ESCOLA DE SARGENTOS DAS ARMAS

ESCOLA SARGENTO MAX WOLF FILHO

CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DE COMUNICAÇÕES MILITARES

CRIPTOGRAFIA RSA: funcionamento e emprego no Exército Brasileiro

Daniel Pereira Alves Redígolo Ferreira
João Victor Venâncio Bondi
Maicon Pietro Pereira Santana de Carvalho
Bruno Barbosa Henrique Lima
Luiz Gabriel Almeida Ferreira
Wesley da Motta Oliveira
Ícaro Morales de Souza

TRÊS CORAÇÕES – MG
2022

Daniel Pereira Alves Redígolo Ferreira
João Victor Venâncio Bondi
Maicon Pietro Pereira Santana de Carvalho
Bruno Barbosa Henrique Lima
Luiz Gabriel Almeida Ferreira
Wesley da Motta Oliveira
Ícaro Morales de Souza

CRIPTOGRAFIA RSA: funcionamento e emprego no Exército Brasileiro

Trabalho Científico do Curso Superior de Tecnologia em Comunicações apresentado à Escola de Sargentos das Armas como requisito para a obtenção do grau de Tecnólogo em Ciências Militares.

Orientador: 1°Tenente Israel Soares De Oliveira

Área de concentração: Ciências Militares

TRÊS CORAÇÕES – MG

2022

FOLHA DE APROVAÇÃO

Daniel Pereira Alves Redígolo Ferreira
João Victor Venâncio Bondi
Maicon Pietro Pereira Santana de Carvalho
Bruno Barbosa Henrique Lima
Luiz Gabriel Almeida Ferreira
Wesley da Motta Oliveira
Ícaro Morales de Souza

CRIPTOGRAFIA RSA: funcionamento e utilidades para o Exército Brasileiro

Trabalho Científico do Curso Superior de Tecnologia em Comunicações apresentado à Escola de Sargentos das Armas como requisito para a obtenção do grau de Tecnólogo em Ciências Militares.

APROVADO EM (DIA) DE (MÊS) 2022.

BANCA EXAMINADORA

_____

1° Ten Israel Soares de OLiveira

_____

Posto/Graduação [nome do professor(a) avaliador(a)] (Metodologia)

_____

Posto/Graduação [nome do professor(a) avaliador(a)] (Português)

RESUMO

Imagine um indivíduo tendo todas suas informações, incluindo senhas de banco, contas de redes sociais e conversas privadas, violadas ou subtraídas com a finalidade de obter vantagens sobre suas informações. Casos assim não são raros de acontecer e existem métodos de segurança da informação capazes de impedir que esse tipo de situação ocorra. Em vista disso, este projeto irá apresentar um método específico de proteção de dados que é conhecido como método RSA (Rivest-Shamir-Adleman). Criado no final da década de 1970, em que a sigla RSA faz referência aos criadores Rivest-Shamir-Adleman que criaram a criptografia a partir de chaves públicas e privadas. Este sistema de segurança utiliza chaves assimétricas e é amplamente utilizado atualmente, inclusive pelo Exército Brasileiro, por ser um dos métodos mais seguros para utilização de criptografia, já que, com cálculos matemáticos, criptografa a chave pública e decriptografa utilizando a chave privada, seja uma mensagem privada, dados de bancos, informações de redes. A definição de chave, nesse caso, pode ser comparada a uma porta em que de um lado é a mensagem legível e, do outro lado, a mensagem criptografada. A chave pública é de acesso a todos, ou seja, qualquer um pode criptografar uma mensagem utilizando a chave pública, porém somente utilizando a chave privada poderá decodificar essa mensagem, tendo seu acesso restrito a uma pessoa, instituição, etc.

Palavras-chave: criptografia. RSA. Segurança da informação. Criptografia RSA. Chave assimétrica. Chave assimétrica. Chave pública. Chave privada.

ABSTRACT

Imagine an individual having all of their information, including bank passwords, social media accounts and private conversations, breached or subtracted for the purpose of taking advantage of their information. Cases like this are not uncommon and there are information security methods capable of preventing this type of situation from happening. In view of this, this project will present a specific method of data protection which is known as RSA method (Rivest-Shamir-Adleman). Created in the late 1970s, the acronym RSA refers to the creators Rivest-Shamir-Adleman who created encryption from public and private keys. This security system uses asymmetric keys and is currently widely used, including by the Brazilian Army, as it is one of the safest methods for using cryptography, since, with mathematical calculations, it encrypts the public key and decrypts it using the private key, be it a private message, bank data, network information. The key definition in this case can be compared to a port where on one side is the readable message and on the other side is the encrypted message. The public key is accessible to everyone, that is, anyone can encrypt a message using the public key, but only using the private key can decode this message, with access restricted to a person, institution, etc.

Keywords: cryptography. RSA. Information security. RSA encryption. Asymmetric key. Asymmetric key. Public key. Private key.

LISTA DE SIGLAS

RSA Rivest–Shamir–Adleman

SUMÁRIO

1. INTRODUÇÃO

A tecnologia é uma fiel aliada da evolução do ser humano e, em consequência disso, a internet veio para facilitar os meios de comunicação e afazeres do dia a dia (WILLIAN, 2019). Entretanto, para que esses benefícios sejam desfrutados de forma adequada é preciso um sistema de segurança que proteja os usuários de invasores. Este projeto tem por objetivo explanar a criptografia Rivest-Shamir-Adleman (RSA) que está em vigor atualmente nos meios de comunicação, seja em e-mails, internet, redes sociais e rádios militares. Em um primeiro momento, deve-se conceituar o que é a criptografia. A criptografia é a técnica utilizada para proteger informações de maneira que um número reduzido de pessoas tenha

> acesso a elas. Com o avanço da tecnologia, compartilhar informações pessoais ficou mais acessível. Porém, ataques a essas informações se tornaram frequentes, o que obriga a fazer o uso da criptografia. Voltando ao passado, as primeiras criptografias utilizadas pelo ser humano foram observadas nos povos antigos como os espartanos e romanos, que fizeram uso de cifras criptográficas em suas trocas de mensagens (CRYPTOID, 2015).

Embora não se saiba exatamente a primeira utilização da criptografia, existem relatos históricos abordando esse assunto e um desses relatos de criptografia documentado foi há cerca de 1900 a.C. numa vila Egípcia, composta por códigos e palavras substituídas por outras (Fiarresga, 2010).

Scytale, um bastão de madeira, era utilizado pelos gregos e espartanos para transmitir mensagens secretas entre comandantes militares. Consistia em enrolar um pedaço de tecido ou couro no tamanho desse bastão e escrever a mensagem. Após isso, era desenrolada e enviada por um mensageiro até o destinatário, o qual deveria ter o bastão de mesmo tamanho para novamente enrolar a mensagem e conseguir ter acesso à informação (COSTA, 2014).

Já na idade contemporânea, especificamente, na Segunda Guerra Mundial, a temida máquina enigma era uma preocupação para os aliados. A máquina foi desenvolvida pelo engenheiro alemão Arthur Scherbius no final da Primeira Guerra Mundial para uso civil que, posteriormente, foi utilizada como máquina de guerra (WILLIAN, 2019). Consistia em 26 teclas com sinais do alfabeto que eram embaralhadas por 3 rotores, cada rotor com 26 anéis envolvendo as letras do alfabeto. Ou seja, havia inúmeras combinações possíveis para serem organizadas de forma criptografada.

Atualmente, existem diversos tipos de criptografia. Algumas delas funcionam com chaves (simétrica e assimétrica) e bits, e sua segurança é definida pela quantidade de bits, ou seja, quanto mais bits, mais difícil será de romper o sistema criptográfico (RankMyApp, 2021). São exemplos desses tipos de criptografia a Data Encryption Standard (DES), o Triple DES, Advanced Encryption Standard (AES), Camellia, Rivest-Shamir-Adleman (RSA), entre outras (CRYPTID, 2019)

Como dito anteriormente, o método RSA será analisado neste projeto de pesquisa. A sigla RSA diz respeito aos criadores desse método de proteção (Ron Rivest, Adi Shamir e Leonard Adleman), que no final da década de 1970, desenvolveram esse método de segurança da informação, pois até então era usada a criptografia simétrica que, foi quebrada com a técnica da força bruta, ou seja, um programa feito para testar as possibilidades de combinações por horas (ALBORS, 2020). Para a codificação e decodificação das mensagens, a criptografia RSA emprega a teoria dos números, utilizando-se de chaves assimétricas e distintas (pública e privada). Uma chave pública está disponível para todos e pode ser usada para criptografar uma mensagem e enviá-la ao proprietário de uma chave privada , que será a única pessoa capaz de decriptografá-la.

Seguindo essa mesma linha de raciocínio, com o avanço tecnológico, diversas informações são enviadas e recebidas todos os dias. Com isso, formas de segurança foram surgindo para que esse tráfego de mensagens fosse mais seguro, tendo em vista que cada assunto pessoal ou coletivo se torna sigiloso para um grupo de pessoas. Logo, torna-se necessário um trabalho científico para explicar a criptografia RSA e seu funcionamento de uma maneira simples e didática, com a finalidade de fornecer informações às pessoas que queiram se familiarizar com o assunto, comprovando sua eficácia e para dar a elas confiança para utilizar tal método.

Para isso, este projeto visa explanar o modo de funcionamento de uma criptografia específica, pois é amplamente utilizada atualmente por conta da grande dificuldade de obter êxito na decodificação (BONFIM, 2017), cujos dados necessitem de sigilo, significando, assim, manter a confidencialidade, integridade e disponibilidade (KIM; SOLOMON, 2014). Ademais, é importante, também, para o Exército para transmissão e

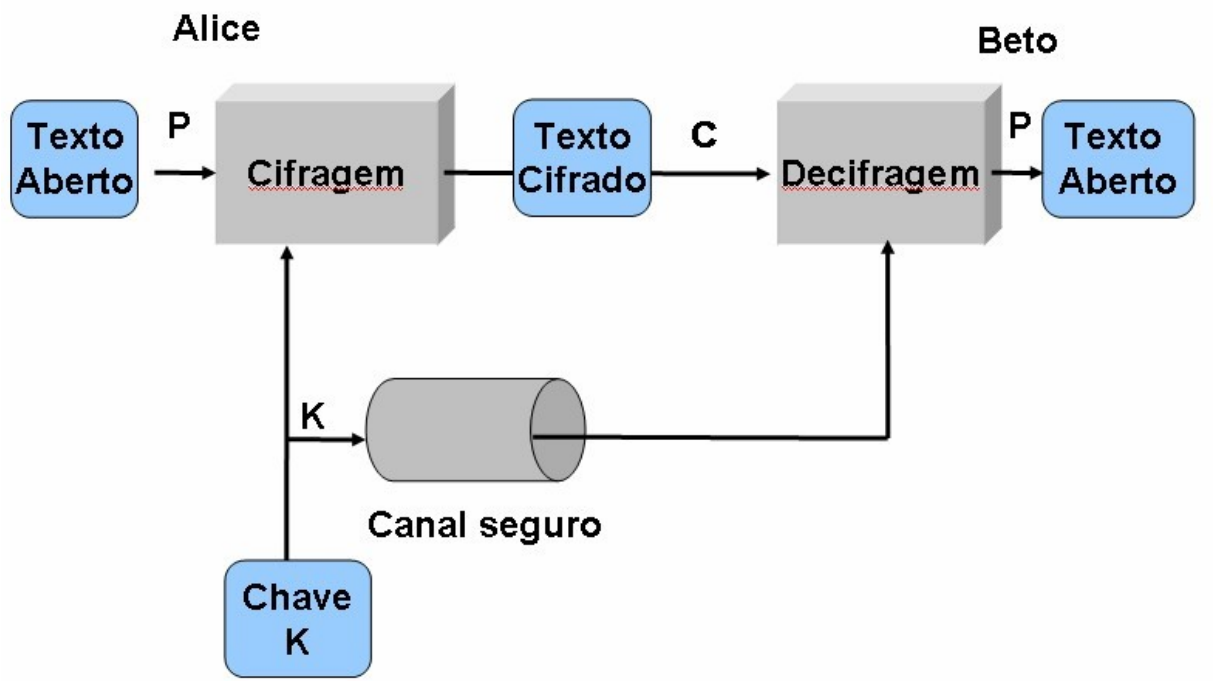
recepção de dados sigilosos. Portanto, faz-se relevante o estudo desse assunto pois codificar uma informação e saber como o processo funciona se reflete na confiabilidade ao utilizar a criptografia RSA.

2. DESENVOLVIMENTO

2.1 REFERENCIAL TEÓRICO

A criptografia é um mecanismo de segurança e privacidade que torna alguns tipos de comunicação (textos, imagens, vídeos, etc) incompreensíveis para quem não tem acesso aos códigos de "tradução" da mensagem. Em um processo genérico de criptografia, devem ser observados alguns aspectos para melhor entendimento. Um texto em claro (legível) é escrito pelo remetente da mensagem com a finalidade de contatar o destinatário. Porém o canal (que liga os dois interlocutores) é considerado inseguro e, para isso, o remetente cifra a mensagem utilizando um algoritmo de cifração para que o canal se torne seguro. Além do algoritmo, existe a chave de cifração. A utilização da chave é necessária pois considera-se que o algoritmo seja algo fixo (geralmente um padrão de mercado) e a chave seja o parâmetro variável que mudará de processo a processo ou de usuário a usuário. Ao chegar a mensagem no destinatário, é utilizado a chave de decifração para obter um texto legível.

Processo de criptografia

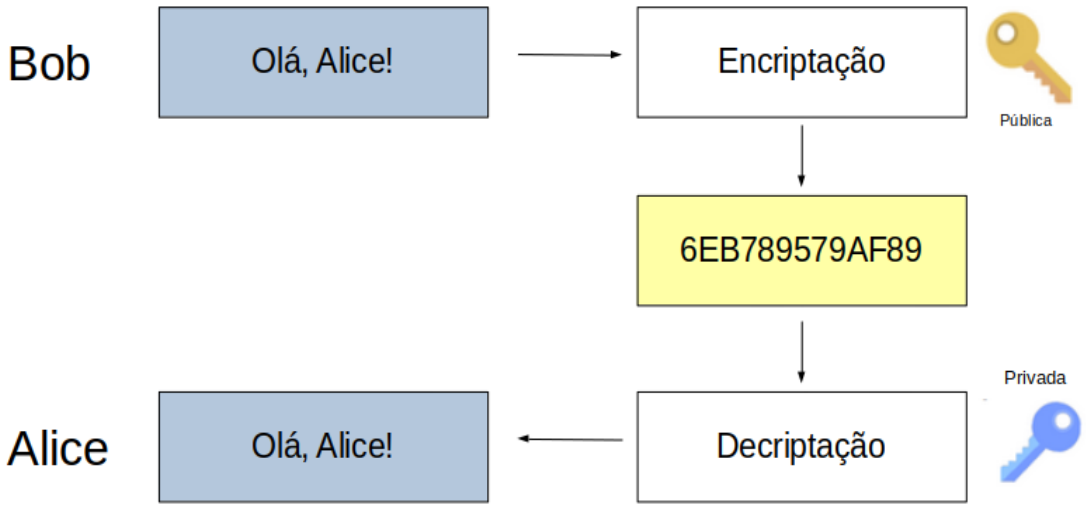


Fonte: Aulas de moz

Logo, emergindo ao assunto existem dois tipos de criptografia, cada uma com características, vantagens e desvantagens: criptografia simétrica e criptografia assimétrica. A criptografia simétrica é, basicamente, usada apenas uma chave para cifrar e decifrar o texto e essa chave deve ser compartilhada entre o remetente e o destinatário, já a assimétrica é usada uma chave para o ciframento e uma outra para deciframento. Em vista disso, manifestando um contexto histórico do surgimento da criptografia Rivest-Shamir-Adleman (RSA) e o motivo da criptografia ser a mais utilizada em meios de comunicações, analisando seu funcionamento, infere-se que foi desenvolvida a RSA, a qual foi criada por R. Rivest, A. Shamir e L. Adleman em 1977. Foi o primeiro algoritmo a usar a técnica Diffie-Hellman, usando criptografia assimétrica. O RSA envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Quando algo é cifrado com uma das chaves, somente a outra chave do par poderá ser utilizada para decifrar o dado. Tendo em vista isso, podemos

garantir confidencialidade, autenticidade, integridade e não-repúdio daquilo que foi criptografado (KIM; SOLOMON, 2014). A criptografia RSA utiliza números primos em seu funcionamento matemático enormes, na casa dos 10^{100} e atua diretamente na internet, por exemplo, em mensagens de e-mails, em compras on-line entre outros; tudo isso é encriptado e decriptado pela criptografia RSA.

Processo de encriptação usando chave assimétrica



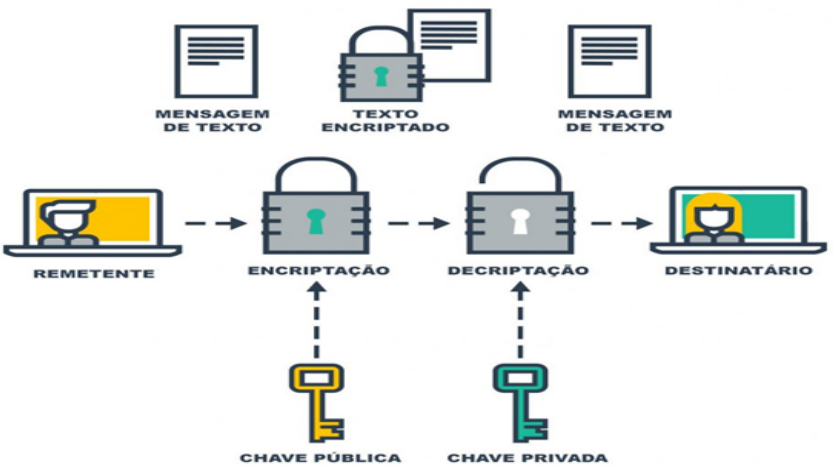
Fonte: Fernando Souza (2020)

Tendo em vista a figura acima, o remetente deve criptografar o texto claro com a chave pública do destinatário (esta chave é de domínio público e, assim, o remetente também a possui), o resultado é enviado para o destinatário, que utilizando a sua chave privada para decriptografar, será o único a ter acesso ao documento. Então, mesmo tendo acesso a chave pública, é inviável decifrar a mensagem, já que só é possível com a chave privada do destinatário a qual somente ele tem acesso.

Há dois aspectos a serem explanados com relação à criptografia RSA. O primeiro aspecto é que não há a necessidade de compartilhamento de segredo igual a criptografia assimétrica, pois a chave pública pode ser compartilhada sem riscos de perda de sigilo nas conexões, visto que o que for cifrado com ela somente poderá ser decifrado com a chave privada correspondente. O outro fator de análise é o fato da criptografia RSA tem um custo computacional elevado, exigindo-se vários ciclos do processador para realização de tarefas de criptografia e decriptografia, tendo, portanto, seu emprego consumindo mais recursos computacionais do que a chave simétrica (HARBITTER;MENASCÉ, 2001).

Para tornar ainda mais claro o funcionamento da criptografia RSA, será explicitado um exemplo do que acontece na prática quando dois indivíduos querem se comunicar, mas que necessitam de segurança para transmissão.

Encriptação de chave pública (RSA)



Fonte: Gabriel Benato (2018)

O remetente necessita enviar uma mensagem para o destinatário e, como explicado anteriormente, o canal pelo qual a mensagem será enviada é inseguro, necessitando de um método eficaz de segurança. Então, utilizando a criptografia RSA na prática, o emissor usa a chave pública do destinatário, que é de domínio público, para criptografar a mensagem, tornando-a ininteligível para qualquer indivíduo que tentar interceptar a mensagem. Ao chegar essa mensagem para o destinatário, com sua chave privada poderá decifrar a mensagem e, assim, tornar legível de novo. É evidente, portanto, que somente a chave privada do receptor poderá tornar a mensagem criptografada em claro e essa chave é de uso restrito dele, por isso o método RSA é de extrema eficácia no momento em que é utilizado para essa finalidade.

RSA no Exército Brasileiro

Associar esse método criptográfico às redes do Exército Brasileiro, constata-se a criptografia RSA no meio militar brasileiro é atualmente fundamental para segurança de informações confidenciais. Exemplo dessa necessidade, é um estudo da Kaspersky Lab, em 2020, um em cada cinco brasileiros sofreu pelo menos uma tentativa de ataque de phishing a estatística, revelada por novo relatório, coloca o Brasil como líder mundial em golpes dessa categoria à frente de Portugal, França, Tunísia e Guiana Francesa, que completam a lista dos cinco países com maior índice de usuários alvos de roubo de dados ao longo do ano. Outro ponto relevante, é que no ranking mundial de ameaças dessa natureza, o País ocupa a nona colocação. Dessa forma, o exército brasileiro mantém os sistemas atualizados de proteção contra ataques virtuais, sendo o método RSA amplamente utilizado devido à eficácia que apresenta. Nesse sentido, por ser uma criptografia muito eficiente, é possível utilizá-la diretamente na internet ou intranet de um batalhão, como no caso de e-mail.

A criptografia RSA tem um papel muito importante nos conflitos exemplo disso na primeira guerra mundial, a Alemanha saiu atrás por não possuir um departamento de criptografia e criptoanálise forte como a França. Suas comunicações a rádio era interceptadas e descobertas, acarretando na perda da efetividade no cumprimento da

missão. Nesse sentido, o exército brasileiro utiliza-se desse método com o intuito de garantir a segurança de suas informações ao transmiti-las principalmente em um teatro de operações, obtendo em um conflito o efeito surpresa sobre o inimigo. Outro ponto relevante caracteriza-se pela segurança eletrônica. A instituição Exército precisa esconder suas informações sigilosas, pois dentro do ambiente hodierno o conhecimento e os dados são valiosíssimos no mundo. Por isso, toda a troca de mensagens cifradas utilizando esse método atualmente, está envolvida no ambiente da internet e das atividades do Exército Brasileiro como na permutação de e-mails pelo software Zimbra ou com o gerenciador de certificados aplicando a cifragem de informações chamado kleopatra. Além disso, o login e senha para acesso no site do AVA EB aula, acesso DGP e em outros websites que necessitem de acesso.

2.2 TIPOS DE PESQUISA

A pesquisa trabalhada é uma pesquisa de caráter exploratório que envolve os estudos de normas de apostilas.Essas análises foram feitas em diversas obras literárias, apostilas e manuais tanto do exército brasileiro, quanto em livros virtuais. Nesse sentido, decidimos utilizar dois livros principais como fonte de informações: "Aplicação de reticulados em criptografia" e " Entendendo (a verdade) da criptografia RSA. Portanto ,as contribuições dos materiais foram fundamentais para a construção do projeto sobre a criptografia Rivest-Shamir-Adleman.

2.3 TRAJETÓRIA METODOLÓGICA DA PESQUISA

Primeiramente, estudamos a partir das referências bibliográficas, analisando os principais autores que corroboram a pesquisa, no tocante a importância da metodologia no trabalho científico, como Freitas e Prodanov (2013). Em seguida, foi feita uma pesquisa sobre a criptografia RSA. Vimos que o melhor a ser feito é basear-se na revisão bibliográfica, em vista da ausência do Comitê de ética. Posteriormente, explanamos a criptografia RSA e suas aplicações, especificamos a utilização da criptografia no Exército

brasileiro, nos sistemas pessoais e nos equipamentos utilizados. Em seguida, escolhemos o assunto, os processos de criptografia e fizemos o referencial teórico, embasado em autores da área de atuação para fortalecer nossa pesquisa.Por último, procuramos associar a utilização dos sistemas criptográficos com os sistemas do Exército brasileiro

3. CONSIDERAÇÕES FINAIS

Para as considerações finais, reconhece-se que este artigo apresentou uma maneira simples de compreender o funcionamento da criptografia RSA e suas aplicações no Exército Brasileiro, voltado às pessoas com pouco conhecimento acerca do tema. Foi descrito um breve histórico do surgimento da criptografia, os criadores do método RSA, seu funcionamento, uma justificativa de sua grande utilização atualmente nos meios de comunicações e, por fim, foi explanado o emprego dessa criptografia no Exército Brasileiro. É evidente, portanto, que os objetivos propostos para compreensão do tema foram atingidos, uma vez que foi apresentado de maneira simples e objetiva a criptografia RSA e seu funcionamento, o que reflete na confiança que o leitor terá ao utilizar esse método criptográfico.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR 6022**:**2003. Informação e documentação - Artigo em publicação periódica científica impressa -Apresentação.** Rio de Janeiro, 2003. 5 p.

BARBOSA, Luis. et al**. RSA: Criptografia Assimétrica e Assinatura Digital**. Campinas,2003.Disponível http://braghetto.eti.br/files/trabalho%20oficial%20final%20rsa.pdf. Acesso em 27 de março de 2022

CARVALHOSA, Jonathan Correia. **Aplicação de reticulados em criptografia.** Instituto Militar de Engenharia. Rio de Janeiro 2012.

CASTRO, Felipe Lopes. **Criptografia RSA: uma abordagem para professores do ensino básico**. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2014. Disponível em https://www.lume.ufrgs.br/bitstream/handle/10183/110014/000951896.pdf. Acesso em: 10 de abril de 2022

NOGUEIRA, Ana. **Proposta de atividades usando Criptografia nas aulas de Matemáticas**.Guaratinguetá,2017.Disponível em https://repositorio.unesp.br/bitstream/handle/11449/156926/000905848.pdf?sequence=1&isAllow. Acesso em 24 de março de 2022

OLIVEIRA, Felipe. **Entendendo (de verdade) a criptografia RSA**. 10 de dezembro de 2012. Disponível em https://www.lambda3.com.br/2012/12/entendendo-de-verdade-a-criptografia-rsa/. Acesso em 01 de abril de 2022

PETEAM, Fernanda Bia. et al. **Criptografia: o método RSA**. Universidade Estadual de Campinas. Disponível em https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/Fernando_TN17M2.pdf. Acesso em: 01 de abril de 2022

SANTOS, R., J. **Álgebra Linear e Aplicações**. UFMG, 2010

SHALLIT, Jeffrey.et al**. Algorithmic Number Theory**. 1996.

SILVA, Willian. **A EVOLUÇÃO DA CRIPTOGRAFIA E SUAS TÉCNICAS AO LONGO DA HISTÓRIA**. Ceres-GO, 2019. Disponível em https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1/tcc_Willian_Wallace_de_Matteus_Silva.pdf. Acesso em 01 de abril de 2022