INTERFACE TECNOLÓGICA

CRIPTOGRAFIA RSA: sua importância e utilização em sistemas atuais

RSA ENCRYPTION: its importance and use in current systems

Lucas Sgarbi Aravéchia – ls.aravechia@gmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – São Paulo – Brasil

Mauricio de Oliveira Dian – mauricio.dian@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – São Paulo – Brasil

DOI: 10.31510/infa.v21i1.1891
Data de submissão: 09/04/2024
Data do aceite: 10/03/2024
Data da publicação: 20/06/2024

RESUMO

Com o crescente avanço da digitalização de informações sensíveis e o aumento das ameaças cibernéticas, torna-se fundamental o domínio de técnicas criptográficas robustas, como o RSA (*Rivest-Shamir-Adleman)*. Essa necessidade é ainda mais evidente em um contexto de pandemia e pós-pandemia, onde observamos um significativo aumento de ataques cibernéticos, vazamentos de dados e incidentes de *ransomware*. A habilidade de proteger dados sensíveis não apenas fortalecerá a confiança dos clientes, mas também garantirá a conformidade com as rigorosas regulamentações de privacidade de dados, como a LGPD (Lei Geral de Proteção de Dados Pessoais). Essa conformidade, por sua vez, consolida a posição competitiva no mercado global. Tal artigo foi desenvolvido tomando como base essas evidências juntamente com pesquisas bibliográficas na área, bem como opiniões de instituições de segurança como a NITS (*National Institute of Standards and Technology)* e IMPA (Instituto de Matemática Pura e Aplicada), sendo essas fontes estudiosos e agências regulatórias sobre segurança da informação. Ao longo dele, será abordado assuntos como o que é o algoritmo de RSA, sua segurança e sua eficácia na atualidade, comparando-o com ECDSA que é de outra categoria. Esse artigo não só demonstra a importância do RSA na criptografia de informações, como também destaca os algoritmos ECC, em especial o ECDSA, que tem potencial para também substituí-lo.

Palavras-chave: RSA. Criptografia. Segurança da Informação.

ABSTRACT

With the increasing advancement of the digitalization of sensitive information and the increase in cyber threats, it is essential to master robust cryptographic techniques, such as RSA (Rivest-Shamir-Adleman*)*. This is necessary and even more evident in a pandemic and post-pandemic context, in which we have seen a significant increase in cyberattack, data leaks and ransomware

incidents. The ability to protect sensitive data will not only strengthen customer trust, but also ensure compliance with strict data privacy regulations such as LGPD (Brazilian General Personal Data Protection Law). This compliance, in turn, consolidates the competitive position in the global market.This article was developed based on these evidences together with bibliographic research in the area, as well as opinions from security institutions such as NITS (National Institute of Standards and Technology) and IMPA (Instituto de Matemática Pura e Aplicada), which are scholars and regulatory agencies on information security. Throughout the paper, topics such as what is the RSA algorithm, its security and its effectiveness today, comparing it with ECDSA which is from another category, will be addressed. This article not only demonstrates the importance of RSA in information encryption, but also highlights ECC algorithms, especially ECDSA, which has the potential to replace it as well.

Keywords: RSA. Cryptography. Information security.

1. INTRODUÇÃO

A preocupação com a segurança da informação não é algo que começou nos tempos atuais. Ela vem desde o mundo antigo, prova disso é a chamada Cifra de Cézar, onde o imperador romano usava de substituição para enviar mensagens cifradas para seus generais de modo que somente eles soubessem o real significado da mensagem. Na atualidade, as informações quando manipuladas e vazadas são determinantes para o sucesso ou a falência de empresas. Desta forma, é de extrema importância verificar se os dados e informações estão sempre seguros, permanecendo sempre íntegros, confidenciais e disponíveis para seus usuários corretos.

Segundo a Universidade Federal de Mato Grosso do Sul (2020), criptografia vem do grego "*kryptós"* e "*gráphein"*, que significa "ocultar" e "escrita" respectivamente, o que demonstra bem o objetivo do uso de algoritmos criptográficos para cifrar um dado de forma que outras pessoas não tem conhecimento sobre uma informação criptografada ou ainda livre acesso à mensagem em texto puro.

Segundo FortiGuard Labs (2022, apud Oliveira 2022), ocorreu um aumento de 94% de tentativa de ataques cibernéticos no primeiro semestre de 2022 comparado ao primeiro semestre de 2021. Foram cerca de 31,5 bilhões de tentativas no primeiro semestre de 2022 contra 16,2 bilhões de tentativas no ano anterior e a tendência é aumentar.

Através de pesquisas bibliográficas em livros, artigos e matérias relacionadas ao assunto, este trabalho tem por objetivo se aprofundar no tema proposto pontuando a importância da

segurança da informação e da criptografia nos sistemas atuais. Ao discorrer sobre alguns desses conceitos, o presente artigo se justifica pelo fato de tentar ressaltar e reforçar a necessidade de mecanismos de segurança e algoritmos de criptografia como o RSA (*Rivest-Shamir-Adleman)* nos mais diversos cenários para agregar proteção pertinente e significativa às aplicações.

2. FUNDAMENTAÇÃO TEÓRICA

Segundo Coutinho (2015), a Criptografia RSA é um algoritmo de criptografia de chave assimétrica que foi criado por três funcionário do MIT (*Massachusetts Institute of Technology)* em 1977, sendo eles Ron Rivast, Adi Shamir e Leonard Adleman e, por isso, o algoritmo leva as iniciais do sobrenome de seus criadores.

Na época, os sistemas de criptografia eram baseados principalmente em algoritmos de chave simétrica, que compartilham uma chave entre origem e destino antes de iniciar a comunicação. A ideia dos pesquisadores era criar um mecanismo com a presença de dois tipos de chaves (pública e privada), geradas uma a partir da outra através de uma relação matemática, e que pudesse agregar segurança computacional a um sistema através destas chaves, desde que elas tenham sido criadas com complexidade e tamanhos suficientes a ponto de a chave pública poder ser veiculada tranquilamente sem que o sistema que a utilizasse fosse quebrado em tempo hábil.

Segundo Barker (2020), para se ter uma boa segurança em sistemas que se utilizam de algoritmos de chave assimétrica, é necessário no mínimo uma chave de tamanho 2048 bits. Binance (2022) firma que a chave assimétrica de 2048 bits de tamanho se equivale, em termos de segurança, a aproximadamente uma chave de 128 bits simétrica.

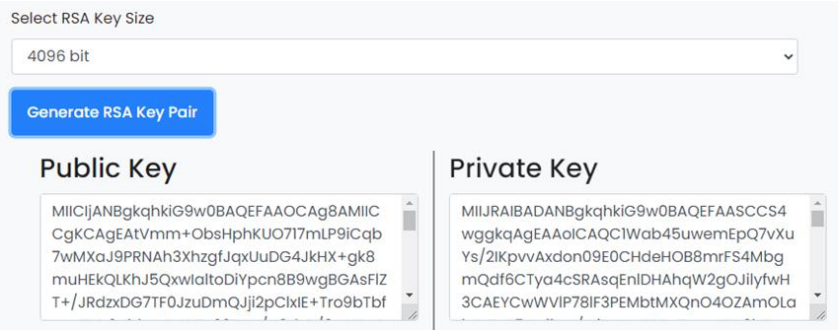
A criptografia RSA se utiliza da teoria dos números, ou seja, um ramo da matemática que estuda a propriedade dos números. No caso do RSA, ele se utiliza da propriedade dos números primos e semiprimos. A utilização de números primos pelo método se dá ao fato do alto poder de processamento que seria necessário para fatorá-los, uma vez que seria necessário fazer uma busca grande e testar todos os números possíveis para satisfazer o desafio.

Segundo Coutinho (2015), quanto maior as casas decimais de um número primo, maior seria a complexidade e, portanto, o tempo gasto para quebrar a lógica. Como em condições normais o RSA usa de números enormes.

Para entender melhor como o algoritmo RSA funciona, a ferramenta "*Online RSA Encryption, Decryption And Key Generator Tool*" pode ser utilizada. Ela pode ser encontrada no site da empresa Devglan no endereço "https://www.devglan.com/online-tools/rsa-encryption-decryption". Com ela é possível gerar os pares de chaves de 515, 1024, 2048, 3072 e 4096 bits para testar a encriptação e decriptação de mensagens.

Na Figura 1 é mostrado a geração de um par de chaves. Onde na parte superior seleciona o tamanho da chave e clica no botão "*Generate RSA Key Pair*", no caso foi escolhido a geração do par de chaves de 4096 bits.

Figura 1 – Geração do par de chaves utilizando o site da Devglan.

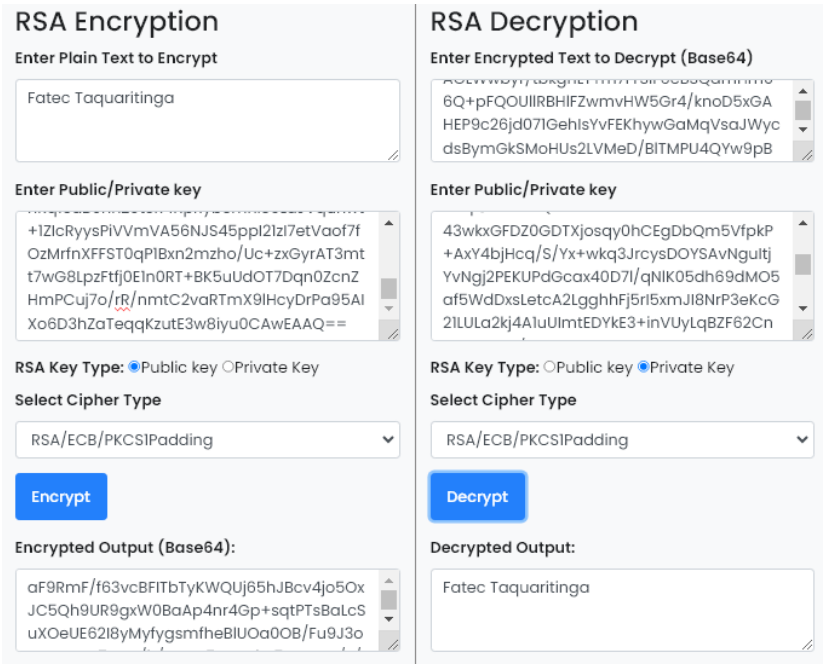


Fonte: Ray (2018).

A esquerda da Figura 2 mostra o local onde deve ser inserida a mensagem a qual se deseja criptografar. Foi digitado "Fatec Taquaritinga" como mensagem e, ao inserir a chave pública gerada anteriormente e clicar em "*Encrypt"*, a mensagem foi criptografada.

Da mesma forma, na parte direita da Figura 2, é possível ver o processo contrário, ou seja, foi inserida a mensagem cifrada juntamente com a chave usada para descriptografar a mensagem.

Figura 2 – Encriptando e decriptando mensagem no site da Devglan



Fonte: Ray (2018).

3. PROCEDIMENTOS METODOLÓGICOS

Para o desenvolvimento deste artigo foram realizadas pesquisa bibliográfica em livros, artigos e matérias que discutiam a segurança e a importância do algoritmo objeto de estudo. Tais pesquisas se caracterizam pelo método qualitativo, uma vez que foi utilizado fontes confiáveis por conta de serem, em sua maioria, de institutos governamentais ou empresa que trabalham no ramo de segurança da informação e suas tecnologias, como Barker (2020), Binance (2022), Fortinet (2022), Coutinho (2015), entre outros autores e empresas que entendem sobre o assunto.

Após leitura exploratória com o intuito de encontrar materiais e conceitos relacionados ao tópico em discussão, foi feita uma leitura seletiva para escolher artigos e matérias que melhor se encaixavam na justificativa deste artigo. Ao estabelecer interligações entre as fontes, pode-se explorar os temas abordados a fim de tentar alcançar alguns objetivos.

4. RESULTADOS E DISCUSSÃO

Por conta do RSA ser uma das primeiras técnicas de criptografia assimétrica, ela revolucionou o uso da criptografia de forma que emissor e receptor podem ter um meio de conversa protegidos e o vazamento de uma chave não dá acesso a toda informação, pois a chave pública pode ser divulgada sem problemas.

Outra vantagem que o tempo trás é a maturidade para o algoritmo, uma vez que já foi testado há muito tempo e por diversas vezes, já se sabe seus pontos fortes. Isso é de extrema importância, pois quanto mais testado algo é, mais se concretiza como é difícil achar falhas catastróficas e quebrar a criptografia.

Independentemente do tamanho da empresa, a proteção dos seus dados é de suma importância, ainda mais com a presença de leis como a LGPD (Lei Geral de Proteção de Dados Pessoais). Segundo Rastogi (2023), mesmo os dados poderem existir em 3 estados diferentes (repouso, em uso e em movimento), o RSA pode ser usado para aplicar proteção em qualquer um destes.

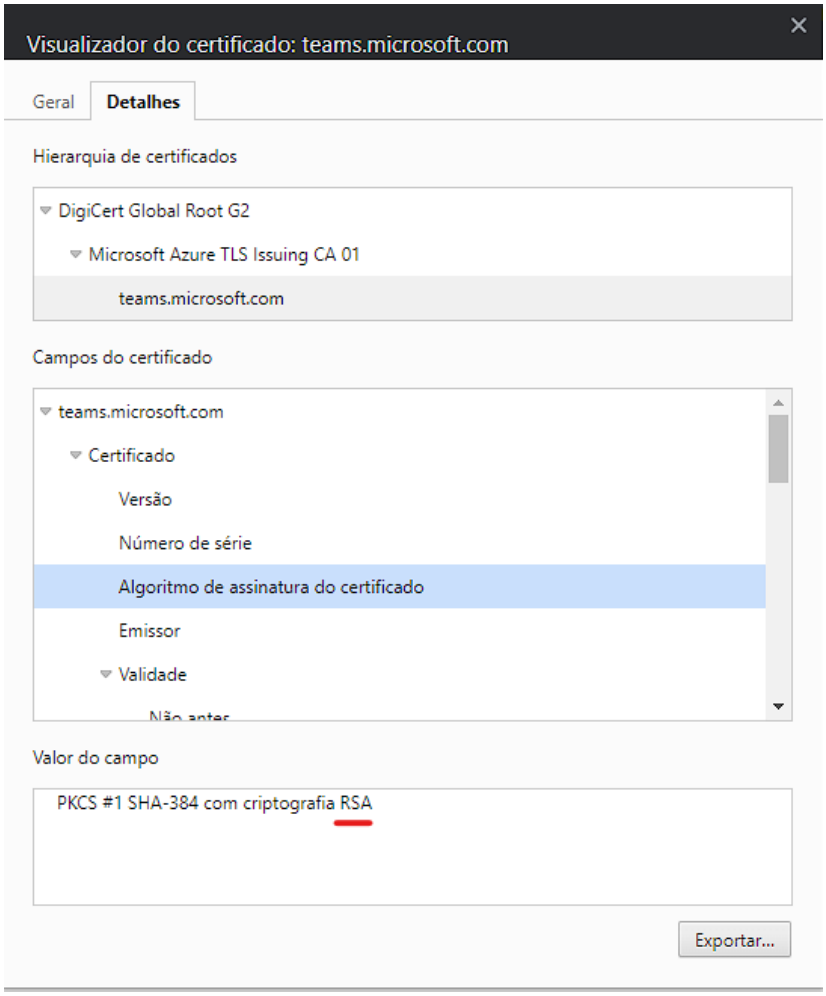
Ainda segundo Rastogi (2023). Pode-se proteger dados em repouso utilizando FDE (criptografia completa de disco), forma de criptografar todo disco onde os dados estão guardados, para impedir de serem facilmente vazados em caso de uma invasão lógica ou virtual dos arquivos. Já para proteger dados em uso deve-se sempre que possível criptografar os dados e procurar a utilização de HSM (*Hardware Security Modules*) que protege e divide o acesso de cada chave dos dados utilizados. Em dados em movimento para a segurança deles podem ser utilizados protocolos TLS/SSL ou VPN para proteger os dados em uma transferência de um dispositivo para outro, para evitar de eles serem interceptados, roubados ou vazados.

O algoritmo RSA é ainda um dos algarismos mais utilizados atualmente principalmente em alguns dos sistemas de comunicação e integridade de informações que precisam garantir segurança. Segundo Novageo (2022) e Nordvpn (2022) alguns destes sistemas usufruem de:

- **TLS/SSL (*Transport Layer Security/Secure Sockets Layer*):** O RSA é usado para estabelecer conexões seguras na internet, permitindo a criptografia das comunicações entre um navegador e um servidor web. É frequentemente utilizado para trocar chaves de sessão seguras durante o processo de negociação de chave em protocolos HTTPS.
- **Criptografia de E-mail:** com RSA os e-mails podem ser criptografados, garantindo assim a autenticidade, privacidade e o não-repúdio.
- **Autenticação e Assinaturas digitais:** O RSA também é empregado para criar assinaturas digitais, o que garante a autenticidade e integridade de documentos eletrônicos. A assinatura digital é gerada a partir da chave privada do remetente e pode ser verificada usando a chave pública correspondente. Assinatura digitais feitas em diplomas de cursos superiores são possíveis graças ao RSA.
- ***Tokens* e Segurança de Pagamentos:** O RSA é utilizado em aplicações de segurança financeira para gerar tokens em transações de pagamento e proteção de informações sensíveis em processos de pagamento online. Alguns meios de pagamento utilizando cartão de crédito só são seguros graças ao RSA.
- **Armazenamento Seguro de Chaves:** O RSA pode ser utilizado para criptografar chaves simétricas, permitindo o armazenamento seguro e a distribuição de chaves em sistemas que requerem um alto nível de segurança.
- **Acesso a Sistemas e Autenticação:** O RSA é aplicado em sistemas de autenticação de dois fatores (2FA) e em soluções de acesso seguro para autenticar usuários e autorizar suas interações com sistemas e serviços. Aplicativos como Google Authenticator podem utilizar a RSA para gerar as chaves de dois fatores.
- **VPN (*Virtual Private Network*):** RSA é usado para autenticação e estabelecimento seguro de conexões por VPN, garantindo a privacidade das comunicações em redes privadas virtuais. Conexões empresariais remotas pela internet são seguras pois muitas das vezes são criptografadas pelo RSA.

A Figura 3 mostra o certificado digital SSL/TLS do site do Teams da Microsoft. Observe que ele utiliza *hash* criptográfico SHA-384 e algoritmo RSA para garantir que a troca de dados entre aplicações cliente e o servidor do Teams sejam criptografadas com segurança.

Figura 3 – Visualizador do certificado



Fonte: Microsoft (2017).

4.1 Desafio da quebra RSA

Em 18 de Março de 1991 a RSA Security LLC lançou um desafio para que pessoas pudessem tentar quebrar a criptografia RSA com chaves que variavam de 330 até 2048 dígitos binários (Leyden, 2001). Apesar de isso ter sido há muito tempo, e mesmo com uma premiação na casa de 1 milhão de reais no tempo atual, até hoje o desafio persiste e o RSA2048 bits ainda não foi quebrado.

O último que foi quebrado foi o RSA250, fato realizado pelos pesquisadores F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé e P. Zimmermann em 28 de fevereiro de 2020. A fatoração deles utilizou aproximadamente o poder computacional equivalente de 2700 core-years (Medida que equivale a uso de um núcleo de CPU continuamente durante um ano inteiro, ou uso de 356 núcleos de CPU por um dia) com um processador Intel Xeon Gold 6130 como base (Gaudry et al., 2020).

Isso mostra como o RSA é algo que mesmo ao passar dos anos ainda é um algoritmo funcional e que protege bem os dados, pois exige um gasto de poder computacional muito grande para sua quebra.

4.2 Algoritmos IFC e ECC

O RSA pertence a um tipo de criptografia chamado IFC (*Integer-Factorization Cryptography*), ou seja, criptografia por fatoração de inteiros, mas existem outros algoritmos importantes como ECDSA, EdDSA, DH e MQV que são algoritmos de criptografia do tipo ECC (*Elliptic-Curve Cryptography*), ou seja, criptografia de curva elíptica.

Durante o desenvolvimento do artigo, foi observado alguns pontos importantes sobre algoritmos do tipo IFC (como o RSA) e os tipos ECC (como ECDSA). Há algumas discussões sobre a possibilidade de sistemas que atualmente trabalhem com RSA passarem a utilizar ECDSA em breve, e isso tem algumas explicações. Uma delas, e talvez a que tenha mais força, se dá ao fator de tempo de processamento pois, segundo Barker (2020), os algoritmos que se utilizam da técnica de ECC gastam menos recurso computacional e conseguem manter níveis de segurança tão altos tanto quanto o RSA possui.

Na Tabela 1 é feita uma comparação entre os tipos IFC e ECC levando em consideração seus níveis de segurança. Ao analisar, entenda que o nível de segurança está baseado em quantias de 2^X vezes que uma operação teria de ser processada para quebrar a cifra.

Ao se utilizar um processador Intel Xeon Gold 6130 com *clock* de CPU de 3,7 Ghz, ele seria capaz de executar $3,7^{10}$ operações por segundo. Sendo assim, tomando como base um nível de segurança de 128 bits, esse processador demoraria $10^{128}/3,7^{10}$ segundos para fazer uma fatoração, o que significa que esse sistema computacional precisaria de aproximadamente $6,57*10^{104}$ anos para quebrar tal nível de segurança.

Tabela 1- Nível de segurança por tamanho de chave

Nível de Segurança	IFC	ECC
≤80	K=1024	F=160-223
112	K=2048	F=224-255
128	K=3072	F=256-383
192	K=7680	F=484-511
256	K=15360	F=512+

Fonte: Adaptado de Barker (2020).

Ao desenvolver este artigo, o tamanho mínimo de chaves para agregar segurança em sistemas que usam algoritmos IFC deve ser 2048 bits, enquanto para algoritmos ECC deve ser de 224 a 255. A linha em destaque na Tabela 1 simboliza os respectivos tamanhos considerados inseguros para o cenário tecnológico computacional atual.

Outro ponto a se observar com a tabela é a relação entre os tamanhos de chaves usados por IFC e ECC. Veja que os ECC conseguem garantir proteção igual aos IFC mesmo tendo chaves menores, ou seja, há uma diferença entre ambos quanto a velocidade de processamento.

Segundo Maletsky (2020), em nível de segurança de 128 é relatado que o IFC é dez vezes mais lento que o ECC em geração de assinatura, operação com chave privada e gerenciamento das chaves. Já com nível de segurança de 256 o RSA é de 50 a 100 vezes mais lento. Maletsky (2020) ainda complementa dizendo que a geração dos pares de chaves do IFC é de 100 a 1000 vezes mais lento se comparado com o do ECC.

Portanto, o poder computacional é um fator crítico para o sucesso e segurança de um algoritmo de criptografia. Segundo Macedo (2022), com 88% da população brasileira acessando serviços pela internet por celulares e com a crescente de dispositivos IoT (*Internet of Things*), é de se entender que esses dispositivos com poder computacional mais limitado demorem um pouco mais para acessar certos serviços que se utilizam SSL com RSA. Daí que surgem as ideias relacionadas a troca do RSA por ECDSA. Segundo matéria da CISO Advisor (2021), já existe uma recomendação de uso da ECDSA *(Elliptic Curve Digital Signature Algorithm*) junto ao protocolo SSL/TLS.

5. CONCLUSÃO

Com o desenvolvimento deste artigo, foi possível perceber que o RSA se mantém como um algoritmo muito utilizado, mesmo tendo sido concebido a mais de 45 anos atrás. Por ser ainda muito seguro, são diversos os cenários onde é aplicado e são diversas as empresas e serviços de rede que o utilizam para garantir criptografia nas suas conexões. Aos leitores recomendo uma leitura mais aprofundada de Coutinho (2015), que explica de forma didática o que é a criptografia utilizando paralelos históricos, além de descrever em detalhes a teoria matemática dos números que o RSA se apoia para agregar sua segurança e robustez.

Outro tema que despertou interesse foram os algoritmos do tipo ECC. Acredita-se que ele vem sendo cada vez mais utilizados pela sua leveza e segurança. Aos leitores talvez também seja este um assunto interessante, uma vez que, algumas fontes vêm sinalizando o ECDSA como potencial substituto ao RSA em diversos cenários, uma vez que está demonstrando conseguir os mesmos níveis de segurança com chaves menores, fator este que impacta inclusive na velocidade de sistemas criptográficos e acessos pela web.

REFERÊNCIAS

BARKER, E. ***NIST SP 800-57: Recommendation for key management: Part1-Geral***. 158. ed. Gaithersburg: NIST, Maio 2020. Disponível em: <https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final>. Acesso em: 26 set. 2023.

BINANCE ACADEMY. **Encriptação Simétrica vs. Assimétrica**. Binance Academy. 2022. Disponível em: <https://www.binance.vision/pt/security/symmetric-vs-asymmetric-encryption>. Acesso em: 31 mai. 2023.

CISO ADVISOR. **Metade dos sites ainda usa chaves criptográficas legadas**. , 10 dez. 2021. Disponível em: <https://www.cisoadvisor.com.br/metade-dos-sites-ainda-usa-chaves-criptograficas-legadas/>. Acesso em: 9 dez. 2023.

COUTINHO. S. C. **Criptografia**. Rio de Janeiro: IMPA, 2015, 217 p. Disponível em: <https://www.obmep.org.br/docs/apostila7.pdf>. Acesso em: 24 ago. 2023.

GAUDRY, P.; GUILLEVIC, A.; HENINGER, N.; THOMÉ, E.; ZIMMERMANN, P. ***Factorization of RSA-250***. 28 fev. 2020. Disponível em: <https://sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html>. Acesso em: 10 nov. 2023.

LEYDEN, J. ***RSA poses $200,000 crypto challenge***. 25 jul. 2001. Disponível em: <https://www.theregister.com/2001/07/25/rsa_poses_200_000_crypto/>. Acesso em: 8 nov. 2023.

MACEDO, S. **Smartphone é, cada vez mais, dominante no acesso à internet**. Folha de São Paulo, 25 jul. 2022. Disponível em: <https://www1.folha.uol.com.br/tec/2022/07/smartphone-e-cada-vez-mais-dominante-no-acesso-a-internet.shtml>. Acesso em: 2 fev. 2024.

MALETSKY, K. ***RSA vs. ECC Comparison for Embedded Systems***. A. ed. rev. Microchip Technology Incorporated, 2020. 6 p. ISBN 978-1-5224-5997-2. Disponível em: <https://ww1.microchip.com/downloads/en/DeviceDoc/00003442A.pdf>. Acesso em: 5 fev. 2024.

MICROSOFT. **Microsoft Teams**. 2017. Disponível em: <https://teams.microsoft.com/>. Acesso em: 6 out. 2023.

NORDVPN. ***What is RSA encryption, and how does it work?***. 31 dez. 2022. Disponível em: <https://nordvpn.com/pt-br/blog/rsa-encryption/>. Acesso em: 16 jan. 2024.

NOVAGEO SOLUTIONS. **O que é a Criptografia Assimétrica RSA**: algoritmo de chave assimétrica?. 4 ago. 2022. Disponível em: <https://www.novageo.pt/novageo/displayArticles?numero=38346&_que__criptografia_assimetrica_rsa_algoritmo_chave_assimetrica_>. Acesso em: 10 jan. 2024.

OLIVEIRA, I. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%**. CNN, 19 ago. 2022. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em: 12 out. 2023.

RASTOGI, A. ***What is the best encryption strategy for protecting your data?.*** [*S. l.*]: Encryption Consulting, 7 set. 2023. Disponível em: <https://www.encryptionconsulting.com/what-is-the-best-encryption-strategy-for-protecting-your-data/>. Acesso em: 4 mar. 2024.

RAY, D. ***Online RSA Encryption, Decryption And Key Generator Tool(Free)***. 2018. Disponível em: <https://www.devglan.com/online-tools/rsa-encryption-decryption>. Acesso em: 20 out. 2023.

RAY, D. ***RSA Encryption and Decryption in Java***. Devglan, 10 mar. 2018. Disponível em: <https://www.devglan.com/java8/rsa-encryption-decryption-java>. Acesso em: 14 fev. 2024.

UFSM. **Introdução à Criptografia**. 5 maio 2020. Disponível em: <https://www.ufsm.br/pet/sistemas-de-informacao/2020/05/05/introducao-a-criptografia>. Acesso em: 8 mar. 2024.