luz Pereira Felipe Guimarães Ramos	
<b>DOI 10.22533/at.ed.97319091018</b>	
<b>CAPÍTULO 19</b> .....	<b>225</b>
INVESTIGAÇÃO PRELIMINAR DE MODIFICAÇÕES NA CÉLULA FOTOVOLTAICA MONOCRISTALINA DE SILÍCIO	
Marcus André Pereira Oliveira Ana Flávia de Sousa Freitas Thiago Barros Pimentel Adão Lincoln Montel	
<b>DOI 10.22533/at.ed.97319091019</b>	
<b>CAPÍTULO 20</b> .....	<b>234</b>
UMA APLICAÇÃO DA EFICIÊNCIA ENERGÉTICA E EFICIÊNCIA EXERGÉTICA DAS TURBINAS A VAPOR NAS INDÚSTRIAS SUCROALCOOLEIRAS	
Nancy Lima Costa Maria de Sousa Leite Filha Arthur Gilzeph Farias Almeida Jaciera Dantas Costa Antônio Daniel Buriti de Macêdo José Nunes de Oliveira Neto Jordany Ramalho Silveira Farias José Jefferson da Silva Nascimento	
<b>DOI 10.22533/at.ed.97319091020</b>	
<b>CAPÍTULO 21</b> .....	<b>242</b>
THE STEAM GENERATION CENTERS AS A VECTOR FOR THE SUGARCANE MILLS EVOLUTION TO THE SUCRO-ENERGETICS PLANTS FORMAT	
Roque Machado de Senna Henrique Senna Rosimeire Aparecida Jerônimo	
<b>DOI 10.22533/at.ed.97319091021</b>	
<b>CAPÍTULO 22</b> .....	<b>252</b>
ANÁLISE DE CERTIFICADOS DIGITAIS EM DOMÍNIOS BRASILEIROS	
Matheus Aranha Diogo Pereira Artur Ziviani Fábio Borges	
<b>DOI 10.22533/at.ed.97319091022</b>	
<b>CAPÍTULO 23</b> .....	<b>264</b>
ANÁLISE DO IMPACTO DO ROTEAMENTO ALTERNATIVO EM REDES ÓPTICAS ELÁSTICAS TRANSLÚCIDAS CONSIDERANDO DIFERENTES CENÁRIOS DE DEGRADAÇÃO DA QUALIDADE DE TRANSMISSÃO	
Arthur Hendricks Mendes de Oliveira Helder Alves Pereira	
<b>DOI 10.22533/at.ed.97319091023</b>	

<b>CAPÍTULO 24 .....</b>	<b>271</b>
<b>SENSORIAMENTO ELETRÔNICO DE BAIXO CUSTO NO MONITORAMENTO HIDRÁULICO DE BOMBAS CENTRÍFUGAS</b>	
Lidiane Bastos Dorneles	
Samuel dos Santos Cardoso	
Samanta Tolentino Ceconello	
Jocelito Saccol de Sá	
<b>DOI 10.22533/at.ed.97319091024</b>	
<b>CAPÍTULO 25 .....</b>	<b>283</b>
<b>TUTORIAL SOBRE REPETIDORES DE DADOS MÓVEIS</b>	
Carine Mineto	
Lyang Leme de Medeiros	
Helder Alves Pereira	
<b>DOI 10.22533/at.ed.97319091025</b>	
<b>SOBRE O ORGANIZADOR.....</b>	<b>295</b>
<b>ÍNDICE REMISSIVO .....</b>	<b>296</b>

## ANÁLISE DE CERTIFICADOS DIGITAIS EM DOMÍNIOS BRASILEIROS

### Matheus Aranha

Universidade Federal do Rio de Janeiro, PESC/  
COPPE

Rio de Janeiro - Rio de Janeiro

### Diogo Pereira

Laboratório Nacional de Computação Científica

Petrópolis - Rio de Janeiro

### Artur Ziviani

Laboratório Nacional de Computação Científica

Petrópolis - Rio de Janeiro

### Fábio Borges

Laboratório Nacional de Computação Científica

Petrópolis - Rio de Janeiro

**RESUMO:** Apresentamos um requisito de segurança e sua avaliação de segurança para um protocolo da Internet. Especificamente, este trabalho apresenta uma verificação das chaves RSA dos certificados digitais presentes nos domínios brasileiros que usam o protocolo HTTPS. Tal verificação depende da aleatoriedade na geração de números primos. Utilizamos conceitos de Teoria dos Grafos para obtermos três resultados baseados nos dados que coletamos de centenas de milhões de domínios. No primeiro resultado, realizamos uma iteração sobre os certificados, gerando centenas de milhões de verificações. Felizmente, mostramos que o HTTPS está seguro a este ataque. No segundo, mostramos

que muitos domínios partilham a mesma chave criptográfica. No terceiro, mostramos que apenas 1% das autoridades certificadoras são relevantes.

**PALAVRAS-CHAVE:** https, internet, segurança, iot

### HTTPS KEYS IN THE BRAZIL

**ABSTRACT:** We introduce a security requirement and its security assessment for an Internet protocol. Specifically, this work presents a verification of the RSA keys of digital certificates present in the Brazilian domains that use the HTTPS protocol. Such verification depends on randomness in the generation of prime numbers. We use Graph Theory concepts to get three results based on the data we collected from hundreds of millions of domains. In the first result, we performed an iteration on the certificates, generating hundreds of millions of verifications. Luckily, we show that HTTPS is safe from this attack. In the second, we show that many domains share the same cryptographic key. In the third, we show that only 1% of the certification authorities are relevant.

**KEYWORDS:** https, internet, security, iot

### 1 | INTRODUÇÃO

Fisicamente possuímos métodos que

permitem a autenticidade de nossas ações e comprovação de nossa identidade, seja por um documento emitido por um órgão oficial, amplamente reconhecido, ou seja, por uma assinatura física. De forma similar, os sites na internet também possuem formas que validam sua autenticidade, garantindo que a informação enviada pelo usuário ao site realmente será enviada ao destinatário correto. A forma mais utilizada para um site validar sua autenticidade é por meio da utilização de certificados digitais, certificados válidos garantem que o site em questão é realmente válido e seguro.

Certificados digitais são produzidos com algoritmos criptográficos assimétricos que geram as assinaturas digitais. Os algoritmos assimétricos mais usados na internet são o RSA (Rivest, Shamir e Adleman) introduzido por (RIVEST; SHAMIR; ADLEMAN, 1978) e os baseados em curvas elípticas que foram introduzidas simultaneamente por (KOBLOITZ, 1987) e (MILLER, 1986) como uma alternativa eficiente para gerar algoritmos assimétricos.

Basicamente, os certificados digitais são documentos digitais que possuem características únicas, como a chave pública de um site, informações inerentes ao site para o qual o certificado foi emitido, seu período de validade e informações relacionadas a sua autoridade certificadora. Em resumo, pode-se adquirir um certificado digital dirigindo-se a uma autoridade de registro que coleta os dados para produção do certificado digital e verifica a validade de tais dados. A autoridade de registro transmite um arquivo com os dados para uma autoridade certificadora que assina tal arquivo com sua chave privada, gerando o certificado digital. Podemos verificar a validade do certificado porque as chaves públicas das autoridades certificadoras estão embutidas no software que usamos, por exemplo, o próprio sistema operacional ou algum navegador (browser).

Neste trabalho, analisamos somente certificados que utilizam o RSA como algoritmo de criptografia. Além de ser muito utilizado em assinatura de certificados digitais, o RSA também é utilizado na transmissão segura de dados em sistemas comerciais, privacidade e autenticidade de e-mails, sistemas de pagamentos, cartões de crédito, entre outros sistemas, por conta disso as vulnerabilidades presentes no RSA são muito estudadas (BONEH, 1999).

Um dos requisitos de segurança do RSA é a aleatoriedade na geração dos números primos, ou seja, entropia alta. Algoritmos de geração de números pseudo aleatórios de baixa qualidade acabam gerando números primos repetidos, provocando uma vulnerabilidade em protocolos baseados no RSA, que tem módulo  $n=pq$  onde  $p$  e  $q$  são primos. Se, pelo menos, duas chaves públicas de RSA possuem um fator comum em seus módulos, o atacante que possuir tais chaves públicas pode utilizá-las para fatorar os módulos e conseqüentemente gerar a chave privada de cada um dos certificados. Usando esta técnica, (LENSTRA et al., 2012) e (BARBULESCU et al., 2016) conseguiram descobrir diversas chaves privadas geradas com RSA. No entanto, não fica claro se alguma das chaves comprometidas pertence ao domínio brasileiro, nem ao menos fica claro se alguma das chaves comprometidas era de certificados

usados no HTTPS (Hyper Text Transfer Protocol Secure). Faz-se necessário uma avaliação de segurança nos certificados gerados com RSA para o protocolo HTTPS.

Inicialmente, levantamos a hipótese que as chaves comprometidas foram geradas para outros protocolos, usando algoritmos inapropriados como no fato das chaves fracas em ambiente Linux, relatado por (YILEK et al., 2009). Felizmente, os domínios brasileiros com HTTPS passaram na avaliação de segurança. Note que tal avaliação de segurança deveria ser feita para cada novo certificado.

Outro ponto importante abordado neste trabalho está relacionado com a infraestrutura de chaves públicas, tais estruturas têm como principal núcleo as autoridades certificadoras, que são responsáveis pela manutenção dos certificados digitais (BRAUN et al., 2014). Em particular, grande parte dos certificados digitais confiáveis atuais estão concentrados em uma pequena quantidade de autoridades certificadoras, não sendo necessário grande parte das autoridades certificadoras existentes, permitindo a emissão de certificados com um índice maior de confiabilidade (BRAUN; RYNKOWSKI, 2013).

Neste trabalho, coletamos e extraímos informações presentes nos certificados digitais dos domínios brasileiros (com extensão .br) com intuito de verificar este requisito de segurança das chaves RSA que são transmitidas nos certificados. Além da verificação das chaves, outro ponto foi a realização de uma análise destes certificados, permitindo ter uma visão geral de como os certificados estão distribuídos nos domínios. Também foi possível analisar a distribuição e importância das autoridades certificadoras utilizadas pelos domínios brasileiros.

As demais seções deste trabalho estão organizadas da forma descrita a seguir. Na Seção 2, apresentamos a metodologia utilizada para execução do trabalho, assim como uma breve descrição das técnicas utilizadas. Na Seção 3, apresentamos os resultados obtidos com a verificação das chaves, também são apresentadas análises sobre os dados coletados e análise dos grafos gerados com os dados e seus respectivos resultados. Por fim, na Seção 4, apresentamos a conclusão deste trabalho e possíveis trabalhos futuros.

## **2 | METODOLOGIA**

Esta seção apresenta informações sobre a obtenção dos certificados, sobre o requisito de segurança e sua respectiva avaliação de segurança das chaves criptográficas do RSA no HTTPS.

### **2.1 Coleta dos certificados digitais e extração das informações**

O processo de coleta dos dados dos certificados digitais que utilizam o RSA foi limitado somente para domínios que possuem extensão .br, registrados entre os anos de 2012 e 2013, disponíveis no site <https://dnscensus2013.neocities.org>.

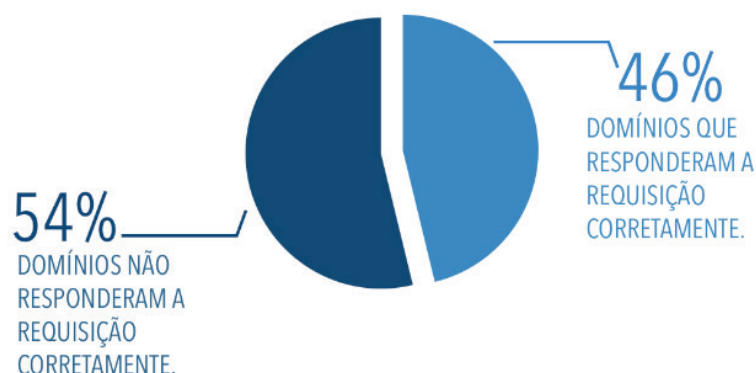


Figura 1 - Taxa de sucesso e erro das requisições.

Para domínios brasileiros, foi totalizado uma quantidade de 572.506 domínios registrados na base de dados utilizada, onde apenas 264.511 responderam de forma satisfatória a requisição para obtenção das chaves públicas do RSA nos certificados, o restante dos domínios, totalizando 307.995 domínios, apresentaram erros de requisição (tempo expirado, domínio inválido, entre outros erros), impossibilitando a coleta dos dados dos certificados. A Figura 1 apresenta a relação entre sucesso e falhas na coleta das chaves pública do RSA nos certificados brasileiros.

Em relação aos domínios que responderam de forma satisfatória a requisição dos certificados digitais, realizamos uma categorização de acordo com os padrões utilizados pelo domínio .br, obtendo uma noção de como os domínios brasileiros que possuem certificados válidos estão distribuídos, tal categorização pode ser observada na Figura 2.

Para o processo de categorização foram utilizados os padrões registrados pelo domínio .br, disponível em <https://registro.br/dominio/categoria.html>. Por isto, utilizamos as categorias “Genéricos”, “Universidades”, “Com restrição” e “DNSSEC obrigatório”. Os domínios contabilizados na categoria “Outros” são domínios que não se enquadram nas categorias mencionadas.

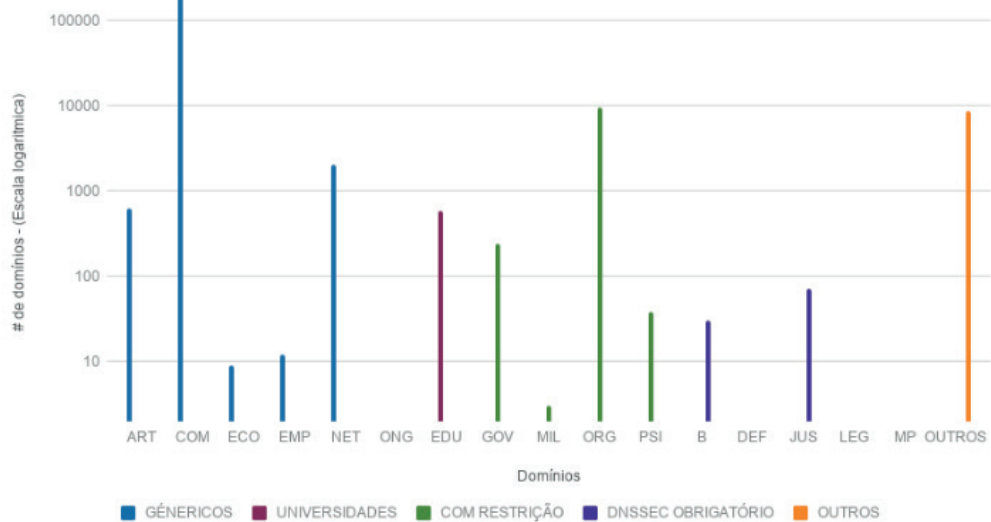


Figura 2 - Categoria de domínios brasileiros em escala logarítmica dos certificados coletados.

Durante o processo de coleta dos certificados foram extraídas informações importantes para verificação e análise, tais como: autoridade certificadora, domínios associados ao certificado, validade do certificado e algoritmo de hash utilizado, além de expoente e módulo de cada chave pública do RSA. As informações extraídas foram armazenadas em um dataset, utilizado posteriormente no processo de verificação e análise dos dados.

Para a coleta, extração dos certificados e criação do dataset, escrevemos um script em Python que utiliza a biblioteca `asn1crypto.x509` (WBOND, 2018). O script utilizado pode ser obtido em <https://github.com/mattslv/rsa-sanity-check>.

## 2.2 Avaliação de segurança das chaves rsa no https de domínios brasileiros

Após a extração do módulo de cada chave RSA nos certificados digitais, foi realizado a verificação das chaves RSA que consiste no cálculo do máximo divisor comum (MDC) de todos os módulos combinados dois a dois utilizando o algoritmo de Euclides, obtendo como saída os módulos cujo MDC fosse maior que 1. Lembre-se que cada módulo deveria ter no mínimo 1024 bits, ou seja, um número de aproximadamente 309 dígitos em decimal. No entanto, observamos que 101 certificados estão abaixo do número mínimo de bits aceitos para uma chave RSA. Tabela 1 mostra a frequência do tamanho dos módulos de chaves RSA nos certificados. (BORGES DE OLIVEIRA, 2017) e (TÉLLEZ; BORGES, 2018) apresentam uma relação entre o tamanho das chaves do RSA e seu respectivo nível de segurança.

Tamanho dos módulos	Quantidade de certificados
<b>512 bits</b>	101 certificados
<b>1024 bits</b>	4.848 certificados
1040 bits	1 certificados
2018 bits	1 certificados



2046 bits	1 certificados
<b>2048 bits</b>	251.080 certificados
2058 bits	1 certificados
2096 bits	1 certificados
2432 bits	1 certificados
3072 bits	14 certificados
<b>4096 bits</b>	8.462 certificados

Tabela 1 - Tamanho dos módulos e suas quantidades nos certificados.

Apesar dos tamanhos de chaves inapropriados, observamos que todos os expoentes dos domínios coletados têm valores iguais a 65.537, mostrando que os certificados digitais dos domínios brasileiros estão em conformidade com valores amplamente utilizado no RSA. (LENSTRA et al., 2012) e (BARBULESCU et al., 2016) encontraram expoentes com outros valores em outros protocolos. Felizmente, nenhum certificado usa a função de hash MD5. A Figura 3 mostra a porcentagem das frequências das funções de hash encontradas nos certificados.

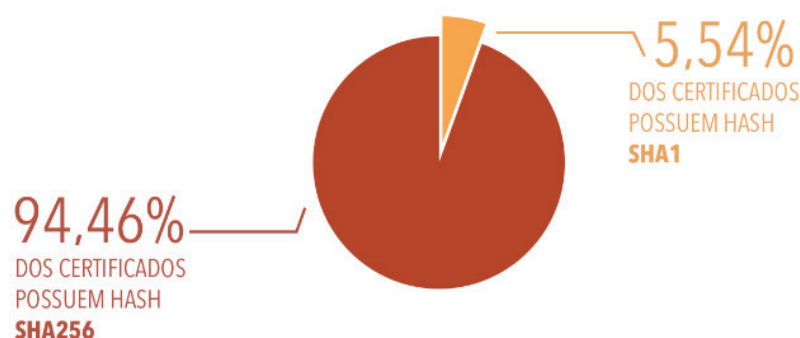


Figura 3 - Algoritmos de hash utilizados nos certificados.

No total foram calculados 415.080.078 funções MDC. Note que o MDC tem complexidade polilogarítmica, sendo muito mais rápido que algoritmos de fatoração, e portanto, já foi usado em ataques ao RSA (BORGES, 2008).

De fato, este ataque apresenta uma forma de descobrir os fatores de módulos que eventualmente tenham algum fator em comum. Vários outros algoritmos criptográficos usam produtos de primos nos módulos (BORGES; LARA; PORTUGAL, 2017), conseqüentemente, também podem ser atacados com a mesma estratégia. Neste caso, a segurança é baseada na aleatoriedade dos números primos que compõem os módulos.

Para o cálculo do MDC entre os módulos, escrevemos um script usando a biblioteca gmpy2 (MARTELLI, 2017) que possibilita operações aritméticas de múltipla precisão, o script pode ser obtido em <https://github.com/mattslv/rsa-sanity-check>.

### 3 | DISCUSSÕES E RESULTADOS

Esta seção apresenta discussões e resultados obtidos após a coleta e verificação dos dados extraídos dos certificados digitais. Foram realizadas análises das informações extraídas dos certificados digitais utilizando conceitos de Teoria dos Grafos e analisando a distribuição de grau, centralidade e modularidade dos grafos gerados com os dados.

Ao longo deste trabalho foram gerados grafos com representações distintas, utilizando parte das informações obtidas na Seção 2. Para cada grafo gerado, foram utilizadas diferentes representações de dados, possibilitando diferentes análises com o mesmo conjunto de dados. Especificamente, geramos três grafos a partir dos dados coletados.

No primeiro grafo, utilizamos apenas as chaves que possuem módulos únicos, com intuito de verificar a existência de certificados que possuem módulos com MDC maior que um. No segundo grafo, utilizamos os módulos e domínios dos certificados, com intuito de verificar se os domínios partilham ou não o mesmo módulo. No terceiro grafo, utilizamos como base os domínios e os nomes das suas autoridades certificadoras com a finalidade de verificar a quantidade de domínios por autoridade certificadora.

Tais representações através dos grafos podem ser observadas com mais detalhes nas seções abaixo, bem como seus respectivos resultados.

#### 3.1 Primeira representação por grafo

Na primeira representação utilizada na análise, consideramos como nós os módulos únicos extraídos dos certificados digitais. Consideramos como arestas a existência de um MDC maior que 1 entre ambos.

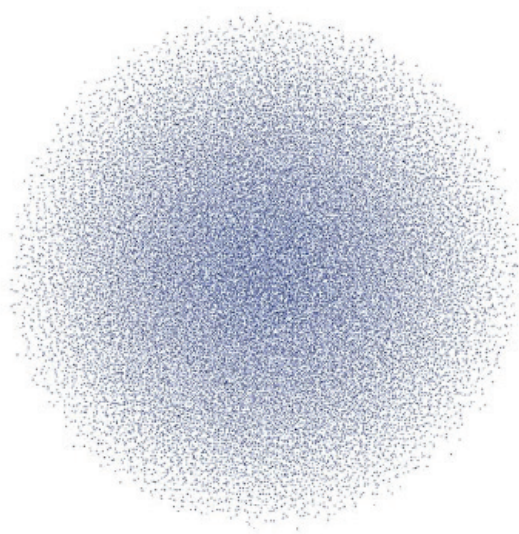


Figura 4 - Grafo gerado pelo MDC entre os módulos únicos.

Durante o processo de verificação do requisito de segurança das chaves não foi encontrado MDC maior que um entre os módulos obtidos, desta forma, foi obtido um grafo com um total de 28.813 nós e nenhuma aresta entre os nós, com grau médio igual a zero, i.e., sem conexão. A Figura 4 apresenta o grafo obtido. É notável observar na figura que foi obtida uma nuvem desconexa de pontos, não existindo componentes ligados entre os nós do grafo.

Para o âmbito de segurança, temos um ótimo resultado. Mostrando que os algoritmos utilizados para geração de números aleatório nos domínios brasileiros são satisfatórios, e consequentemente, os domínios não são vulneráveis entre si a esta classe de ataques. No entanto, quanto maior o número de módulos coletados, o ataque efetua mais verificações aumentando a chance de sucesso do ataque. Portanto, estamos trabalhando para coletarmos todos os módulos presentes no HTTPS.

### 3.2 Segunda representação por grafo

Foi gerada um grafo bipartido, onde os nós utilizados na primeira representação foram trocados de módulos únicos por módulos e endereços dos domínios (URLs - Uniform Resource Locators) extraídos dos certificados digitais. Com essa nova representação, foi obtido um grafo com um total de 292.824 nós e 264.511 arestas, com grau médio igual a 0,903.

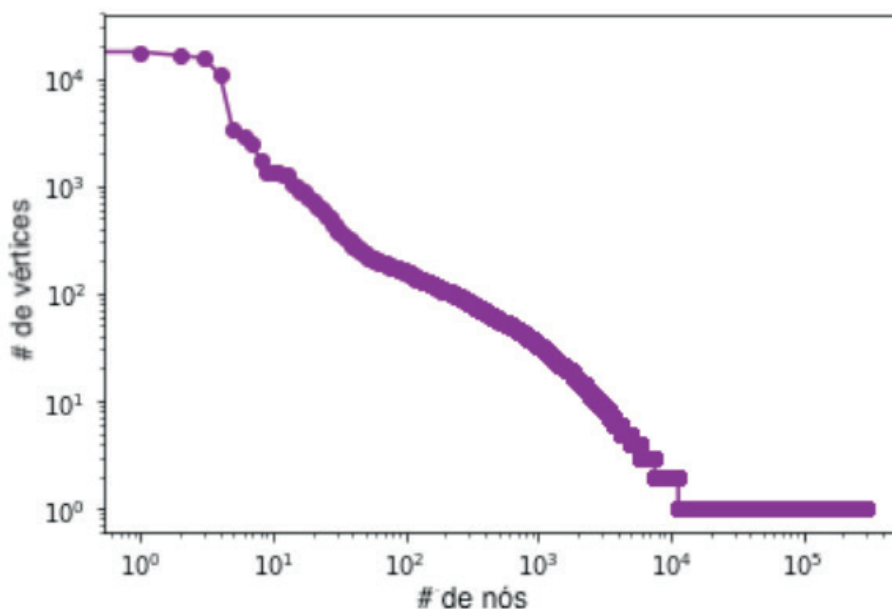


Figura 5 - Distribuição de grau do grafo gerado em escala logarítmica.

Por meio da Figura 5, podemos observar a distribuição de grau gerada. Analisando a imagem, podemos perceber muitos nós possuindo uma concentração muito alta de arestas, ou seja, existem muitos módulos que possuem conexão com vários domínios, mostrando que uma grande quantidade de domínios brasileiros (na grandeza de 10<sup>4</sup>) partilham o mesmo módulo. Consequentemente, quem tem

conhecimento uma única chave destas quatro maiores concentrações, tem acesso as transações de dezenas de milhares de sites brasileiros que usam o HTTPS.

(BARABÁSI; PÓSFAL, 2016) apresentam que este tipo de grafo segue um modelo de rede complexa de escala livre regida por uma lei de potência, sendo bastante vulnerável a ataques direcionados. Sendo assim, um ataque direcionado aos nós que possuem uma grande quantidade de domínios associados podem fazer um grande estrago, por exemplo, o vazamento da chave privada ou a fatoração de um módulo da chave do RSA associado a milhares de domínios causaria um grande impacto para estes domínios.

Apesar de a grande maioria dos domínios terem apenas um módulo, para a área de segurança, o ideal seria a existência de um módulo diferente para cada domínio registrado, não havendo este compartilhamento de módulos entre os domínios.

### 3.3 Terceira representação por grafo

Utilizamos os nomes das autoridades certificadoras e os domínios como nós para gerar um grafo bipartido. As arestas são relações entre autoridades e módulos. A partir desta representação, obtivemos um grafo com 29.161 nós e 28.321 arestas, com grau médio igual a 0,971.

É possível observar na Figura 6 que existe uma pequena quantidade de autoridades certificadoras que são responsáveis pela certificação da grande maioria dos domínios brasileiros. Também é possível visualizar que o grafo segue um padrão parecido com o do grafo anterior, ou seja, o grafo também é suscetível a ataques direcionados, sendo prejudicial se um atacante direcionar um ataque para uma autoridade certificadora responsável por muitos certificados digitais. Contrariamente, é muito melhor que se tenha poucas autoridades para confiar. (BRAUN; RYNKOWSKI, 2013) defendem que é muito mais fácil auditar e confiar em um número pequeno de certificadoras do que em um número muito alto.

Outro ponto importante a ser observado, caso 99% das autoridades certificadoras menos influentes que atuam nos domínios brasileiros fossem retiradas, aproximadamente 90% dos domínios que possuem certificados digitais ainda seriam certificados por uma autoridade válida, corroborando o ponto mostrado por (BRAUN; RYNKOWSKI, 2013). Em particular, os certificados poderiam ser distribuídos baseados na localidade geográfica, seguindo um modelo similar ao DNS (Domain Name System).

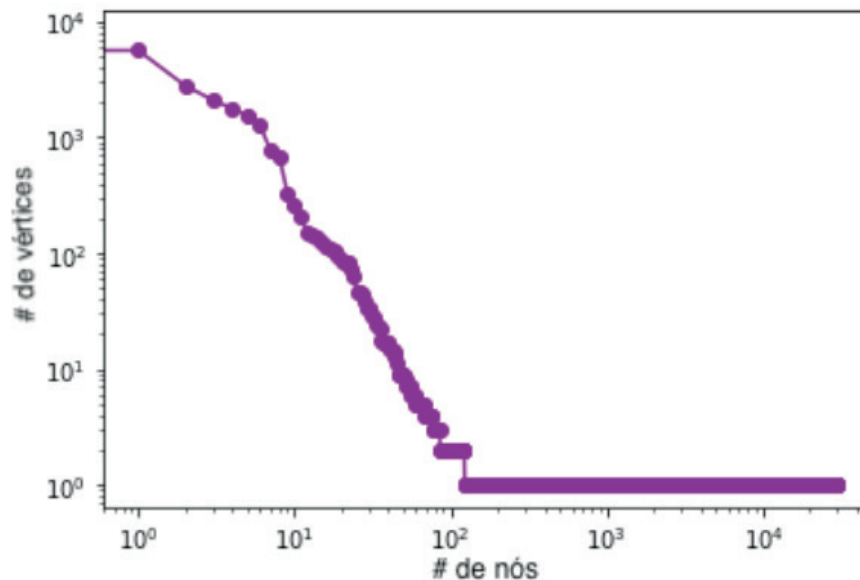


Figura 6 - Distribuição de grau do grafo gerada em escala logarítmica.

Outra análise realizada para este grafo foi o cálculo de modularidade, onde foi obtido uma modularidade igual a 0,858 com um total de 849 comunidades formadas, mostrando que o grafo obtido tem alta chance de formar comunidades com nós de características parecidas, ou seja, grandes autoridades certificadoras tendem a continuar atuando e certificando grande parte dos certificados digitais. A distribuição de nós e modularidade pode ser observada na Figura 7.

#### 4 | CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho apresenta a realização da avaliação de segurança de um requisito de segurança das chaves do RSA presentes nos certificados digitais dos domínios com extensão .br. No processo de verificação, fizemos uma análise através de Teoria dos Grafos e encontramos um resultado diferente de outros trabalhos na literatura. A diferença deve ser devida aos algoritmos de geração de números pseudo aleatórios de outros protocolos.

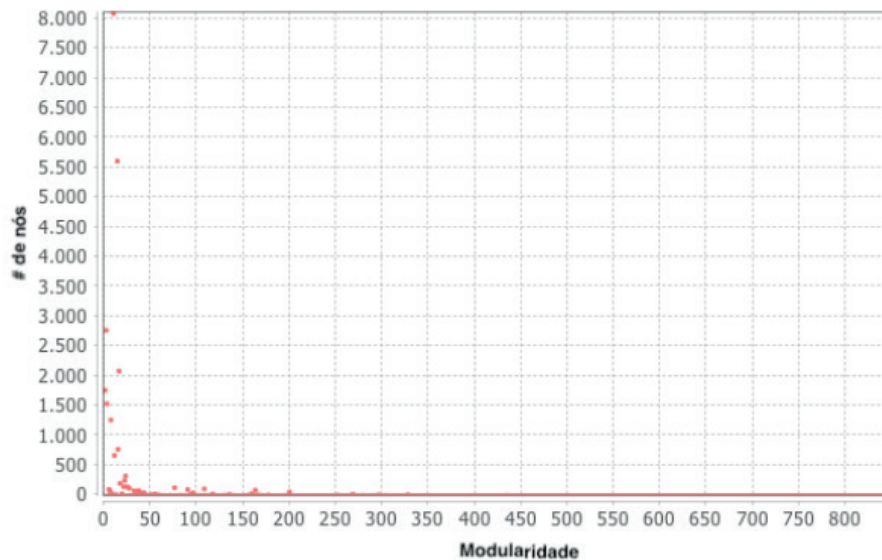


Figura 7. Distribuição de nós por modularidade do grafo gerado.

Mostramos na seção 3.1 que os domínios brasileiros estão livres entre si desta classe de ataques utilizando o módulo das chaves nos certificados. Porém, é preciso realizar esta verificação em um escopo maior, pois a amostra utilizada é relativamente pequena para tirar conclusões definitivas.

Mostramos na seção 3.2 que grande parte dos domínios brasileiros partilham os mesmos módulos e conseqüentemente os mesmos certificados, o que gera um grande problema de segurança, bastando que a chave privada de apenas um seja exposta para prejudicar os demais domínios pertencentes ao mesmo grupo.

Por fim na seção 3.3, mostramos a existência de uma concentração muito grande das autoridades certificadoras, sendo possível visualizar que grande parte dos domínios brasileiros são certificados por poucas autoridades. Temos que 99% das autoridades certificadoras dos certificados coletados são irrelevantes atualmente para manter os domínios brasileiros certificados.

É interessante realizar as mesmas análises para todos os domínios da Internet, principalmente a verificação das chaves RSA. Já estamos trabalhando nesta direção. Estamos buscando também a realização de outras representações, através de grafos, com os dados extraídos.

## REFERÊNCIAS

BARABÁSI, A.-L.; PÓSFAL, M. **Network science**. Cambridge: Cambridge University Press, 2016.

BARBULESCU, Mihai et al. RSA weak public keys available on the Internet. In: **International Conference for Information Technology and Communications**. Springer, Cham, 2016. p. 92-102.

BONEH, Dan et al. Twenty years of attacks on the RSA cryptosystem. **Notices of the AMS**, v. 46, n. 2, p. 203-213, 1999.



BORGES DE OLIVEIRA, Fábio. Selected Privacy-Preserving Protocols. In: **On Privacy-Preserving Protocols for Smart Metering Systems**. Springer, Cham, 2017. p. 61-100.

BORGES, F. Um Novo Algoritmo Probabilístico para Fatoração de Inteiros com Primos Relativamente Distantes. In: **Anais do VIII SBSEG – Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2008. p. 269-270.

BORGES, Fábio; LARA, Pedro; PORTUGAL, Renato. Parallel algorithms for modular multi-exponentiation. **Applied Mathematics and Computation**, v. 292, p. 406-416, 2017.

BRAUN, Johannes et al. CA trust management for the web PKI. **Journal of Computer Security**, v. 22, n. 6, p. 913-959, 2014.

BRAUN, Johannes; RYNKOWSKI, Gregor. The potential of an individualized set of trusted cas: Defending against ca failures in the web pki. In: **2013 International Conference on Social Computing**. IEEE, 2013. p. 600-605.

KOBLITZ, Neal. Elliptic curve cryptosystems. **Mathematics of computation**, v. 48, n. 177, p. 203-209, 1987.

LENSTRA, Arjen et al. **Ron was wrong, Whit is right**. IACR, 2012.

MARTELLI, A. **gmpy2 Library**. <https://github.com/aleaxit/gmpy2> Library, 2017. Disponível em: <<https://github.com/aleaxit/gmpy2>>

MILLER, Victor S. Use of elliptic curves in cryptography. In: **Conference on the theory and application of cryptographic techniques**. Springer, Berlin, Heidelberg, 1985. p. 417-426.

RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Leonard. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, v. 21, n. 2, p. 120-126, 1978.

TÉLLEZ, Claudio; BORGES, Fábio. Trade-off between Performance and Security for Supersingular Isogeny-Based Cryptosystems. In: **Anais do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2018. p. 113-126.

WBOND. **asn1crypto Library**. <https://github.com/wbond/asn1crypto> GitHub, 2018. Disponível em: <<https://github.com/wbond/asn1crypto>>

YILEK, Scott et al. When private keys are public: Results from the 2008 Debian OpenSSL vulnerability. In: **Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement**. ACM, 2009. p. 15-27.



## ÍNDICE REMISSIVO

### A

Alto forno 105, 108

### B

Bancada didática 120, 123, 129, 273, 274, 277, 281, 282

### C

Cartografia 131

Casca de arroz 131, 133, 135, 136, 137, 138, 139, 140

Cidades Inteligentes (CI) 1, 5, 7, 8

Comissionamento das unidades hidrelétricas 157, 165, 167

Concentrador solar 170

Conscientização ambiental 93

CPC 170, 171, 172, 175, 176

### D

Dimensionamento 170, 171, 175, 176, 193

### E

Educação ambiental 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104

Educação na escola 93

Energia solar 170, 171, 186, 187, 228, 233

Engenheiro de produção 53, 54, 55, 58, 59, 61, 62, 63, 64

Ensino universitário 13

Ergonomia 26, 27, 28, 35, 40, 41, 42, 51, 52, 58, 295

Estilo de liderança 53, 54, 55, 57, 58, 60, 61, 62, 63, 64

### F

Fenômenos organizacionais 80

Função de produção hidrelétrica 160, 169

### G

Gerador síncrono isolado 143

Governança corporativa 80, 82, 88, 89, 90, 91

### I

Índice de aproveitamento 13

Indústria 4.0 120, 122, 123, 125, 126, 128, 129, 130

Inovação 3, 6, 7, 8, 57, 66, 67, 68, 73, 74, 75, 77, 78, 79, 281, 295

(Inter) Multidisciplinaridade 1, 2, 9

## L

Liderança 38, 53, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65

## M

Método de Suzanne Rodgers 26, 28, 29, 34

Métodologias ativas 13

Método OWAS 26, 42, 44, 45, 50, 51

Microcontrolador PIC 143

Miniusinas 131, 139

## O

Óptica 170, 175, 264, 265, 266, 268, 282, 285, 286, 287

## P

Plano diretor 1

Política industrial 66, 67, 68, 69, 70, 71, 72, 73, 75, 76, 77, 78, 79

Política pública 66

Prevenção a acidentes 105

Programação não-linear inteira-mista 157, 158, 162

Projetos urbanos 1

## Q

Questionário nórdico 26, 30, 34, 37

## R

Regulador automático de tensão 143, 144, 145, 149, 150

Responsabilidade social 58, 80, 81, 82, 83, 84, 85, 86, 87, 89, 90, 91, 200

## S

Saúde do colaborador 26

Segurança do trabalho 38, 40, 52, 58, 295

Sistema de excitação 143, 145

Sistemas hidrelétricos 120, 121, 123, 124, 129, 130, 157

Sustentabilidade 7, 10, 58, 71, 80, 82, 86, 87, 88, 89, 90, 91, 104, 295

## T

Tecnologia da informação e comunicação (TIC) 1, 2, 3, 12

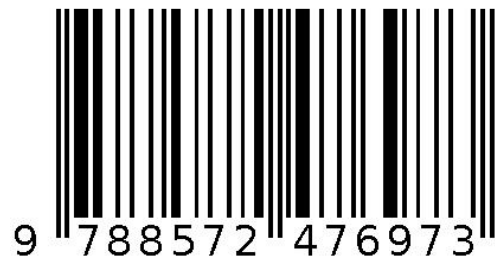
Temas transversais 93, 96, 98, 103, 127

Temperatura 36, 37, 105, 106, 107, 108, 109, 112, 116, 117, 118, 143, 147, 170, 172, 173, 174, 175, 179, 218, 220, 225, 226, 227, 229, 230, 231, 232, 233, 238, 282

## V

Vigilância 40, 45, 47, 50

Agência Brasileira do ISBN  
ISBN 978-85-7247-697-3



9 788572 476973