CRIPTOGRAFIA E SEGURANÇA CIBERNÉTICA

ENCRYPTION AND CYBERSECURITY

Lucas Henrique Vicente dos Santos[*]
Eliézer Beraldo Ribeiro[**]
Marcelo Buscioli Tenório[***]

Resumo

Este artigo examina a relevância da criptografia na segurança digital, crucial frente aos ataques cibernéticos e às exigências da LGPD. O estudo objetivou demonstrar o funcionamento prático dos algoritmos AES (Simétrico) e RSA (Assimétrico) para garantir a proteção e integridade dos dados. A metodologia incluiu análise comparativa e testes práticos com a ferramenta CyberChef. Os resultados confirmaram a eficácia de ambos os modelos na conversão de dados em códigos inacessíveis, assegurando confidencialidade e integridade. Foi validada a aplicação específica de cada método: o AES pela velocidade (para grandes volumes) e o RSA pela segurança (para troca de chaves em canais inseguros). Conclui-se que a correta implementação desses algoritmos é indispensável para o cumprimento das diretrizes da LGPD, consolidando-se como recurso fundamental na segurança dos dados.

Palavras-chave: Criptografia, Segurança, Segurança de Dados, LGPD.

Abstract

This article examines the relevance of cryptography in digital security, crucial in the face of cyberattacks and the requirements of the LGPD (Brazilian General Data Protection Law). The study aimed to demonstrate the practical functioning of the AES (Symmetric) and RSA (Asymmetric) algorithms to guarantee data protection and integrity. The methodology included comparative analysis and practical tests with the CyberChef tool. The results confirmed the effectiveness of both models in converting data into inaccessible codes, ensuring confidentiality and integrity. The specific application of each method was validated: AES for its speed (for large volumes) and RSA for its security (for key exchange in insecure channels). It concludes that the correct implementation of these algorithms is indispensable for complying with the LGPD guidelines, consolidating them as a fundamental resource in data security.

Keywords*: Encryption, Security, Data Security, LGPD.*

[*] Aluno do curso de Tecnologia em Análise e Desenvolvimento de Sistemas, da Faculdade de Presidente Prudente. Email: lucas.Santos528@fatec.sp.gov.br
[**] Aluno do curso de Tecnologia em Análise e Desenvolvimento de Sistemas, da Faculdade de Presidente Prudente. Email: eliezer.ribeiro@fatec.sp.gov.br
[***] Marcelo Buscioli Tenório, da Faculdade de Presidente Prudente. E-mail: marcelo.tenorio@fatec.sp.gov.br

1. INTRODUÇÃO

No que tange à respeito sobre a criptografia utilizada para garantir a segurança dos dados dos usuários, ou seja, nos métodos empregados para proteger as informações fornecidas por aqueles que utilizam sistemas digitais, ainda é um tema cercado de dúvidas, mesmo com toda a praticidade e velocidade que a tecnologia atual nos proporciona. Segundo Cruz, Caetano e Biff (2024, p. 4), diante disso, surgem questionamentos em relação às técnicas aplicadas para assegurar a integridade e a confidencialidade dessas informações, pois é direito do usuário conhecer de forma clara como funcionam os métodos de segurança contra os cada vez mais frequentes ataques cibernéticos.

Segundo Douglas e Freitas (2016, p.1) “Criptografia consiste em cifrar um arquivo ou mensagem usando um conjunto de cálculos. O arquivo cifrado (ou encriptado) torna-se incompreensível até que seja desencriptado”.

Neste contexto, a criptografia desempenha um papel central, garantindo que os dados sejam ilegíveis para usuários não autorizados, mesmo que eles acessem os recursos de armazenamento em nuvem (LIMA; SGARBI, 2025, p. 330).

Segundo Lima e Sgarbi (2025, p. 330), com o avanço das tecnologias digitais e a modernização dos métodos de tratamento e proteção de dados, percebeu-se que, além da rapidez e eficiência, era necessário um fator essencial: a confiabilidade no resguardo das informações, tanto pessoais quanto empresariais. Essa preocupação impacta diretamente a experiência dos usuários e especialistas que lidam diariamente com grandes volumes de dados. Desta forma, este trabalho se justifica pela importância de demonstrar de forma detalhada o funcionamento interno com os modelos de criptografia AES e RSA aplicados à segurança da informação e ao armazenamento em nuvem, destacando o porquê de sua utilização e sua relevância na proteção diária dos dados.

2. FUNDAMENTAÇÕES TEÓRICAS

2.1 Coleta e armazenamento de dados

A fase de coleta de dados é etapa onde ocorre a interação direta entre o usuário e o sistema no qual foi escolhido, por isso a coleta e armazenamento de dados no contexto de criptografia no armazenamento envolve uma série de etapas e processos fundamentais para

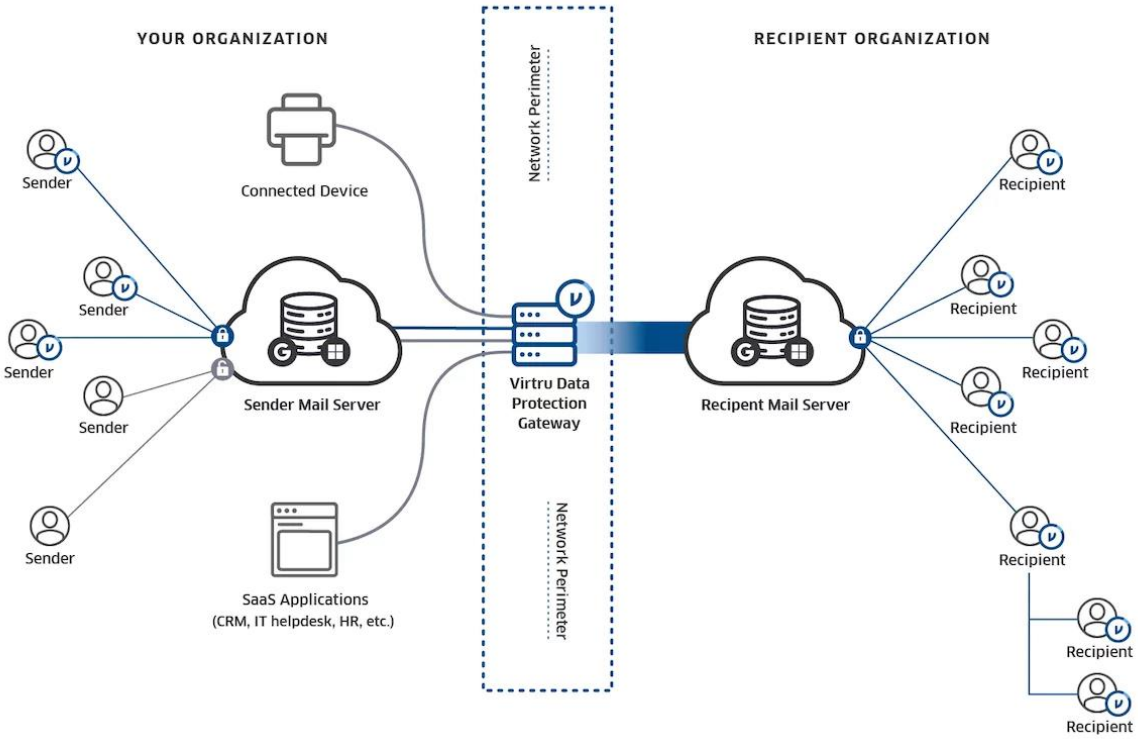
garantir que as informações sejam obtidas, armazenadas, gerenciadas e protegidas de maneira eficiente e segura (Sousa et al., 2016, p. 110).

A etapa de coleta de dados é responsável por coletar as informações fornecidas pelos usuários que podem variar de fotos, arquivos de texto, pastas, documentos e dentre outros tipos de formatos de arquivos (Lima; Sgarbi, 2025, p. 331).

A transmissão de dados é onde ocorre a criptografia desses dados fornecidos pelos usuários, assim possuindo uma maior responsabilidade em seu funcionamento, por se tratar de dados confidenciais esse mecanismo não é passível de erros em sua segurança (Rezende, 2012, p. 4).

Todos os processos da coleta de dados e armazenamento é evidenciado na figura 1, que ilustra resumidamente como é a passagem dos dados fornecidos pelos usuários, que se conecta com o servidor e é criado uma criptografia para cada dado fornecido, até a chegada no armazenamento final, que é onde os dados já tratados e criptografados ficarão armazenados na base de dados da aplicação utilizada pelo usuário.

Figura 1 - Modelo ilustrativo da passagem dos dados, do início até o final de suas etapas



Fonte: Virtru (2025)

A utilização de transações distribuídas define o controle do processamento de dados em todo ambiente de computação e tem a responsabilidade de garantir as propriedades ACID ou variações destas no ambiente (Sousa et al., 2016, p. 111).

2.2 Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018) estabelece que os dados sensíveis confiados pelos usuários a qualquer tipo de sistema de armazenamento devem ser submetidos a rigorosas normas de tratamento. Tais medidas têm como objetivo assegurar que essas informações estejam protegidas de forma eficaz contra invasões, incluindo ataques cibernéticos iniciados por indivíduos ou *softwares* mal-intencionados.

De acordo com Cruz, Caetano e Biff (2024, p.4) diz que:

> A privacidade é reconhecida como um direito básico, consagrado em leis e constituições. Dessa forma, o direito à privacidade é um princípio fundamental que protege o indivíduo contra interferências e invasões indesejadas em sua vida privada. Ele reconhece o direito das pessoas de controlar suas informações pessoais, limitar o acesso a sua intimidade e proteger sua liberdade individual.

A Lei Geral de Proteção de Dados (LGPD) busca por parâmetros e padronizações de métodos que sejam eficazes quando os dados são passados por etapas de tratamento, segundo o (GOV.BR, 2022) os 10 princípios da Lei de Proteção de dados pessoais são:

- Finalidade:

  Especificada e informada explicitamente ao titular.
- Adequação:

  À finalidade previamente acordada e divulgada.
- Necessidade:

  Do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial
- Acesso Livre:

  Fácil e gratuito das pessoas à forma como seus dados são tratados.
- Qualidade dos Dados:

  Deixando-os exatos e atualizados, segundo a real necessidade no tratamento.
- Transparência:

  Ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis.

- Segurança:

  Para coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão.

- Prevenção:

  Contra danos ao titular e a demais envolvidos.

- Não Discriminação:

  Ou seja, não permitir atos ilícitos ou abusivos.

- Responsabilização:
  Do agente, obrigado a demonstrar a eficácia das medidas adotadas.

2.3 Métodos Fundamentais da Criptografia

No processo de transmissão e tornam mais evidentes. Para mitigar essas ameaças e atender aos rigorosos princípios da Lei Geral de Proteção de Dados (LGPD), como os de Segurança e Prevenção, é imperativo aplicar técnicas que garantam a confidencialidade e a integridade das informações. A eficácia dessa proteção, no entanto, depende diretamente do método criptográfico escolhido. A criptografia moderna se baseia em duas abordagens fundamentais: a simétrica e a assimétrica. Cada uma opera com uma lógica distinta e oferece um balanço diferente entre velocidade, poder computacional e nível de segurança, sendo essencial compreendê-las para planejar uma estratégia de proteção de dados robusta.

Criptografia Simétrica

O AES (*Advanced Encryption Standard*) que é um tipo de criptografia simétrica ou também conhecida como criptografia de chave secreta foi o modelo escolhido para os futuros testes e utiliza uma única chave tanto para o processo de encriptação quanto para o de decriptação dos dados. A principal vantagem deste método é a sua alta velocidade e eficiência, o que o torna ideal para proteger grandes volumes de informação. A principal vantagem deste método é a sua alta velocidade e eficiência, sendo proporcionalmente mais rápido que algoritmos assimétricos, o que o torna ideal para proteger grandes volumes de informação (Oliveira, 2024).

No entanto, seu maior desafio de segurança reside na necessidade de compartilhar a chave secreta de forma segura entre as partes que precisam de acesso aos dados. Se a chave for interceptada, a confidencialidade das informações fica completamente comprometida, este modelo é utilizado por empresas como: *Netflix*, *Dropbox* e a *Amazon Web Services* (AWS).

Criptografia Assimétrica

Em contrapartida, o RSA (*Rivest–Shamir–Adleman*), um algoritmo de criptografia assimétrica ou de chave pública, opera com um par de chaves matematicamente interligadas uma chave pública para encriptar e uma privada para decifrar (Oliveira, 2024).

A chave pública pode ser livremente distribuída e é usada para encriptar os dados, mas apenas a chave privada correspondente, que é mantida em segredo pelo proprietário, pode decifrá-los. Este mecanismo é mais lento e exige maior poder computacional em comparação com o método simétrico. Contudo, oferece um nível de segurança muito superior para a transmissão de dados em canais inseguros, como a internet, eliminando o problema da partilha de chaves. Essa abordagem é crucial para assegurar a proteção de dados pessoais e coibir situações ilícitas como a invasão e difusão de informações, este modelo é utilizado por empresas como: *Google*, *Microsoft* e a *Apple*.

De acordo com Rezende (2012, p.5) diz que:

> Para entender o conceito, basta pensar num cadeado comum protegendo um determinado bem. A mensagem é este bem, e o cadeado, que pode ficar exposto, é a chave pública. Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem.

3. MATERIAIS E MÉTODOS

3.1 Classificação da Pesquisa e Procedimentos

Esta pesquisa classifica-se como aplicada e descritiva. Aplicada, pois demonstra o funcionamento prático dos algoritmos AES e RSA na proteção de dados, e descritiva, pois expõe as características de cada método.

Para atender aos objetivos propostos e compreender as técnicas de segurança, o estudo seguiu as seguintes etapas metodológicas:

1. **Levantamento Bibliográfico:** Estudo dos fundamentos da criptografia e da LGPD.
2. **Definição do Cenário:** Escolha da ferramenta *CyberChef* e criação de dados padronizados para teste.
3. **Execução Experimental:** Aplicação dos algoritmos simétrico e assimétrico, seguindo um protocolo rigoroso de configuração de chaves e parâmetros.
4. **Análise de Resultados:** Avaliação da eficácia com base na ilegibilidade do texto cifrado

(confidencialidade) e na recuperação exata do texto original (integridade).

3.2 Ferramenta e Dados Utilizados

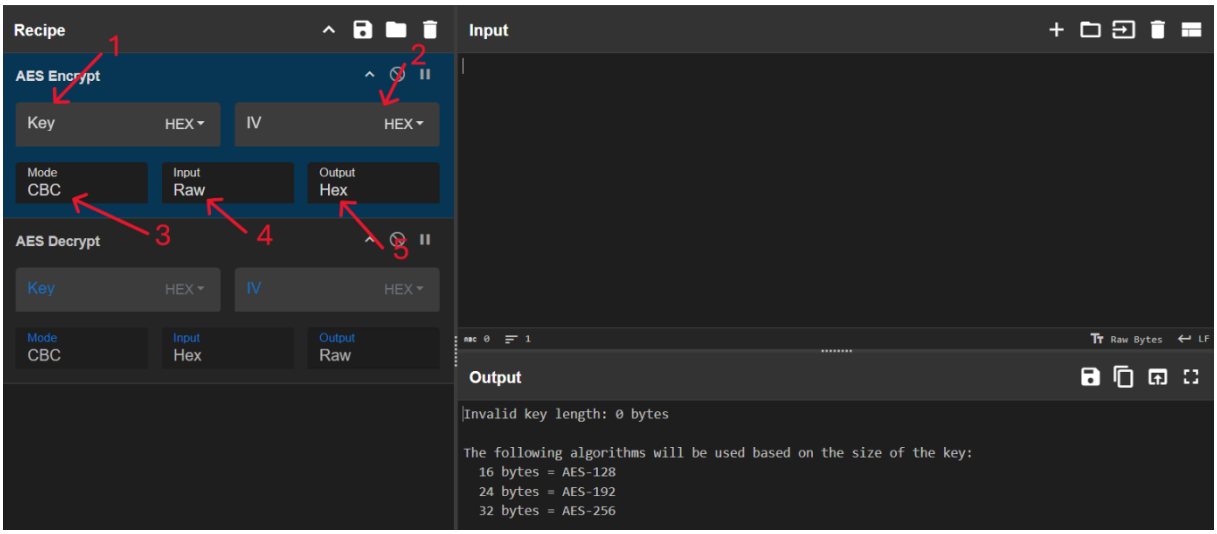
A ferramenta utilizada para os testes foi o CyberChef, um recurso web que permite a manipulação de diversos tipos de criptografia. O CyberChef consiste em escolher um modelo existente e preencher os dados necessários para que a cifragem e a decifragem ocorram.

Como massa de dados para os testes, utilizou-se a frase "Teste de Criptografia para o TCC", simulando uma informação confidencial que necessita de proteção contra acesso não autorizado.

3.3 Categoria de Criptografia: Simétrica (AES)

Para a avaliação da criptografia simétrica, utilizou-se o algoritmo AES (*Advanced Encryption Standard*). O processo foi dividido em duas fases: encriptação e decriptação, conforme detalhado a seguir.

Figura 2 - Passo a passo de como preencher os dados do modelo de criptografia AES.



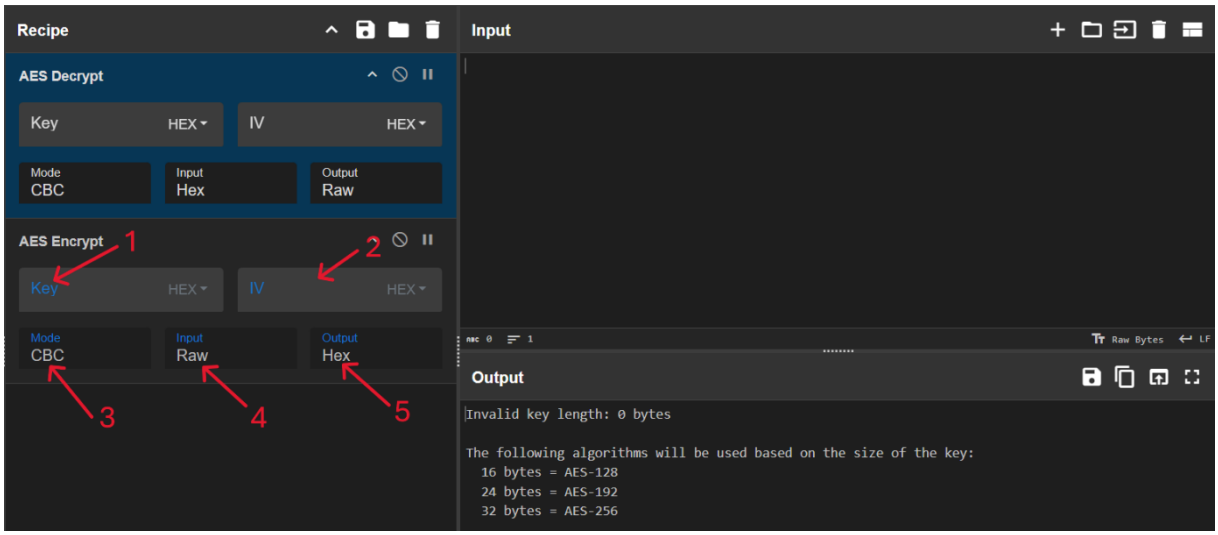
Elaborada pelos autores (2025)

1. **Definir a Chave:** No campo *Key*, inseriu-se a senha ou segredo. O formato foi definido

como *Hex* (hexadecimal).

2. **Vetor de Inicialização (IV):** Preencheu-se o campo IV. Este valor é fundamental para garantir que cada criptografia produza um resultado diferente, adicionando aleatoriedade.
3. **Modo de Operação:** No menu *Mode*, selecionou-se a opção **CBC** (*Cipher Block Chaining*), ideal para evitar padrões repetidos na mensagem.
4. **Formato de Entrada:** No menu *Input*, escolheu-se a opção **Raw**, garantindo que a mensagem seja tratada como dados brutos.
5. **Formato de Saída:** No menu *Output*, selecionou-se a opção **Hex**, resultando em uma sequência de caracteres hexadecimais.

Figura 3 - Passo a passo de como preencher os dados do modelo de descriptografia AES.



Elaborada pelos autores (2025)

1. **Inserir a Chave:** No campo *Key*, inseriu-se a mesma chave secreta utilizada anteriormente, mantendo o formato *Hex*.
2. **Inserir o Vetor de Inicialização (IV):** Inseriu-se o mesmo valor de IV da etapa de criptografia.
3. **Selecionar o Modo de Operação:** Selecionou-se novamente a opção **CBC**.
4. **Formato de Entrada:** No menu *Input*, selecionou-se **Hex**, informando que a entrada é a mensagem criptografada em hexadecimal.
5. **Formato de Saída:** No menu *Output*, escolheu-se **Raw**, para que o resultado fosse exibido

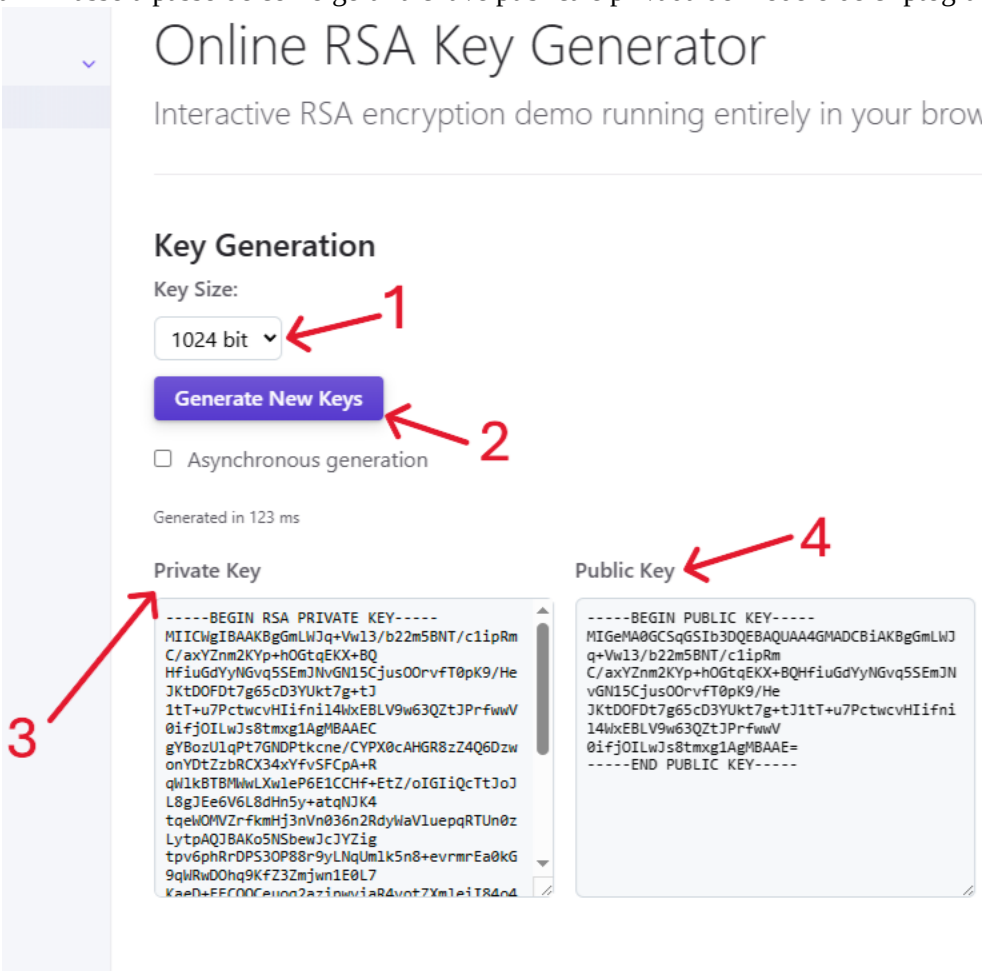
como texto legível.

3.4 Categoria de criptografia: Assimétrica

Para a categoria assimétrica, utilizou-se o algoritmo RSA, que opera com um par de chaves (pública e privada).

Geração das Chaves: A Figura 4 apresenta a ferramenta utilizada para a geração das chaves (*Online RSA Key Generator*).

Figura 4 - Passo a passo de como gerar a chave pública e privada do modelo de criptografia RSA



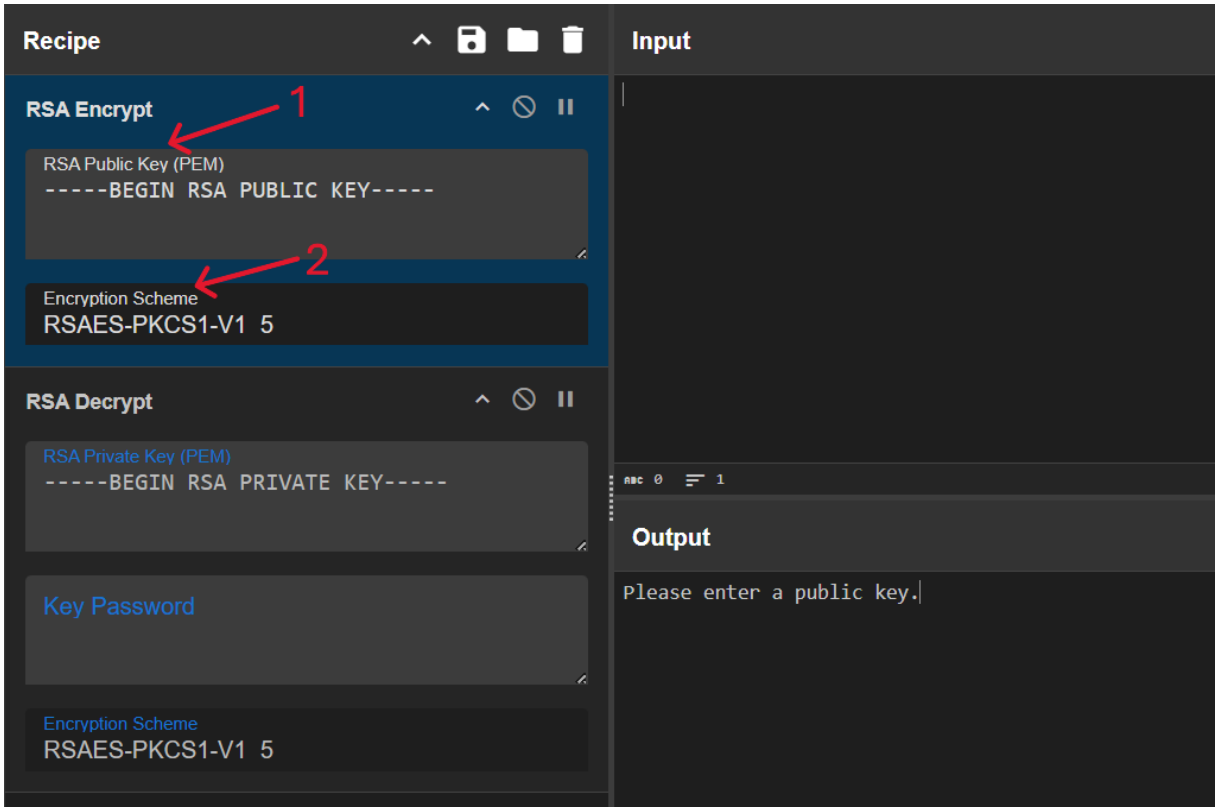
Elaborada pelos autores (2025)

Os parâmetros definidos foram

1. ***Key Size*:** Definiu-se o tamanho da chave em 1024bit, o utilizado para teste foi de 1024 bit.
2. ***Generate new key*:** Utilizou-se a opção Generate New Keys para criar o par de chaves

3. ***Private Key*:** É o campo onde se encontra a chave privada do modelo RSA,
4. ***Public Key*:** É o campo onde se encontra a chave pública do modelo RSA.

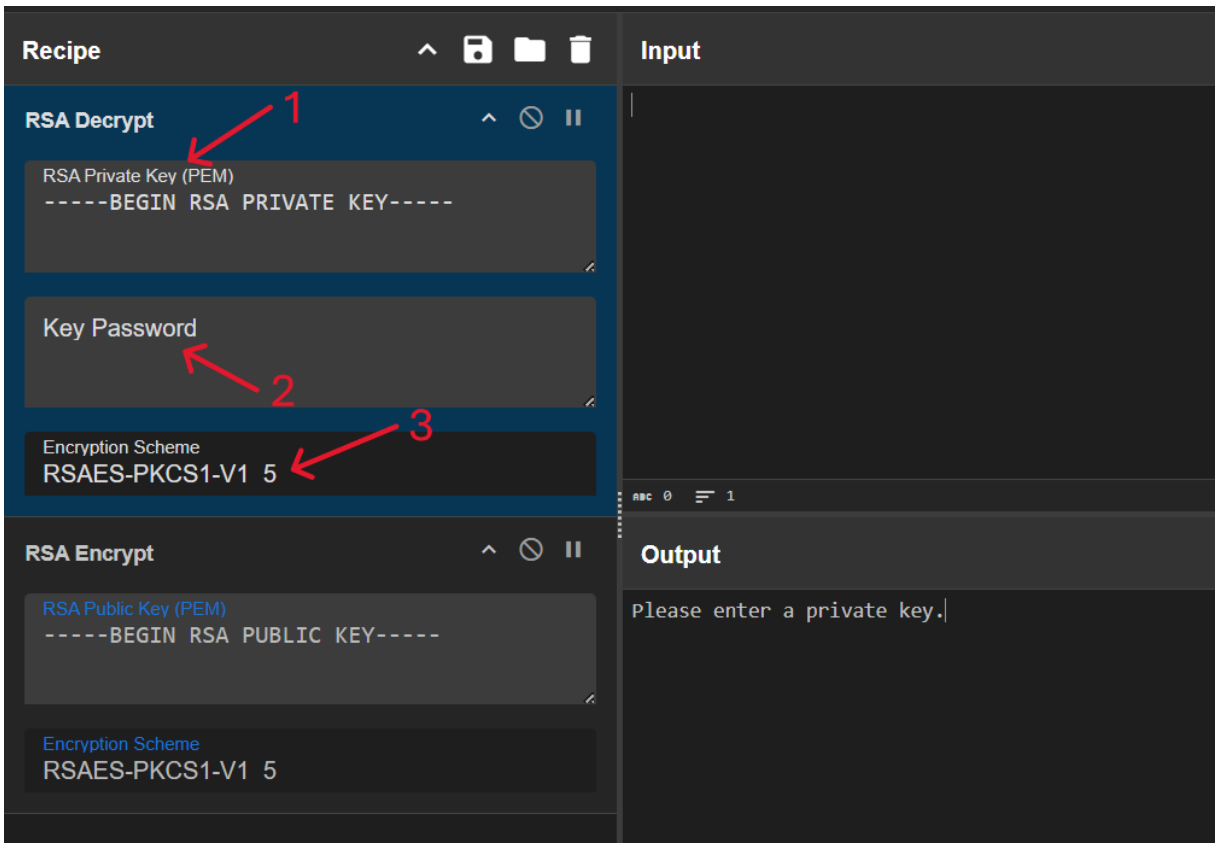
Figura 5 - Passo a passo de como preencher os dados do modelo de criptografia RSA



Elaborada pelos autores (2025)

1. **Inserir a Chave Pública:** No campo *RSA Public Key (PEM)*, colou-se a chave pública gerada anteriormente, respeitando o formato PEM, incluindo as linhas de início (-----*BEGIN RSA PUBLIC KEY*-----) e fim (-----*END RSA PUBLIC KEY*-----).
2. **Selecionar o Esquema de Criptografia:** No menu *Encryption Scheme*, escolheu-se o padrão **RSAES-PKCS1-v1_5**, uma opção comum para garantir a robustez da criptografia.

Figura 6 - Passo a passo de como preencher os dados do modelo de descriptografia RSA



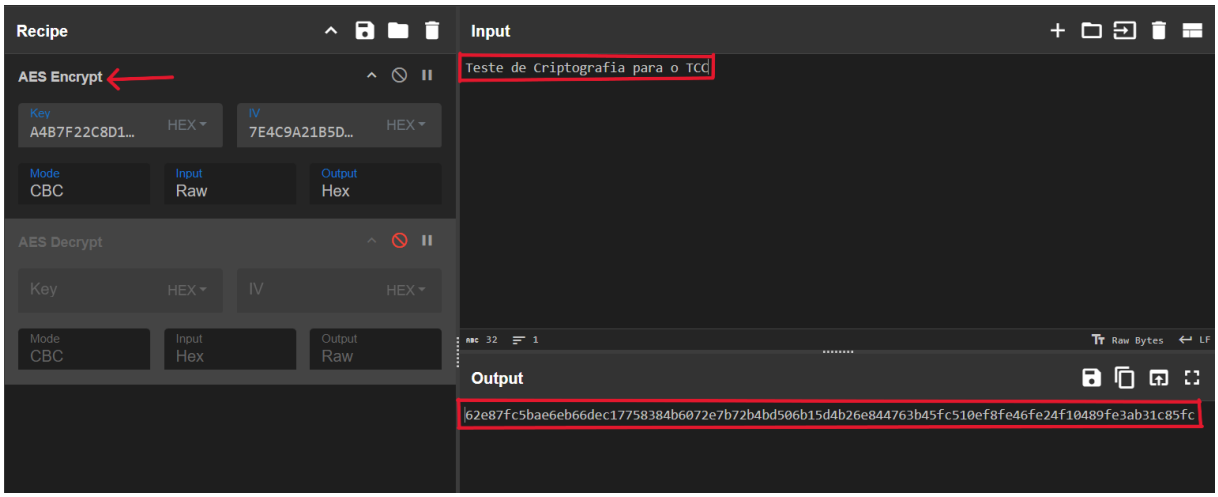
Elaborada pelos autores (2025)

1. **Inserir a Chave Privada:** Colou-se a chave privada no campo *RSA Private Key (PEM)*.
2. **Senha da Chave (Se aplicável):** O campo *Key Password* foi deixado em branco, pois a chave gerada não possuía proteção por senha.
3. **Esquema de Criptografia:** Selecionou-se exatamente o mesmo padrão utilizado na criptografia (**RSAES-PKCS1-v1_5**) para evitar falhas no processo.

4. RESULTADOS E DISCUSSÕES

Seguindo o passo a passo que foi mostrado anteriormente podemos obter os seguintes resultados que estão presentes na figura 8 e 9, que representa o modelo de criptografia simétrica, assim demonstrando também a criptografia e descriptografia do texto inserido no campo *input* e o resultado que saí no campo *output*:

Figura 7 - Resultado da criptografia AES utilizando o modelo simétrico

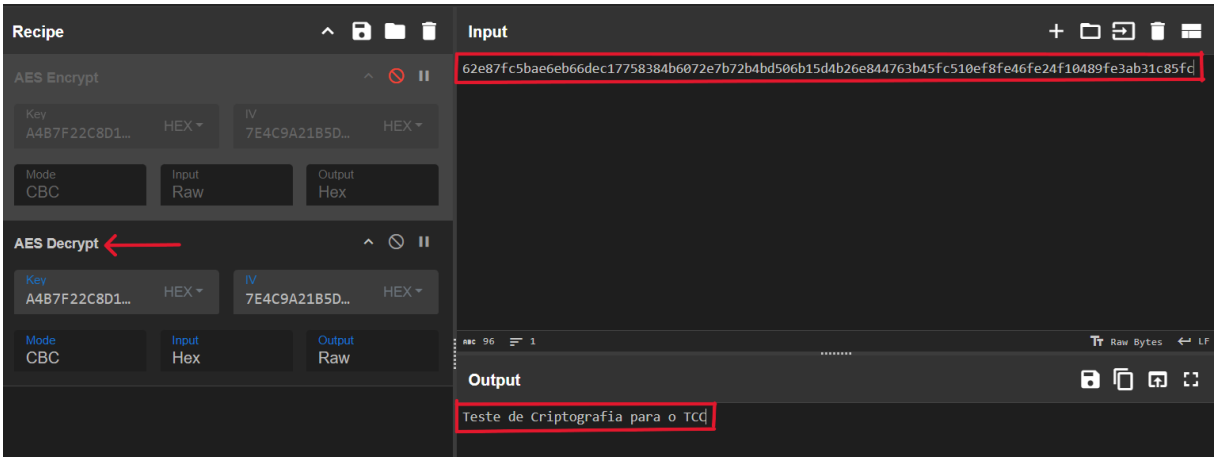


Elaborada pelos autores (2025)

Percebe-se que, após a inserção correta dos dados necessários para a realização da criptografia, a frase que foi escrita no campo do *Input* está completamente criptografada por meio do modelo simétrico, como mostrado anteriormente.

Nota-se as características desse modelo de criptografia, como possuem a aleatoriedade de números e letras em diferentes posições, o que tem como objetivo dificultar o acesso por pessoas não autorizadas e *softwares* mal-intencionados.

Figura 8 - resultado da descriptografia AES utilizando o modelo simétrico



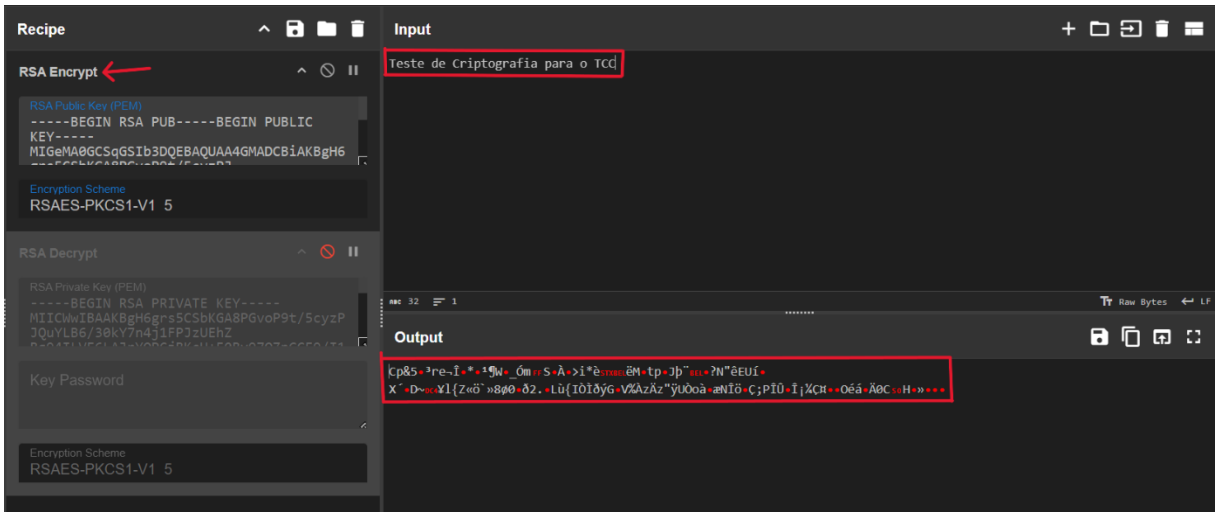
Elaborada pelos autores (2025)

Após a troca do modelo de AES *encrypt* para AES *decrypt* e copiarmos e colarmos a criptografia gerada anteriormente, percebe-se que o texto gerado é o mesmo do anterior, ou

seja, mesmo após a criptografia o texto não perdeu as suas características, mantendo assim a integridade e segurança dos dados.

Nas Figuras 10 e 11, apresentam-se os resultados obtidos após a execução do passo a passo descrito anteriormente, desta vez evidenciando o processo de criptografia e descriptografia pelo algoritmo RSA, que se baseia no modelo de criptografia assimétrica, utilizando uma chave pública e uma chave privada.

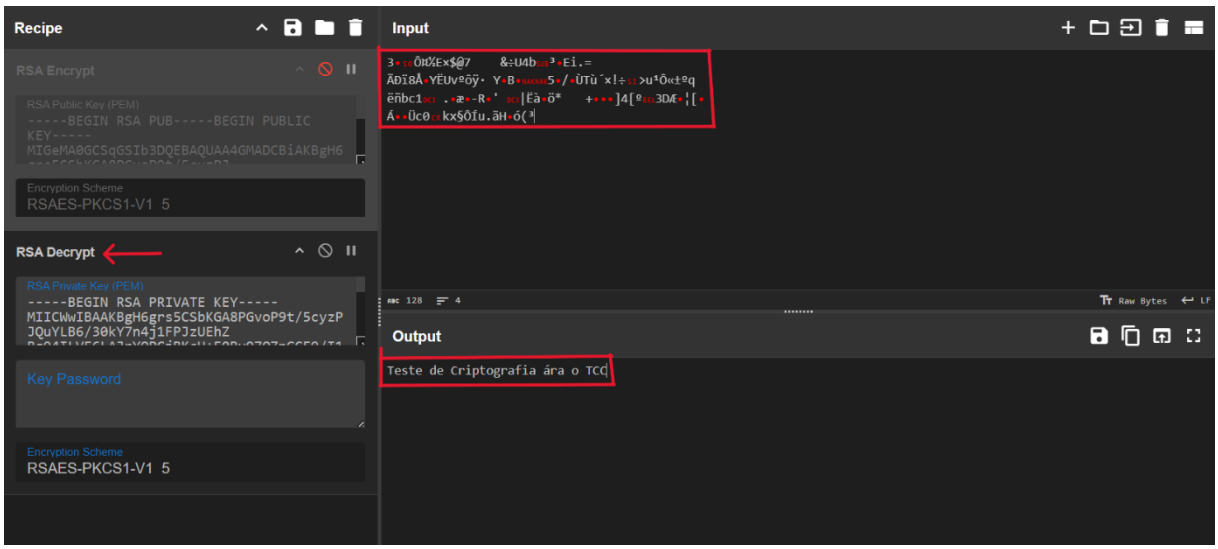
Figura 9 - Resultado da criptografia RSA utilizando o modelo assimétrico



Elaborada pelos autores (2025)

Nota-se que o modelo de criptografia assimétrico é totalmente diferente em sua estrutura principal, combinando não apenas letras e números em localizações aleatórias e sim também caracteres especiais em sua composição, isso ocorre pelo fato de que quando o modelo assimétrico é realizado, ele em base64 ou hexadecimal os caracteres podem se tornar símbolos variados.

Figura 10 - Resultado da descriptografia RSA utilizando o modelo assimétrico



Elaborada pelos autores (2025)

Realizado a troca do RSA *encrypt* para o RSA *decrypt* e inserido o conteúdo da criptografia gerada anteriormente para o campo *input*, nota-se que os dados não foram corrompidos por causa da criptografia, assim também mantendo a integridade e segurança dos dados como no modelo anterior, porém utilizando de métodos diferentes.

5. CONSIDERAÇÕES FINAIS

Este estudo teve como propósito evidenciar a relevância da criptografia como elemento central da segurança digital, especialmente diante do aumento constante de ataques virtuais e da aplicação da Lei Geral de Proteção de Dados (LGPD). Ao longo da pesquisa, verificou-se que a meta de compreender e demonstrar o funcionamento prático dos métodos criptográficos simétricos (AES) e assimétricos (RSA) foi alcançada, revelando a aplicabilidade de cada um em diferentes cenários de proteção de dados.

Os experimentos conduzidos com a ferramenta CyberChef possibilitaram visualizar de forma objetiva como o uso adequado de chaves e parâmetros que assegura a confidencialidade e a integridade das informações, convertendo dados legíveis em códigos ininteligíveis para agentes não autorizados. A análise reforçou que, quando bem implementada, a criptografia não apenas resguarda os dados contra acessos indevidos, mas também se consolida como recurso fundamental para o cumprimento dos princípios da LGPD.

No entanto, é importante ressaltar as limitações deste trabalho. A pesquisa concentrou-se em uma abordagem demonstrativa e funcional utilizando uma ferramenta baseada na web

CyberChef, sem o objetivo de realizar análises quantitativas aprofundadas sobre o desempenho computacional (uso de CPU e tempo de processamento) dos algoritmos em grandes volumes de dados. Além disso, o cenário de testes utilizou cadeias de caracteres simples, não abrangendo a complexidade da gestão de chaves em ambientes de produção real ou a integração com bancos de dados corporativos.

Como sugestão para trabalhos futuros, propõe-se a implementação destes algoritmos (AES e RSA) utilizando linguagens de programação de alto nível, como Python ou Java, para a realização de benchmarks de desempenho e consumo de recursos. Outra vertente de pesquisa relevante seria a análise de algoritmos de Criptografia de Curva Elíptica (ECC), que oferecem segurança equivalente ao RSA com chaves menores, bem como o estudo sobre o impacto da computação quântica na quebra das criptografias atuais e as novas soluções de criptografia pós-quântica.

Conclui-se, portanto, que a criptografia é um dos pilares da segurança da informação, sendo indispensável tanto em ambientes pessoais quanto corporativos. Sua aplicação adequada, ciente de suas características e evoluções, favorece a preservação da privacidade, a redução de riscos e o fortalecimento da confiança em soluções digitais.

REFERÊNCIAS

ABDULLAH, Ako. **Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data**: *subtítulo*. 2017. Trabalho de Conclusão de Curso (Department of Applied Mathematics & Computer Science) – Eastern Mediterranean University, Cyprus. MSc in Computer Science – UK, 2017. Disponível em: https://www.researchgate.net/profile/Ako-Abdullah/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data/links/59437cd8a6fdccb93ab28a48/Advanced-Encryption-Standard-AES-Algorithm-to-Encrypt-and-Decrypt-Data.pdf. Acesso em: 05 dez. 2025.

BRASIL (SERPRO). **Princípios da LGPD**. GOV.BR (Portal do Governo Brasileiro), publicado em 30 abr. 2021; atualizado em 26 jul. 2022. Disponível em: https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd Acesso em: 05 dez. 2025.

CARVALHO, Állan; FREITAS, Ântonio, **Análise de criptografia e quebra de senhas utilizando *softwares* livres**. Universidade Federal de São João del-Rei, 2016. Disponível em: https://www.ufsj.edu.br/portal2-repositorio/File/ctele/TCC/2016/Allan%20Douglas%20Porto%20de%20Carvalho.pdf. Acesso em: 05 dez. 2025.

CRUZ, Caio Vinícius; CAETANO, Felipe de Oliveira; BIFF, Larissa de Oliveira. **Lei Geral da Proteção de Dados**: fundamentos e impactos jurídicos. Repositório Institucional do IFES, 2024. Artigo acadêmico. Disponível em: https://repositorio.ifes.edu.br/bitstream/handle/123456789/4375/Artigo%20Lei%20Geral%20da%20Prote%C3%A7%C3%A3o%20de%20Dados.pdf. Acesso em: 05 dez. 2025.

GCHQ. **CyberChef**: The Cyber Swiss Army Knife. Disponível em: https://gchq.github.io/CyberChef/. Acesso em: 05 dez. 2025.

OLIVEIRA, Jailton Mendes. **Verificação da segurança da criptografia AES e RSA em relação ao tamanho das chaves**. 2024. 65 f. Trabalho de Conclusão de Curso (Tecnologia em Informática para Negócios) – Faculdade de Tecnologia de Mauá, Centro Paula Souza, Mauá, 2024. Disponível em: http://ric-cps.eastus2.cloudapp.azure.com/bitstream/123456789/20982/1/informaticaparanegocios_2024_1_jailtonmendesoliveira_verificacaodasegurancadacriptografia.pdf .Acesso em: 07 dez. 2025.

LIMA, Valdenilson dos Santos; SGARBI, Elielson Antonio. ABORDAGENS E DESAFIOS DA SEGURANÇA NA COMPUTAÇÃO EM NUVEM: criptografia, privacidade e controle de acesso. **Revista Interface Tecnológica**, Taquaritinga, SP, v. 21, n. 2, p. 329–342, 2025. DOI: 10.31510/infa.v21i2.2142. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/2142. Acesso em: 6 dez. 2025.

REZENDE, Ronielton. **Criptografia simétrica e assimétrica**: Os principais algoritmos de cifragem. Faculdade Novos Horizontes – Belo Horizonte, 2012. Disponível em: https://www.researchgate.net/publication/303367222_Criptografia_simetrica_e_assimetrica_os_principais_algoritmos_de_cifragem Acesso em: 05 dez. 2025.

SOUSA, Luciano M.; MOREIRA, Luan C.; MACÊDO, Davi F.; MACHADO, João C. Transações distribuídas. In: SOUSA, Luciano M. (org.). **Introdução à Computação em Nuvem**. Porto Alegre: Sociedade Brasileira de Computação, 2016. E-book. Disponível em: https://books-

sol.sbc.org.br/index.php/sbc/catalog/download/18/81/167?inline=1 .Acesso em: 14 jul. 2025.

TIDWELL, Travis. **Online RSA *Key Generator***. Disponível em: https://travistidwell.com/jsencrypt/demo/. Acesso em: 05 dez. 2025.

VIRTRU. **Virtru Data Gateway**. Virtru, 2025. Disponível em: https://www.virtru.com/data-security-platform/virtru-data-gateway. Acesso em: 06 dez. 2025.