RELIMAT
Revista Eletrônica do Curso de Licenciatura em Matemática
Uni-FACEF
Centro Universitário Municipal de Franca

TEORIA DOS NÚMEROS E A CRIPTOGRAFIA RSA

Nícolas Moscardi Garcia
Discente do Curso de Licenciatura em Matemática – Uni-FACEF
nicolaspst@gmail.com

Profª. Ms. Letícia Faleiros Chaves Rodrigues
Mestre em Matemática Universitária e Docente do Uni-FACEF
leticia@facef.br

RESUMO

Este trabalho aborda a aplicação da teoria dos números na criptografia, com foco no método RSA. O objetivo deste trabalho é demonstrar a importância do método RSA na atualidade e o uso de conceitos matemáticos abordados durante a graduação em matemática que embasam seu funcionamento, demonstrando uma aplicação concreta destes. Inicialmente são abordados conceitos fundamentais da teoria dos números, que embasam o funcionamento dos métodos criptográficos, principalmente o RSA. Em seguida, é feita uma contextualização histórica da criação e da evolução da criptografia desde os gregos antigos, passando pelos métodos clássicos de cifragem e chegando nos desafios modernos envolvendo a criptografia, como o problema da distribuição das chaves, contextualizando assim o momento histórico para que se desse o desenvolvimento dos métodos de criptografia de chave pública. Foi feita então uma abordagem do funcionamento do método, utilizando os conceitos vistos no primeiro capítulo e demonstrando que sempre se obtém a mensagem original após a decriptação, construindo um exemplo próprio do autor, sobre o qual os cálculos foram realizados. Por fim, é discutido sobre a importância do método, sua segurança e quais fatores atuam sobre ela e também perspectivas futuras envolvendo o tema da criptografia.

Palavras-chave: criptografia; teoria dos números; RSA

ABSTRACT

This paper addresses the application of number theory in cryptography, focusing on the RSA method. The aim of this work is to demonstrate the importance of the RSA method today and the use of mathematical concepts covered during undergraduate mathematics courses that underpin its operation, demonstrating a concrete application of these concepts. Initially, fundamental concepts of number theory are covered, which underpin the operation of cryptographic methods, mainly RSA. Then, it's historically contextualized the creation and development of cryptography since the ancient Greeks, going through classical cyphering methods and ending on contemporary questions involving cryptography, like the key distribution problem, this way contextualizing the historical moment when the public-key cryptography methods were created. The functioning of the method is addressed using concepts studied in the first chapter, then it's demonstrated, through the developing of an example of the author's own, on which the calculations were made, that it always outputs the plain text after the decryption process. Finally, it discusses the importance, the security of the method and which factors act upon it and prospects involving the matter of cryptography.

Keywords: cryptography; number theory; RSA.

1 INTRODUÇÃO

A palavra criptografia vem dos termos gregos cryptos, “secreto, escondido” e gráphein, “escrita”, e denomina o estudo dos métodos para a codificação de informações de forma que apenas o receptor desejado possa compreender, evitando assim que terceiros que possam vir a ter acesso à mensagem criptografada consigam descobrir qual era o texto original.

A criptografia é usada desde a antiguidade, com registros de seu uso pelos gregos antigos. No período, era utilizada majoritariamente para a ocultação de informações militares, impedindo que os inimigos pudessem obter vantagens estratégicas com base nas informações transmitidas (Paixão, 2020).

Apesar de grande parte do desenvolvimento das técnicas de criptografia e da análise criptográfica (parte da ciência que foca na análise dos métodos de cifragem para quebrá-los e descobrir as mensagens, revelando assim potenciais fraquezas) ter se dado até na idade contemporânea por demandas militares, atualmente a criptografia se vê protagonista no mundo devido à informatização cada vez maior de vários aspectos da vida cotidiana, como transferências bancárias, uso de cartões de crédito, comunicação por mensagens e e-mail, assinaturas digitais de documentos, criptomoedas e ativos digitais, entre outros, conforme afirma Paixão (2020, p. 27):

> É conveniente lembrar que enquanto na antiguidade a técnica da criptografia era utilizada para confundir inimigos e transmitir mensagens de forma segura, nos dias de hoje a criptografia é utilizada em compras feitas pela internet, transações bancárias e até em aplicativos de troca de mensagens instantâneas.

Com a evolução da demanda proporcionada pelo uso cada vez maior de computadores e da internet, novos métodos mais sofisticados do que os clássicos foram se mostrando necessários. Um desses algoritmos é o RSA, sigla advinda dos nomes de seus três criadores, Rivest, Shamir e Adleman, sendo até hoje um dos sistemas mais importantes de criptografia (Coutinho, 2013).

Neste sentido, o objetivo da pesquisa é demonstrar a matemática envolvida no uso da criptografia e traçar uma contextualização histórica de seu uso e

desenvolvimento até a idade contemporânea, mostrando a importância do método RSA.

A justificativa da pesquisa se dá pela importância do algoritmo sobre o qual este trabalho se debruça na atualidade, principalmente num contexto de consolidação da vida no mundo digital. Logo, a compreensão da matemática envolvida no contexto da criptografia é uma boa forma de se abordar um conteúdo visto durante as graduações em matemática (Teoria dos Números) pois está presente, cada vez mais, no cotidiano.

Sendo assim, este trabalho buscará, em seu segundo capítulo, retomar os conceitos matemáticos, mais especificamente aqueles enquadrados na Teoria dos Números, utilizados dentro da criptografia.

No terceiro capítulo será apresentado um pouco da história da criptografia, do desenvolvimento da criptoanálise e dos métodos clássicos de cifragem.

Por fim, no quarto capítulo, será apresentado o funcionamento do algoritmo RSA, demonstrando inicialmente as grandes diferenças e evoluções deste para com os métodos de criptografia clássicos apresentados no capítulo três e utilizando os conceitos de Teoria dos Números abordados no capítulo dois.

2 TEORIA DOS NÚMEROS

A Teoria dos Números é uma das áreas mais antigas e fundamentais da Matemática, dedicada ao estudo das propriedades e relações dos números inteiros. Desde tempos antigos, matemáticos de diversas civilizações buscaram entender padrões e resolver problemas relacionados a números. Na Grécia Antiga, filósofos e matemáticos como Pitágoras e Euclides fizeram contribuições notáveis, como o estudo dos números primos e das relações numéricas. Euclides, em particular, desenvolveu o que hoje chamamos de Algoritmo de Euclides, um método eficiente para encontrar o máximo divisor comum entre dois números inteiros que é abordado neste trabalho.

Durante o período medieval, matemáticos islâmicos, como al-Khwarizmi e al-Kindi, expandiram o conhecimento matemático e contribuíram para o desenvolvimento de técnicas algébricas que mais tarde seriam aplicadas à teoria dos números. No Renascimento, a Teoria dos Números ganhou um novo impulso com o trabalho de Pierre de Fermat, que formulou diversos teoremas e conjecturas, incluindo o Pequeno Teorema de Fermat, que se tornaria uma ferramenta essencial em criptografia.

Foi apenas no século XVIII que a Teoria dos Números passou a se consolidar como uma área autônoma da Matemática, principalmente graças a Leonhard Euler, que generalizou o trabalho de Fermat e introduziu a função totiente, conhecida como função de Euler, fundamental para estudos em congruências e sistemas de criptografia moderna. Mais tarde, Carl Friedrich Gauss formalizou a aritmética modular em sua obra Disquisitiones Arithmeticae, estabelecendo as bases para a Matemática modular usada até hoje (Santos, 1998, p.32).

Até os anos 1960, a Teoria dos Números era considerada uma área com pouco aplicabilidade prática (Coutinho, 2013). Hoje, a Teoria dos Números é amplamente aplicada em áreas como criptografia, onde conceitos como números primos, divisibilidade e aritmética modular são usados para garantir a segurança de informações. Essa ligação entre a Matemática pura e a tecnologia faz da Teoria dos Números uma área de constante pesquisa e desenvolvimento.

2.1 CONCEITOS FUNDAMENTAIS

A Teoria dos Números envolve uma série de conceitos e propriedades que são essenciais para o entendimento de algoritmos modernos de criptografia, como o RSA. Entre esses conceitos, destacam-se a divisibilidade, os números primos e compostos, e o Teorema Fundamental da Aritmética. Esta seção abordará esses fundamentos, que servirão como base para o estudo de operações matemáticas avançadas aplicadas na segurança de dados.

2.1.1 DIVISIBILIDADE

Divisibilidade é um conceito central na Teoria dos Números, e está relacionado à possibilidade de um número inteiro ser dividido exatamente por outro. Formalmente, dados inteiros a e b, com $b \neq 0$, diz-se que b divide a se houver um terceiro inteiro c para qual $a = bc$, ou seja, b divide a se a divisão não deixar resto. Também é equivalente a dizer que se b divide a, b é divisor de a. Para indicar que um inteiro b divide a utiliza-se a notação $b|a$. Já a notação $b \nmid a$ indica que b não divide a, ou que não é divisor de a.

Propriedades da Divisibilidade: A divisibilidade possui várias propriedades importantes que facilitam o trabalho com números inteiros. Algumas delas incluem:

- $a|0$ e $a|a$; (Reflexiva)

- $1|a$;

- Se $a|1$ então $a = \pm 1$;

- Se $a|b$ e $b|c$ então $a|c$; (Transitividade)

- Se $a|b$ então $a|bq$ para qualquer q inteiro; (Multiplicação por um escalar)

- Se $a|b$ e $a|c$ então $a|(b + c)$ e $a|(b - c)$;

- Se $a|b$, então $0 < |a| \leq |b|$, para $b \neq 0$;

- Se $a|b$ e $b|a$ então $|a| = |b|$;

- Se $a|b$ e $a|c$ então $a|(bq + cp)$ para quaisquer q e p Inteiros;

Essas propriedades são fundamentais em provas matemáticas e na resolução de problemas complexos de criptografia. Além disso, o conceito de divisibilidade leva ao desenvolvimento de métodos para encontrar divisores comuns entre números, como o Algoritmo de Euclides, que será discutido mais adiante.

2.1.2 MÁXIMO DIVISOR COMUM

Para definir o máximo divisor comum (MDC), antes é necessário definir o que é divisor comum. Dados a e b inteiros, um número d é divisor comum de a e b se $d|a$ e $d|b$. Por exemplo, o conjunto dos divisores comuns de 20 e 40 é {−20, −10, −5, −4, −2, −1,1,2,4,5,10,20}.

Pode -se definir o MDC de a e b como o maior inteiro positivo dentre os seus divisores comuns. A notação adotada é $mdc(a, b)$.

O MDC de um par de inteiros pode ser calculado através da fatoração em números primos de tais inteiros. Dados $n = p^1 \alpha^1 . p^2 \alpha^2 . . . . . pk^{\alpha k}$ e $m = p^1 \beta^1 . p^2 \beta^2 . . . . . p^k b^k$, onde $p^1, p^2, . . . , p^k$ são números primos distintos e αi e βi são os expoentes de cada fator primo de n e m respectivamente, o $mdc(n, m) = p1^{\min(\alpha 1, \beta 1)} . p2^{\min(\alpha 2, \beta 2)} . . . . . pk^{\min(\alpha k, \beta k)}$, isto é, dada a fatoração em fatores primos de dois inteiros, encontra-se seu máximo divisor comum tomando o menor expoente de cada número primo que aparece na fatoração de ambos. Por exemplo, $24 = 2^3 . 3$ e $100 = 2^2 . 5^2$, então $mdc(24,100) = 2^2 . 3^0 . 5^0 = 2^2 = 4$.

2.1.3 NÚMERO PRIMOS

Antes de falar sobre o Teorema Fundamental da Aritmética, é necessário definir o que são números primos e números compostos.

Um número n ($n \in Z$, $|n| \geq 2$) é dito primo se, e somente se, seu conjunto de divisores é {−1,1, $-n$, n), isto é, n só é divisível por 1 e por ele próprio. Se um número não é primo, então ele é composto.

Pode-se também dizer que dois números a e b são primos entre si caso $mdc(a, b) = 1$, isto é a e b não possuem divisores em comum além de ±1. Caso contrário, o número é composto, ou seja, pode ser expresso como o produto de dois ou mais inteiros menores que ele.

Exemplos de Números Primos e Compostos: os primeiros números primos são 2, 3, 5, 7, 11, e 13, enquanto números como 4, 6, 8, 9, e 12 são

compostos, pois podem ser divididos por números além de 1 e deles mesmos. O número 2 é o único número par que é primo; todos os outros números pares são divisíveis por 2, o que os torna compostos.

Primos entre si: dois números são considerados "primos entre si" (ou coprimos) se o seu máximo divisor comum é 1. Isso significa que, embora ambos possam ser compostos, não possuem divisores comuns além de 1. Analisando os números 9 e 16, por exemplo, verifica-se que estes, apesar de serem ambos compostos, são primos entre si, pois não compartilham fatores (divisores) em comum. É de fácil constatação, entretanto, que dois números primos sempre serão primos entre si. Esse conceito é crucial na criptografia RSA, onde a coprimalidade é usada para garantir a segurança dos algoritmos.

2.1.4 Teorema fundamental da Aritmética

Um dos resultados mais importantes envolvendo números primos é o Teorema Fundamental da Aritmética. Ele afirma que qualquer número inteiro maior que 1 pode ser representado de maneira única (salvo a ordem dos fatores) como um produto de números primos. Esse teorema estabelece a base para o conceito de fatoração, que é usado para gerar chaves criptográficas. A fatoração em números primos é um problema complexo e, para números muito grandes, a dificuldade de fatoração é o que garante a segurança do algoritmo RSA.

Logo, o Teorema Fundamental da Aritmética dita que qualquer inteiro positivo $n \geq 2$ pode ser escrito de forma única através da expressão:

$$n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot pk^{\alpha k}$$

Onde $p_1, p_2, \ldots, p_k$ são números primos distintos e $a_1, a_2, \ldots, a_k$ são números inteiros maiores que 0.

Por exemplo, o número 60 pode ser expresso como o produto de primos $60 = 2^2 \cdot 3 \cdot 5$. Essa expressão é única para 60 e demonstra como a fatoração se aplica de forma determinística.

Esses conceitos de divisibilidade e números primos são fundamentais para as operações avançadas na criptografia e para o entendimento de algoritmos

baseados em aritmética modular, como o RSA.

2.2 ALGORITMO DA DIVISÃO E MÁXIMO DIVISOR COMUM

Nesta seção, serão abordados dois conceitos fundamentais da Teoria dos Números: o Algoritmo da Divisão e o cálculo do Máximo Divisor Comum (MDC). Ambos são ferramentas essenciais para a compreensão de operações com números inteiros, sendo o MDC particularmente importante em criptografia e em algoritmos que dependem de propriedades de divisibilidade e coprimalidade.

Dados a e b inteiros positivos, ao realizar a divisão de a por b, obtém-se um quociente inteiro q e um resto inteiro r, únicos, descritos pela relação:

$$a = bq + r \text{ com } 0 \leq r < b$$

Por tradição, esta equação é conhecida como Algoritmo da Divisão, apesar de ser, na verdade, um teorema.

A unicidade dos valores de q e r pode ser demonstrada por contradição. Supondo que existam dois pares diferentes, q, r e q', r' que satisfaçam o Algoritmo, ou seja:

$$a = bq + r \text{ e } a = bq' + r', \text{ com } 0 \leq r, r' < b.$$

Pode-se igualar as duas equações obtendo:

$$bq + r = bq' + r' \rightarrow r - r' = b(q' - q),$$

Isto implica que $b|(r - r')$, porém, como $0 \leq r, r' < b$, $r - r'$ deve estar compreendido no intervalo $[0, b - 1]$, o único valor possível para $r - r'$ é 0:

$$r - r' = 0 \rightarrow r = r'$$

Prova-se assim que o valor de r é único. Agora é possível provar que $q = q'$, pois:

$$a = bq + r = bq' + r \rightarrow bq = bq' \rightarrow q = q'$$

Provando que o valor de q é único.

Portanto, o Algoritmo da Divisão afirma que existem inteiros únicos q

(quociente) e r (resto) tais que:

$$a = bq + r \text{ com } 0 \leq r < b$$

Esse resultado é significativo porque fornece uma maneira de expressar qualquer número a em termos de uma divisão exata por b, com um resto menor que o divisor.

Exemplo: Suponha que a = 17 e b = 5. Dividindo 17 por 5, obtémse q = 3 e r = 2, já que:

$$17 = 5 \cdot 3 + 2$$

Esse algoritmo é amplamente utilizado em operações aritméticas e se aplica também na aritmética modular.

2.2.1 ALGORITMO DE EUCLIDES

A determinação do MDC é importante para a compreensão e o funcionamento do algoritmo RSA, porém, este utiliza números inteiros muito grandes em sua execução, os quais são difíceis de fatorar convencionalmente. Surge então o Algoritmo de Euclides como uma alternativa eficiente para a determinação do máximo divisor comum de dois números sem depender de fatoração.

Dados a e b números inteiros positivos tais que $a = bq + r$ (algoritmo da divisão) com q e r inteiros, o conjunto dos divisores comuns de a e b é o mesmo dos divisores comuns de b e r, e, por consequência, $mdc(a, b) = mdc(b, r)$. É possível demonstrar tal identidade através da propriedade “se $d|a$ e $d|b$ então $d|(pa + qb)$, para quaisquer q e p inteiros”, portanto, se $d|a$ e $d|b$ e $r = a - bq$ então $d|r$.

Reitera-se o processo do Algoritmo da Divisão até chegar ao último resto não nulo, o qual será o valor do MDC que buscado:

$$a = bq_1 + r_1, \text{ com } 0 \leq r_1 < b$$

$$b = r_1q_2 + r_2, \text{ com } 0 \leq r_2 < r_1$$

$$r1 = r_2q_3 + r_3, \text{ com } 0 \leq r_3 < r_2$$

$r_{n-2} = r_{n-1}q_n + r_n$, com $0 \leq r_n < r_{n-1}$

$r_{n-1} = r_n q_{n+1}$

No caso, o último resto não nulo encontrado, rn, é o $mdc(a, b)$. É possível calcular, por exemplo, o mdc(7469,2387):

7469 = 2387.3 + 308

2387 = 308.7 + 231

308 = 231.1 + 77

231 = 77.3

Como o último resto não nulo encontrado foi 77, tem-se que

mdc(7469,2387) = 77

2.2.2 ALGORITMO DE EUCLIDES ESTENDIDO

O Algoritmo de Euclides também pode ser estendido para encontrar coeficientes inteiros x e y que satisfaçam a equação de Bézout:

$$mdc(a, b) = a \cdot x + b \cdot y$$

Esses coeficientes são úteis em várias aplicações, incluindo a criptografia RSA, onde são utilizados para calcular inversos modulares.

Logo, dados a e b inteiros positivos e $d = mdc(a, b)$, existem α e β inteiros tais que $\alpha . a + \beta . b = d$. É possível demonstrar isso efetuando o Algoritmo de Euclides da seguinte forma:

$a = bq_1 + r_1$, com $r_1 = ax_1 + by_1$

$b = r_1q_2 + r_2$, com $r_2 = ax_2 + by_2$

$r_1 = r_2q_3 + r_3$, com $r_3 = ax_3 + by_3$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \text{ com } r_{n-1} = ax_{n-1} + by_{n-1}$$

$$r_{n-2} = r_{n-1}q_n, \text{ com } r_n = 0$$

Onde os valores xi e yi são inteiros que podem ser determinados analisando sempre duas iterações anteriores do algoritmo:

$$r_{i-2} = r_{i-1}q_i + r_i \rightarrow r_i = r_{i-2} - r_{i-1}q_i$$

Onde i indica a iteração, ou linha, do Algoritmo. Pode-se agora substituir as expressões $ri{-}2 = axi{-}2 + byi{-}2$ e $ri{-}i = axi{-}1 + byi{-}1$ na primeira equação:

$$r_i = ax_{i-2} + by_{i-2} - (ax_{i-1} + by_{i-1})q_i = a(x_{i-2} - x_{i-1}q_i) + b(y_{i-2} - y_{i-1}q_i)$$

Daí, como $r_i = ax_i + by_i$, temos que:

$$x_i = x_{i-2} - x_{i-1}q_i \text{ e } y_i = y_{i-2} - y_{i-1}q_i$$

Ou seja, é possível determinar qualquer x_i e y_i utilizando os valores encontrados nas duas iterações anteriores e o quociente da própria iteração. Para dar início ao processo, portanto, precisa-se dos valores de x_i e y_i de duas iterações anteriores à primeira, para isso, serão chamados de x_0, y_0 e x_{-1} e y_{-1} onde $a = ax_{-1} + by_{-1}$ e $b = ax_0 + by_0$, tais expressões podem ser obtidas ao extrapolar o padrão que aparece no Algoritmo:

$$u = vq_{-1} + a, \text{ com } a = ax_{-1} + by_{-1}$$

$$v = aq_0 + b, \text{ com } \boldsymbol{b = ax_0 + by_0}$$

$$a = bq_1 + r1, \text{ com } r_1 = ax_1 + by_1$$

$$b = r_1q_2 + r2, \text{ com } r_2 = ax_2 + by_2$$

$$r_1 = r_2q_3 + r3, \text{ com } r_3 = ax_3 + by_3$$

Analisando as expressões desejadas, fica claro que os valores buscados são $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$ e $y_0 = 1$. Uma vez que tem-se $d = mdc(a, b) = r_{n-1}$, pode-se fazer $d = r_{n-1} = ax_{n-1} + by_{n-1}$ que implica em $\alpha = x_{n-1}$ e $\beta = y_{n-1}$.

Por exemplo, é possível calcular α e β no mesmo exemplo, mdc(7469,2387) = 77:

$$7469 = 2387.3 + 308 \rightarrow 308 = 7469 - 2387.3$$

$$2387 = 308.7 + 231 \rightarrow 231 = 2387 - 308.7$$

$$308 = 231.1 + 77 \rightarrow 77 = 308 - 231.1$$

$$231 = 77.3$$

Daí, obtém-se:

$$77 = 308 - 231.1 = 308 + (-1)(2387 - 308.7)$$

$$= 8.308 + (-1).2387 = 8.\ (7469 - 2387.3) + (-1).2387$$

$$= 8.7469 + (-25).2387$$

Portanto, $\alpha = 8$ e $\beta = -25$

2.3 ARITMÉTICA MODULAR E SUAS PROPRIEDADES

A aritmética modular versa sobre o estudo de fenômenos periódicos, ou seja, que se repetem com período, ou módulo, constante. Alguns exemplos de tais fenômenos são: dias num ano, dias numa semana, horas num dia, entre outros.

A formalização de uma aritmética para estudar tais fenômenos é interessante, pois os restos das divisões também são um fenômeno periódico. Dada uma divisão de a por b, expressa pelo algoritmo da divisão, $a = bq + r$ com $0 \leq r < b$, percebe-se que conforme varia-se o valor de a, r só pode assumir b valores diferentes, portanto, afirma-se que o período, ou módulo de r é b.

Dado um n inteiro positivo e um a inteiro, é definido $a\ mod\ n$ como sendo o resto da divisão de a por n. Por exemplo, 3 mod 2 = 1, pois 3 = 2.1 + 1.

Além de funcionar como operador binário, o módulo também é utilizado para definir a noção de congruência. Define-se que dois inteiros a e b são congruentes módulo n se $a\ mod\ n = b\ mod\ n$, a notação utilizada é

$$a \equiv b(mod\ n)$$

Por exemplo, 3 e 7 são congruentes módulo 2, pois 3 mod 2 = 7 mod 2 = 1, então escreve-se que 3 ≡ 7(mod2). Disso, é possível afirmar que $a \equiv b(mod\ n)$ se $n|(a - b)$.

2.3.1 PROPRIEDADES DA CONGRUÊNCIA MODULAR

As propriedades da congruência modular se assemelham às da igualdade, sendo elas as propriedades:

- reflexiva: $a \equiv a(mod\ n)$

- simétrica: se $a \equiv b(mod\ n)$ então $b \equiv a(mod\ n)$

- transitiva: se $a \equiv b(mod\ n)$ e $b \equiv c(mod\ n)$ então $a \equiv c(mod\ n)$

É possível definir as operações de soma e produto dentro da aritmética modular, dados $a \equiv a'\ (mod\ n)$ e $b \equiv b'\ (mod\ n)$, tem-se:

- $a + b \equiv a' + b'\ (mod\ n)$, pois $a - a' = qn$ e $b - b' = kn$, então:

$$(a - a') + (b - b') = n(q + k) \rightarrow (a + b) - (a' + b') = n(q + k)$$

O que implica que $n|(a + b) - (a' + b')$.

- $ab \equiv a'b'(mod\ n)$, pois $a = a' + qn$ e $b = b' + kn$, de forma que:

$$ab = a'b' + a'kn + bqn + qkn\ 2 \rightarrow ab - a'b' = n(a'k + bq + qkn)$$

O que implica que $n|(ab - a'b')$.

De forma particular, pelo obtido na operação de multiplicação, tem-se que $a\ k \equiv a'\ k\ (mod\ n)$, para k não negativo.

Essas propriedades simplificam cálculos envolvendo grandes números, permitindo a redução dos resultados ao intervalo determinado pelo módulo n.

2.3.2 CLASSES DE EQUIVALÊNCIA E O CONJUNTO Z_n

Define-se uma classe de equivalência $\bar{a}$ da seguinte forma: $\bar{a} = \{a + qn; q \in Z\}$, ou seja, quaisquer elementos de $\bar{a}$ são congruentes entre si módulo n. Vale ressaltar que qualquer elemento de uma determinada classe de equivalência pode ser utilizado como seu representante. Por exemplo, em módulo 3, $\bar{2} = \{2,5,8,11, \ldots\}$, pois $2 \equiv 5 \equiv 8 \equiv 11 \ (mod\ 3)$.

É chamado de Z_n o conjunto de todas as classes de equivalência módulo n, de forma que $Z_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. É importante dizer que para quaisquer classes $\bar{a}, \bar{b} \in Zn$, $\bar{a} \cap \bar{b} = \emptyset$, pois dois números distintos entre 0 e $n - 1$ só podem ser congruentes, módulo n, caso sejam iguais.

Exemplo: Para n = 5:

$$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Cada classe $\bar{a}$ contém todos os inteiros que deixam o mesmo resto a quando divididos por 5.

2.3.3 INVERSOS MODULARES

Diz-se que, em Z_n, $\bar{a}$ é a classe inversa de $\bar{b}$ se $\overline{a.\ b} = \bar{1}$, ou seja $a.\ b \equiv 1(mod\ n)$. A questão é que nem todas as classes de equivalência módulo n são inversíveis, por exemplo, em $Z4$, existem as classes $\bar{0}, \bar{1}, \bar{2}, \bar{3}$, buscando a classe inversa de $\bar{2}$, esta não é encontrada: $\bar{0}.\ \bar{2} = \bar{0}$; $\bar{1}.\ \bar{2} = \bar{2}$; $\bar{2}.\ \bar{2} = \bar{0}$ e $\bar{3}.\ \bar{2} = \bar{0}$, porém, para $\bar{3}$, tem-se $\bar{3}.\ \bar{3} = \bar{1}$.

Daí, vem o Teorema da Inversão, que diz que, $\bar{a}$ tem inverso em Zn se, e somente se, a e n são primos entre si.

Demonstração: Supondo que exista $\bar{b}$, inverso de $\bar{a}$ em Z_n, então $ab \equiv 1(mod\ n) \rightarrow n|(ab - 1)$, portanto, existe um inteiro q, tal que $qn + ab = 1$. Seja $d = mdc(a,\ n)$, tem-se que $d|a$ e $d|n$, então $d|(qn + ab) \rightarrow d|1$, portanto $d = 1$. Demonstrando a volta agora, se $d = 1$, tem-se, pelo Algoritmo de Euclides Estendido, que existem inteiros α e β tais que $\alpha.\ a + \beta.\ n = 1$, daí:

$\alpha . a - 1 = -\beta . n \rightarrow n|(\alpha . a - 1) \rightarrow \alpha . a \equiv 1(mod\ n) \rightarrow \bar{\alpha}.\ \bar{a} = \bar{1}$

Portanto, $\bar{a}$ é inversível em Z_n.

Chama-se de $v(n)$ o conjunto das classes em Zn que possuem inverso, ou seja $v(n) = \{\bar{a} \in Zn;\ mdc(a,\ n) = 1\}$. Da conclusão do parágrafo anterior, em particular, tem-se que se n for um número primo, todas as classes de Zn, com exceção de $\bar{0}$, possuem inversos, pois n é coprimo com qualquer número entre 1 e $n - 1$.

Outra constatação importante é que, para quaisquer $\bar{a}$, $\bar{b} \in v(n)$, $\bar{a}.\ \bar{b} \in v(n)$: sendo $\bar{a'}$ e $\bar{b'}$ as respectivas classes inversas de $\bar{a}$ e $\bar{b}$, tem-se que $aa' \equiv 1(mod\ n)$ e $bb' \equiv 1\ (mod\ n)$, então $aa'bb' \equiv 1\ (mod\ n) \rightarrow (ab).\ (a'b') \equiv 1\ (mod\ n)$, ou seja, a classe $\overline{a.\ b}$ possui inverso, que é, justamente, $\overline{a'.\ b'}$.

Exemplo: No conjunto Z_7, o número 3 possui um inverso modular. O inverso é 5, pois:

$$3 \cdot 5 = 15 \equiv 1\ (mod\ 7)$$

Os inversos modulares são uma parte importante do algoritmo RSA, onde eles são usados para gerar chaves privadas a partir das públicas. O cálculo eficiente de inversos modulares é frequentemente realizado usando o Algoritmo de Euclides Estendido.

2.4 FUNÇÃO TOTIENTE DE EULER E PEQUENO TEOREMA DE FERMAT

Nesta seção, serão abordados dois conceitos fundamentais na Teoria dos Números aplicados à criptografia: a Função Totiente de Euler e o Pequeno Teorema de Fermat. Esses tópicos são essenciais para o entendimento do algoritmo RSA, que depende da propriedade de números primos e de congruências modulares.

2.4.1 O PEQUENO TEOREMA DE FERMAT

O Pequeno Teorema de Fermat diz que, dados um primo p e um inteiro

a, $a\ p \equiv a\ (mod\ p)$.

A comprovação de tal afirmação pode ser dividida em dois casos, primeiro com $p|a$, onde $a \equiv 0\ (mod\ p) \rightarrow 0^{\ p} \equiv 0\ (mod\ p)$, o que já comprova este caso.

Em seguida, é necessário olhar para o caso onde $p \nmid a$, que implica que $mdc\ (a,\ p) = 1$. Como a e p são primos entre si, a classe a possui inverso módulo p, então pode-se reescrever o Teorema da seguinte forma:

$$aa'a^{\ p-1} \equiv aa'\ (mod\ p)$$

Onde a' é o inverso de a, daí, tem-se:

$$a^{p-1} \equiv 1\ (mod\ p)$$

Serão consideradas agora as sequências {1,2,3, . . . , $(p-1)$} e {a, $2a$, $3a$, . . . , $(p-1)a$}. É de fácil constatação que não há elementos múltiplos de p em {a, $2a$, $3a$, . . . , $(p-1)a$}, uma vez que se existe um cofator q tal que $p = qa$, como $p \nmid a$, q deve ser múltiplo de p, porém verifica-se que não existem valores múltiplos de p em {1,2,3, . . . , $(p-1)$}, verificando assim a afirmação. Também se verifica desta forma que não existem dois elementos diferentes congruentes módulo p em {a, $2a$, $3a$, . . . , $(p-1)a$}. É possível então concluir então que tanto os elementos da primeira sequência quanto os da segunda são representantes de todas as classes de equivalência em Zp, o que implica que cada elemento de {1,2,3, . . . , $(p-1)$} é congruente a algum elemento de {a, $2a$, $3a$, . . . , $(p-1)a$}, não necessariamente na mesma ordem. Com isso é possível escrever que:

$$a.\ 2a.\ 3a.\ .\ .\ .\ .\ (p-1)a \equiv 1.2.3.\ (p-1)\ (mod\ p) \rightarrow a^{\ p-1}\ (p-1)! \equiv (p-1)!\ (mod\ p)$$

Cancelando $(p-1)!$, obtém-se:

$$a^{\ p-1} \equiv 1\ (mod\ p)$$

Assim, verifica-se o Teorema.

Exemplo: Se $a = 2$ e $p = 7$, como 2 e 7 são coprimos, tem-se:

$$2^{7-1} = 2^{6} = 64 \equiv 1 \ (mod\ 7)$$

Portanto, $2^{6} \equiv 1 \ (mod\ 7)$.

Esse teorema é um dos fundamentos para garantir a segurança da criptografia de chave pública, permitindo que potências de números grandes sejam calculadas de forma eficiente e modular.

2.4.2 FUNÇÃO TOTIENTE DE EULER

A função Totiente, ou Tociente, resulta na quantidade de elementos do conjunto $v(n)$, ou seja, a quantidade de classes de equivalência em Znque possuem inverso multiplicativo. Como é fator necessário e único para que uma classe $\bar{a}$ possua inverso em Z_n que a e n sejam primos entre si, é possível definir a Função Totiente como sendo a quantidade de inteiros entre 1 e $n - 1$ coprimos com n. Denota-se tal Função por $\phi(n)$. Por definição, $\phi(n) = 1$.

Da definição da Função Totiente, é possível provar o seguinte teorema: dado um inteiro positivo k e um primo p, tem-se que:

$$\phi(p^{k}) = p^{k} - p^{k-1}$$

A lógica é buscar a quantidade de inteiros entre 0 e p^{k} que sejam coprimos com p^{k}. Tem-se, porém, que é mais fácil enumerar a quantidade de inteiros em tal intervalo que não são primos com p^{k}, que são justamente as potências de p, portanto, existem p^{k-1} inteiros entre 0 e p^{k} que não são coprimos com p^{k}, então há $p^{k} - p^{k-1}$ inteiros que são coprimos com p^{k} neste intervalo. Desta forma, $\phi(p^{k}) = p^{k} - p^{k-1}$. É possível escrever também da seguinte forma:

$$\phi(p\ k) = p^{k}\left(1 - \frac{1}{p}\right)$$

De forma particular, tem-se que $\phi(p) = p - 1$, para p primo. Bastando fazer $k = 1$ no teorema proposto:

$$\phi(p^{1}) = p^{1} - p^{0} \rightarrow \phi(p) = p - 1$$

Tem-se também que, para m e n inteiros, positivos e primos entre si,

vale o seguinte:

$$\phi(mn) = \phi(m).\phi(n)$$

É possível expandir tal afirmação de forma que seja possível calcular $\phi(n)$ para qualquer n inteiro positivo fatorado na forma $n = p1^{\alpha 1}. p2^{\alpha 2}. \ldots . pk^{\alpha k}$, onde pi são números primos distintos e αi são números inteiros positivos (Teorema Fundamental da Aritmética). Assim:

$$\phi(n) = \phi(p_1^{\alpha 1}. p2^{\alpha 2.} \ldots . p_k^{\alpha k})$$

$$\phi(n) = \phi(p_1^{\alpha 1}).\phi(p2^{\alpha 2}). \ldots .\phi(p_k\, \alpha k)$$

$$\phi(n) = (p_1^{\alpha 1} - p_1^{\alpha 1-1}). (p_2^{\alpha 2} - p_2^{\alpha 2-1}). \ldots . (p_k^{\alpha k} - p_k^{\alpha k-1})$$

$$\phi(n) = p_1^{\alpha 1}(1 - \frac{1}{\mathrm{p1}}). p_2^{\alpha 2}(1 - \frac{1}{p_2}). \ldots . p_k^{\alpha k}(1 - \frac{1}{p_\mathrm{k}})$$

$$\phi(n) = n. (1 - - \frac{1}{p_1}). (1 - \frac{1}{p_2}) . (1 - \frac{1}{p_3}). \ldots . (1 - \frac{1}{p_\mathrm{k}})$$

Exemplo: Para calcular $\phi(12)$, tem-se que 12 = 2 2 · 3, então:

$$\phi(12) = 12\ (1\ - \frac{1}{2})\ (1\ - \frac{1}{3}) = 12 \cdot - \frac{1}{2}\ \cdot - \frac{2}{3} = 4$$

Portanto, há 4 números menores que 12 que são coprimos com 12: 1, 5, 7 e 11.

A Função Totiente de Euler é especialmente importante para a criptografia RSA, onde o valor de $\phi(n)$ de um número composto $n = p \cdot q$ (produto de dois primos grandes) é usado para definir a chave privada. A dificuldade em fatorar n é o que torna o sistema seguro.

2.4.3 TEOREMA DE EULER

O Teorema de Euler diz que, dado um n inteiro positivo e um a inteiro, primos entre si, então

$$a^{\phi(n)} \equiv 1\ (mod\ n)$$

Como a e n são coprimos, a é possui inverso módulo n. Considera-se agora o conjunto $\{a_1, a_2, a_3, \ldots, a_{\phi(n)}\}$ de representantes das classes que possuem inverso em Z_n, uma vez que há $\phi(n)$ inteiros entre 1 e $n-1$ que são coprimos com n. Toma-se agora um inteiro α que também é inversível módulo n. Tem-se então que $\{\alpha.\ a_1, \alpha.\ a_2, \alpha.\ a_3, \ldots, \alpha.\ a_{\phi(n)}\}$ também é um conjunto de representantes de todas as classes inversíveis em Zn. Prova-se isso supondo que existam a_i e a_j distintos, então:

$$\alpha.\ a_i \equiv \alpha.\ a_j\ (mod\ n) \rightarrow a_i \equiv a_j\ (mod\ n)$$

Na equação acima, pode-se cancelar α porque ele é inversível módulo n. Portanto, como cada ai pertence a uma determinada classe de equivalência, cada elemento de $\{a_1, a_2, a_3, \ldots, a_{\phi(n)}\}$ é congruente a algum elemento de $\{\alpha.\ a_1, \alpha.\ a_2, \alpha.\ a_3, \ldots, \alpha.\ a_{\phi(n)}\}$, não necessariamente na mesma ordem. É possível então escrever:

$$\overline{a.a_1}.\ \overline{a.a_2}.\ \overline{a.a_3}.\ \ldots.\ \overline{a.a_{\phi(n)}} = \overline{a_1}.\ \overline{a_2}.\ \overline{a_3}.\ \ldots.\ \overline{a_{\phi(n)}}$$

Isto é:

$$a.\ a_1.\ a.\ a_2.\ a.\ a_3.\ \ldots.\ a.\ a_{\phi(n)} \equiv a_1.\ a_2.\ a_3.\ \ldots.\ a_{\phi(n)}\ (mod\ n)$$

O que implica em:

$$a\ \phi(n)\ (a_1.\ a_2.\ a_3.\ \ldots.\ a_{\phi(n)}) \equiv a_1.\ a_2.\ a_3.\ \ldots.\ a_{\phi(n)}\ (mod\ n)$$

Pode-se então cancelar o fator $a_1.\ a_2.\ a_3.\ \ldots.\ a_{\phi(n)}$ pois este é um produto de fatores inversíveis, sendo também, portanto, inversível, resultando, então, em:

$$a^{\phi(n)} \equiv 1\ (mod\ n)$$

Exemplo: Para calcular $3^{\phi(10)}\ (mod\ 10)$:

1. Primeiro, calculamos $\phi(10)$. Como 10=2·5, então:

$$\phi(10) = 10\ (1 - \frac{1}{2})\ (1 - \frac{1}{5}) = 10 \cdot \frac{1}{2}) \cdot \frac{4}{5}) = 4$$

2. Assim, o teorema garante que $3^4 \equiv 1\ (mod\ 10)$, pois 3 e 10 são coprimos.

Neste capítulo, foram explorados os fundamentos matemáticos da Teoria dos Números, que formam a base teórica para a criptografia moderna. Conceitos como divisibilidade, números primos, aritmética modular, a Função Totiente de Euler e o Pequeno Teorema de Fermat são essenciais para entender como se estruturam os algoritmos criptográficos e, em especial, o RSA. Através dessas ferramentas matemáticas, é possível realizar operações complexas com números inteiros e construir sistemas de segurança baseados na dificuldade de fatoração e na coprimalidade.

Esses fundamentos matemáticos são cruciais para a implementação de algoritmos que garantem a privacidade e a integridade das comunicações digitais. No próximo capítulo, esses conceitos serão aplicados para criar e decifrar códigos, introduzindo o histórico e o desenvolvimento dos métodos de cifragem e o papel central da criptografia na segurança da informação.

3 HISTÓRIA DA CRIPTOGRAFIA E MÉTODOS CLÁSSICOS

3.1 HISTÓRIA E EVOLUÇÃO DA CRIPTOGRAFIA

A criptografia é usada há pelo menos 2500 anos, com evidências de uso militar pelos gregos antigos narradas por historiadores do período. Também há evidências do uso de cifragem de mensagens pelo povo egípcio, porém estes utilizavam a codificação de mensagens para atribuir um caráter de solenidade e mistério aos textos hieroglíficos, conforme afirma Carneiro (2017):

> A criptografia é tão antiga quanto à própria escrita, podendo ser encontrada no sistema de escrita Hieroglífica dos egípcios, onde era usada para esconder o significado real do texto e dar-lhe um caráter mais solene. Vários povos da antiguidade, dentre eles, gregos, hebreus, persas e árabes a utilizavam para tentar impedir que informações confidenciais, caso caíssem em mãos inimigas fossem interpretadas.

Os métodos de criptografia se dividem em dois tipos, os de transposição e os de substituição.

As cifras de transposição buscam permutar as letras de uma mensagem de forma a formar um anagrama do texto original. Um desses métodos é

conhecido como “cerca de ferrovia”, no qual uma mensagem é escrita de forma alternada entre duas linhas, uma letra na linha de cima e outra na de baixo, e depois copia-se primeiramente as letras da linha de cima e depois as letras da linha de baixo. Por exemplo, para criptografar a mensagem “EU AMO MATEMÁTICA”:

Quadro 1: cifragem pelo método "cerca de ferrovia"

E	U	A	M	O	M	A	T	E	M	A	T	I	C	A

Fonte: próprio autor.

Primeiramente, elimina-se os acentos gráficos e os espaços entre as palavras dispondo-as separando as letras, conforme ilustrado no quadro 1. Em seguida, copia-se as letras nos espaços brancos e depois as dos espaços cinzas:

Quadro 2: mensagem cifrada pelo método "cerca de ferrovia"

E	A	O	A	E	A	I	A	U	M	M	T	M	T	C

Fonte: próprio autor.

Sendo assim, conforme demonstrado no quadro 2, a mensagem codificada resultante é “EAOAEAIAUMMTMTC”. Para decodificar a mensagem, basta fazer o processo inverso.

Uma técnica criptográfica de transposição utilizada pelos espartanos foi a de enrolar uma tira de papel ou couro em um bastão, chamado de cítala, com um determinado número de faces e escrever a mensagem, de forma que, ao desenrolar a tira, as letras estariam permutadas. A mensagem só poderia ser decifrada pelo receptor da mensagem se esse enrolasse novamente a tira num bastão com o mesmo número de faces e com as mesmas medidas (Paixão, 2020). Por exemplo, a mensagem “EU AMO MATEMÁTICA”, ao ser escrita em um bastão de três faces, ficaria da seguinte forma:

Quadro 3: cifragem pelo método do bastão "cítala"

1ª FACE	E	U	A	M	O
2ª FACE	M	A	T	E	M
3ª FACE	A	T	I	C	A

Fonte: próprio autor.

Ao desenrolar a fita, como mostrado no quadro 3, obtém-se a mensagem cifrada “EMAUATATIMECOMA”

O problema das cifras de transposição é a facilidade para “quebrar o código”, isto é, decifrar a mensagem. Se o método utilizado para permutar as letras seguir um sistema, basta que o receptor descubra e faça o processo inverso. Caso as letras tenham sido trocadas de forma aleatória, sem o uso de um padrão, as mensagens muito curtas podem ser facilmente decifradas por um terceiro indesejado, já as longas serão quase impossíveis de decifrar devido ao grande número de permutações possíveis (Paixão, 2020).

As cifras de substituição buscam, ao invés de permutar as posições das letras do texto original, trocar as letras por outras.

3.1.1 CIFRA DE CÉSAR E CIFRA DE VIGENÉRE

Um dos métodos mais famosos de criptografia é justamente uma cifra de substituição, conhecida como Cifra de César. Esse sistema consiste em trocar cada letra da mensagem original pela que estivesse três posições à frente no alfabeto. A mensagem “EU AMO MATEMÁTICA” seria codificada para “HX DPR PDWHPDWLFD” pela Cifra de César.

Apesar de ser historicamente conhecida por deslocar as letras em três posições, a mesma ideia da Cifra de César pode ser aplicada para outras quantidades de posições. O número de casas do deslocamento deve ser de conhecimento do receptor da mensagem para que este o possa decifrar. Tal número é conhecido como chave, sendo este um conceito muito importante tanto para os

métodos de criptografia clássicos que vieram depois, quanto para os métodos contemporâneos como o próprio RSA.

A Cifra de César e os métodos semelhantes são chamados de cifras de substituição monoalfabéticas, isto é, que usam apenas um alfabeto para realizar a troca das letras. Devido ao desenvolvimento de técnicas para quebrar os códigos, os estudiosos buscaram desenvolver cifragens mais complexas, como as cifras de substituição polialfabéticas, as quais utilizam dois ou mais alfabetos como referência para a substituição das letras.

Assim como a Cifra de César é um dos métodos de substituição monoalfabéticos mais famosos, a Cifra de Vigenére cumpre este papel para as cifras polialfabéticas. Tal técnica utiliza 26 alfabetos para substituição das letras da mensagem, seguindo uma tabela conhecida como “tabula recta” ou “tabela de Vigenére":

Figura 1: tabula recta ou Tabela de Vigenére

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Wikipedia, 2024, online.

A Cifra de Vigenére depende do uso de uma palavra-chave, previamente combinada entre o autor e o receptor desejado da mensagem, a qual é

usada tanto para cifrar quanto para decifrar a mensagem. Para a cifragem, utilizando como referência a figura 1, é repetida a palavra-chave por toda a extensão do texto original, associando cada letra deste com uma da palavra-chave, então, substitui-se cada letra da mensagem pela correspondente no alfabeto iniciado pela letra da palavra-chave associada a ela.

Por exemplo, a mensagem “EU AMO MATEMÁTICA” seria cifrada seguinte forma, se a palavra-chave fosse “CRIPTO”:

Quadro 4: cifragem pela Cifra de Vigenére

PALAVRA-CHAVE	C	R	I	P	T	O	C	R	I	P	T	O	C	R	I
TEXTO ORIGINAL	E	U	A	M	O	M	A	T	E	M	A	T	I	C	A
TEXTO CIFRADO	G	L	I	B	H	A	C	K	M	B	T	H	K	T	I

Fonte: próprio autor.

Dessa forma, conforme demonstrado no quadro 4, a mensagem codificada seria “GL IBH ACKMBTHKTI”. Para decifrar o texto, basta fazer o processo inverso, o que é simples quando se sabe a palavra-chave.

3.2 CRIPTOANÁLISE

Por vários séculos, o uso das cifras de substituição monoalfabéticas se deu de forma ampla e era considerado extremamente seguro ou até mesmo indecifrável.

Em paralelo ao desenvolvimento da criptografia, também se desenvolveu a ciência da criptoanálise, focada em quebrar os códigos cifrados sem o conhecimento da chave. Seu desenvolvimento se deve grandemente ao povo árabe, que aliaram os conhecimentos de Matemática, estatística e linguística e desenvolveram as bases da ideia da análise de frequência, possibilitando assim quebrar os códigos das cifras de substituição.

> Os árabes, eram familiarizados com o uso da cifra de substituição monoalfabética, no entanto a eles não é concedida nenhuma relevância na história da criptografia, tanto que, além de utilizar cifras, os estudiosos árabes foram capazes de quebrá-las. Foram eles que inventaram a criptoanálise, a ciência da dedução do texto original a partir do texto cifrado, sem o conhecimento da chave. Enquanto o criptógrafo desenvolve novos métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar mensagens secretas (Carneiro, 2017, p. 7).

A análise de frequência busca, através do conhecimento de uma linguagem, determinar a frequência em que as letras aparecem, além de analisar combinações comuns de duas ou mais letras, combinações impossíveis de letras, probabilidade de uma palavra começar com determinada letra, tamanho médio de uma palavra, entre outras estratégias. No português, por exemplo, há a seguinte frequência de ocorrência das letras:

Figura 2: tabela de frequência das letras no português

Letra	Freqüência		Letra	Freqüência
A	14.63%		N	5.05%
B	1.04%		O	10.73%
C	3.88%		P	2.52%
D	4.99%		Q	1.20%
E	12.57%		R	6.53%
F	1.02%		S	7.81%
G	1.30%		T	4.34%
H	1.28%		U	4.63%
I	6.18%		V	1.67%
J	0.40%		W	0.01%
K	0.02%		X	0.21%
L	2.78%		Y	0.01%
M	4.74%		Z	0.47%

Fonte: UFRJ, 2024, online.

Através de tais análises, é possível identificar padrões que ocorreriam em um texto claro escrito naquela determinada língua que também ocorrerão dentro do texto criptografado, sendo possível assim, quebrar o código. Realizar tais análises pode não ser tão efetivo em textos curtos pois os padrões que são utilizados nas comparações talvez não apareçam, mas em mensagens maiores, é possível utilizar de tais recursos para descobrir qual era o texto original.

Com a difusão da análise de frequência, surgiu uma demanda por novas técnicas criptográficas mais seguras, passam então a surgir as cifras de substituição polialfabéticas, as quais utilizam dois ou mais alfabetos para a substituição das letras, como visto no capítulo anterior.

3.3 CONCEITOS MODERNOS DE CRIPTOGRAFIA

3.3.1 CHAVES SIMÉTRICAS E ASSIMÉTRICAS

Já dentro do contexto da criptografia pós-guerra, surgem os conceitos chaves simétricas e assimétricas, as quais a compreensão é de grande importância para a contextualização do funcionamento e da segurança do algoritmo RSA.

Primeiramente, é necessário abordar um grande problema deste período. Com o acesso a computadores se difundindo, a demanda por segurança através da criptografia deixou de ser algo limitado apenas aos militares e aos governos. Daí surge o problema de como distribuir de forma segura as chaves necessárias aos sistemas de criptografia que estavam sendo empregados em grande escala por computadores ao redor do mundo, conforme afirma Paixão (2020, p. 54)

> Assim, não nos causa espanto, que o principal problema ao final do século XX fosse a segurança da distribuição das chaves. Uma solução possível seria emissor e receptor encontrarem-se pessoalmente para a entrega da chave, mas isso não era viável na maioria dos casos, pois levaria tempo. Outra opção seria o uso de mensageiros, que viajariam entregando as chaves de forma segura.

Os algoritmos criptográficos que utilizam chaves simétricas são aqueles em que a mesma chave é utilizada tanto para criptografar quanto para descriptografar. Os métodos clássicos de criptografia apresentados no início deste capítulo se enquadrariam como de chave simétrica. Por exemplo, na cifra de César, o mesmo valor é utilizado tanto para encriptar a mensagem e seu receptor, utilizando o mesmo valor, previamente combinado, seria capaz de decifrar a mensagem.

Já os algoritmos de chave assimétrica contam com duas chaves diferentes associadas, uma utilizada para criptografar a mensagem e outra para

descriptografar.

O advento da criptografia de chave assimétrica, também conhecido como criptografia de chave pública, solucionou este grande problema da criptografia pós-guerra, que é o problema da distribuição de chaves.

3.3.2 NOÇÕES BÁSICAS SOBRE ALGORITMO DE CHAVE PÚBLICA

Como o próprio nome diz, os algoritmos de chave pública, ou de chave assimétrica, consistem em utilizar pares de chaves associadas, uma para codificar, que é pública e pode ser divulgada sem que se comprometa a segurança e uma outra utilizada para decodificar, a qual é privada e não pode ser descoberta. A criação de tal estratégia soluciona o problema da distribuição de chaves porque elimina a necessidade de compartilhar uma única chave de forma segura.

Por exemplo, uma pessoa que vá fazer uma compra numa loja online e precise inserir os dados de seu cartão de crédito. A loja envia a sua chave pública para o cliente que a utiliza para criptografar os dados e os envia para a loja que, em posse dos dados criptografados, utiliza sua chave privada para decifrar a mensagem. Deste modo, havendo uma terceira pessoa que possa vir a interceptar tanto a chave pública da loja quanto a mensagem cifrada que está sendo comunicada, não conseguirá decifrar, pois não possui a chave privada, que não precisa ser divulgada na comunicação.

4 CRIPTOGRAFIA RSA

4.1 INTRODUÇÃO AO MÉTODO RSA E SUA IMPORTÂNCIA NA CRIPTOGRAFIA MODERNA

O RSA surge dentro do contexto da criação dos métodos criptográficos de chave pública e se tornou um dos algoritmos mais difundidos devido à sua segurança e simplicidade.

A sigla advém do nome de seus criadores, Ron Rivest, Adi Shamir e Leonard Adleman que, em 1977, debruçaram-se sobre o problema de criar uma

função que fosse simples, mas que a determinação de sua inversa (decriptação) fosse essencialmente difícil.

4.2 PROCESSO DE ENCRIPTAÇÃO E DECRIPTAÇÃO

Inicialmente, para codificar uma mensagem através do método RSA, é necessário escrever o texto como um código numérico e, em seguida, dividi-lo em blocos que serão cifrados individualmente. Para a conversão do texto em números, utiliza-se uma tabela para referência:

Quadro 5: referência para pré-codificação no RSA

A	B	C	D	E	F	G	H	I	J	K	L
10	11	12	13	14	15	16	17	18	19	20	21
M	N	O	P	Q	R	S	T	U	V	W	X
22	23	24	25	26	27	28	29	30	31	32	33
Y	Z	0	1	2	3	4	5	6	7	8	9
34	35	36	37	38	39	40	41	42	43	44	45

Fonte: próprio autor.

Não são utilizados números com apenas um algarismo para que não haja ambiguidade. Se fosse utilizado 3 e 4 como os valores para C e D, haveria ambiguidade se 34 corresponderia a CD ou ao número 7, por exemplo. Para representar espaços entre as palavras, é possível utilizar o número 99.

Em seguida, é necessário que o texto seja dividido em blocos para que sejam codificados separadamente. Os blocos não precisam possuir um tamanho padronizado, mas é necessário que não correspondam ao tamanho de uma palavra, para impossibilitar a contagem de frequência.

Define-se então o valor n, o qual é o produto de dois números primos p e q escolhidos. Este valor deve ser maior do que o tamanho dos blocos em que se partiu a mensagem original.

Para a codificação da mensagem é utilizado o valor $n = p.\ q$ e um valor

inteiro e que possua inverso módulo $\phi(n)$, isto é, $\phi(n)$ e e devem ser coprimos. Estes valores serão a chave pública utilizada no método.

A codificação de um valor a para b se dará pelo cálculo do resto da divisão do expoente $a\ e$ por n, ou seja:

$$C(a) \equiv a\ e \equiv b\ (mod\ n)$$

Já para a decodificação de um bloco codificado b para a, utiliza-se o mesmo inteiro n e o inteiro d, que é o inverso de e módulo $\phi(n)$. Os valores n e d são a chave privada utilizada no método. A decodificação é feita através do cálculo do resto da divisão do expoente $b\ d$ por n, ou seja:

$$D(b) \equiv b^{\,d} \equiv a\ (mod\ n)$$

É possível demonstrar a garantia de que o valor obtido após o processo de decodificação sempre será o valor original demonstrando que $D(C(a)) \equiv a\ (mod\ n)$, pois tanto $D(C(a))$ quanto a estão compreendidos entre 0 e $n - 1$, então só podem ser iguais se forem congruentes módulo n.

Tem-se que $D(C(a)) \equiv (a^{\,e})^{\,d} \equiv a^{\,ed}\ (mod\ n)$ e que $ed \equiv 1\ (mod\ \phi(n))$, ou seja, $ed = k.\phi(n) + 1 = k.\ (p - 1).\ (q - 1) + 1$. Temos então que:

$$D(C(a)) \equiv a^{\,ed} \equiv a^{\,k.\phi(n)+1} \equiv (a^{\,\phi(n)})^{\,k}.\ a\ (mod\ n)$$

Caso a e n sejam coprimos, é válido o teorema de Euler, então:

$$D(C(a)) \equiv (a^{\,\phi(n)})^{\,k}.\ a \equiv 1^{\,k}.\ a \equiv a\ (mod\ n)$$

Chegando na conclusão desejada.

Caso não sejam coprimos, analisa-se o resto da divisão de $a\ ed$ por um dos fatores primos de n, p ou q, para que seja possível aplicar o teorema de Fermat.

Tem-se então:

$$a^{\,ed} \equiv a^{\,k.(p-1).(q-1)+1} \equiv (a^{\,p-1})^{\,k.(q-1)}.\ a\ (mod\ p)$$

Pelo teorema de Fermat, para p primo, se $p \nmid a$, então $a^{\,p-1} \equiv 1\ (mod\ p)$, obtendo:

$$(a^{p-1})^{k.(q-1)} . a \equiv 1^{k.(q-1)} . a \equiv a \ (mod\ p)$$

Para o caso em que $p|a$, tem-se $a \equiv 0\ (mod\ p)$, então $a^{ed} \equiv 0 \equiv a\ (mod\ p)$.

Da mesma forma, confirma-se que a congruência também é válida em módulo q, então $a^{ed} \equiv a\ (mod\ p)$ e $a^{ed} \equiv a\ (mod\ q)$, o que quer dizer que tanto p quanto q dividem $a^{ed} - a$. Como p e q são primos distintos e $n = pq$, então n divide $a^{ed} - a$, portanto, $a^{ed} \equiv a\ (mod\ n)$.

Confirma-se então que, em qualquer caso, dentro das condições impostas para o funcionamento do algoritmo, a congruência $D(C(a)) \equiv a^{ed} \equiv a\ (mod\ n)$ é verdadeira, então $D(C(a)) = a$, provando que é obtido sempre o valor do texto original após a decodificação.

Percebe-se que os conceitos de teoria dos números abordados no capítulo 2 deste trabalho são de extrema importância para o funcionamento do método RSA e a compreensão do algoritmo é intrinsecamente ligada à compreensão dos conceitos trabalhados.

Todo o processo de cifragem e decifragem depende da aritmética modular, dos teoremas de Fermat e Euler, do algoritmo de Euclides estendido e da função de Euler.

Além do funcionamento e da compreensão, a segurança do sistema também é diretamente ligada à fatoração de n, a qual depende de fatores também abordados no capítulo sobre teoria dos números. A explicação sobre a segurança se dará no próximo capítulo.

4.2.1 DEMONSTRAÇÃO DO PROCESSO DE CODIFICAÇÃO E DECODIFICAÇÃO

Será codificada a mensagem “FACEF 2025” para demonstrar o processo descrito no capítulo anterior.

Inicialmente, utilizando o quadro 5 como referência, faz-se a précodificação da mensagem, obtendo a sequência “15101214159938363841”. Em seguida, parte-se a mensagem em blocos para que cada unidade numérica não seja

maior que o valor de n. É possível dividir a sequência da seguinte forma: 15-101-21-41-59-93-83-6-38-41.

Define-se agora, aleatoriamente, os valores de p e q, obtendo também n. Para este exemplo será utilizado p = 53 e q = 5, daí vem $n = pq$ = 265. Calcula-se agora $\phi(n)$ = (53 − 1). (5 − 1) = 52.4 = 208 e busca-se um e co-primo com 208, que será 11.

Com os valores da chave pública definidos (265, 11), codifica-se cada bloco individual da mensagem através do método descrito no capítulo anterior. Na codificação do primeiro bloco, será demonstrado uma das formas que se pode prosseguir para o cálculo do resto de expoentes através da aritmética modular, onde reescreve-se o expoente em expoentes menores, os quais os resultados sejam suficientemente pequenos, facilitando a conta do resto modular de cada um desses expoentes de forma individual:

• $C(15) \equiv 15^{11} (mod\ 265)$

$\equiv (15^3)^3 . 15^2 (mod\ 265)$

$\equiv 3375^3 . 225 (mod\ 265)$

$\equiv 195^3 . 225 (mod\ 265)$

$\equiv 195^2 . 195.225 (mod\ 265)$

$\equiv 38025.43875 (mod\ 265)$

$\equiv 130.150 (mod\ 265)$

$\equiv 19500 (mod\ 265)$

$\equiv 155 (mod\ 265)\ C(15)$

$\equiv 155 (mod\ 265)$

O bloco 15 será codificado para 155;

• $C(101) \equiv 101^{11}\ (mod\ 265)$

$C(101) \equiv 86\ mod\ (265)$

O bloco 101 será codificado para 86;

• $C(21) \equiv 21^{11}\ (mod\ 265)$

$C(21) \equiv 151\ mod\ (265)$

O bloco 21 será codificado para 151;

• $C(41) \equiv 41^{11}\ (mod\ 265)$

$C(41) \equiv 51\ mod\ (265)$

O bloco 41 será codificado para 51;

• $C(59) \equiv 59^{11}\ (mod\ 265)$

$C(59) \equiv 184\ mod\ (265)$

O bloco 59 será codificado para 184;

• $C(93) \equiv 93^{11}\ (mod\ 265)$

$C(93) \equiv 37\ mod\ (265)$

O bloco 93 será codificado para 37;

• $C(83) \equiv 83^{11}\ (mod\ 265)$

$C(83) \equiv 182\ mod\ (265)$

O bloco 83 será codificado para 182;

• $C(6) \equiv 6^{11} \ (mod\ 265)$

$C(6) \equiv 131 \ mod \ (265)$

O bloco 6 será codificado para 131;

• $C(38) \equiv 28^{11} \ (mod\ 265)$

$C(38) \equiv 57 \ mod \ (265)$

O bloco 38 será codificado para 57;

• $C(41) \equiv 4111 \ (mod\ 265)$

$C(41) \equiv 51 \ mod \ (265)$

O bloco 41 será codificado para 51;

Portanto, o texto cifrado ficará: 155-86-151-51-184-37-182-131-57-51.

Para decifrar o texto, precisa-se do valor de d, inverso de e módulo $\phi(n)$. Para isto, é utilizado o algoritmo de Euclides estendido. O que se busca é a solução para 11. $d \equiv 1 \ (mod\ 208)$, que pode ser interpretado como 11. $d - 1 = 208. q$, implicando em 11. $d + 208. (-q) = 1$. Tem-se então:

$$208 = 11.18 + 10 \rightarrow 10 = 208 - 11.18$$

$$11 = 10.1 + 1 \longrightarrow 1 = 11 - 10.1$$

$$1 = 11 - 1. (208 - 11.18)$$

$$1 = -1.208 + 19.11$$

Obtém-se $d = 19$. Os valores d e n configuram a chave privada, a qual é usada para decifrar a mensagem. Aplicando o algoritmo sobre cada um dos blocos cifrados individualmente obtém-se:

• $D(155) \equiv 155^{19} \ (mod\ 265)$

$D(155) \equiv 15 \ (mod\ 265)$

O bloco 155 é decriptado para 15;

• $D(86) \equiv 86^{19} \ (mod\ 265)$

$D(86) \equiv 101 \ (mod\ 265)$

O bloco 86 é decriptado para 101;

• $D(151) \equiv 151^{19} \ (mod\ 265)$

$D(151) \equiv 21 \ (mod\ 265)$

O bloco 151 é decriptado para 21;

• $D(51) \equiv 51^{19} \ (mod\ 265)$

$D(51) \equiv 41 \ (mod\ 265)$

O bloco 51 é decriptado para 41;

• $D(184) \equiv 184^{19} \ (mod\ 265)$

$D(184) \equiv 59 \ (mod\ 265)$

O bloco 184 é decriptado para 59;

• $D(37) \equiv 37^{19} \ (mod\ 265)$

$D(37) \equiv 93 \ (mod\ 265)$

O bloco 37 é decriptado para 93;

• $D(182) \equiv 182^{19} \ (mod\ 265)$

$D(182) \equiv 83 \ (mod\ 265)$

O bloco 182 é decriptado para 83;

• $D(131) \equiv 131^{19} \ (mod\ 265)$

$D(131) \equiv 6 \ (mod\ 265)$

O bloco 131 é decriptado para 6;

• $D(57) \equiv 57^{19} \ (mod\ 265)$

$D(57) \equiv 38 \ (mod\ 265)$

O bloco 57 é decriptado para 38;

• $D(51) \equiv 51^{19} \ (mod\ 265)$

$D(51) \equiv 41 \ (mod\ 265)$

O bloco 51 é decriptado para 41;

Após a decriptação, é obtida a sequência 15-101-21-41-59-93-83-6-38-41, que através da tabela de pré-codificação, traduz-se exatamente para o texto original “FACEF 2025”.

4.3 SEGURANÇA DO RSA: FUNDAMENTOS E VULNERABILIDADES

A segurança do RSA está diretamente ligada à dificuldade de fatorar números grandes. No exemplo dado para a ilustração do algoritmo utilizamos valores pequenos, os quais numa aplicação real não garantiriam segurança alguma, uma vez que é possível rapidamente encontrar os valores da chave privada.

Para quebrar um código cifrado pelo algoritmo, é necessário a obtenção do valor d a partir dos valores n e e, que são públicos. No exemplo, vimos que é simples encontrar d se se sabe o valor de $\phi(n)$, bastando aplicar o algoritmo de Euclides estendido, mas, para saber o valor de $\phi(n)$, precisa-se saber os valores de p e q, os quais são restritos a quem definiu os valores incialmente. Paixão (2020), afirma:

> Com a possibilidade de usar números tão grandes quanto se queira e a dificuldade de fatorá-los, garantir a insegurança da RSA viria por dois meios: um salto teórico no campo matemático, como a descoberta de um método rápido e eficaz para a fatoração de números ou um salto tecnológico que garantiria a criação de computadores potentes e capazes de fazer muitas operações matemáticas em um número bastante reduzido de tempo.

A única forma possível de encontrar $\phi(n)$ sem saber os fatores primos de n, é o fatorando, o que, apesar de não ser impossível, é uma tarefa difícil e demorada dentro do atual contexto da computação. Para fatores de n suficientemente grandes, fatora-lo dentro dos limites dos computadores contemporâneos é inviável, podendo levar mais tempo do que o tempo de vida do universo (Coutinho, 2013, p. 157), o que garante a segurança do RSA.

5 CONSIDERAÇÕES FINAIS

Dentro do contexto atual de informatização cada vez mais difundida, com a migração de várias atividades cotidianas para o digital e aliado a uma demanda cada vez maior por segurança e sigilo nos meios digitais, a criptografia se vê cada vez mais protagonista, e o RSA é um método simples e robusto que supre tais necessidades, empregado em várias aplicações digitais que utilizamos diariamente, sendo alguns exemplos os protocolos https, certificados digitais, assinaturas digitais, aplicativos de trocas de mensagem e e-mail, proteção de dados em nuvem, pagamentos online, entre outros.

Contudo, é de se esperar que novas formas de criptografia surjam com o tempo, já que lidamos com uma informatização cada vez maior, de onde surgirão demandas cada vez mais específicas, como as criptomoedas, por exemplo. A criação de computadores cada vez mais rápidos, ou até mesmo com o advento da

computação quântica, pode colocar em xeque a segurança do algoritmo e de métodos semelhantes, uma vez que a velocidade das operações realizadas por estes processadores pode conseguir fatorar rapidamente os valores necessários para quebrar os códigos. Alguns métodos de criptografia importantes que surgem posteriormente ao RSA são o PGP e o SHA (Secure Hash Algorithm), o qual possui grande aplicação no contexto das criptomoedas, cada vez mais presentes e debatidas.

De qualquer forma, a relevância do método RSA é inquestionável por lançar ao público o conceito da criptografia de chave pública, indispensável para as aplicações utilizadas diariamente por todos, e que mantém, até o presente momento, uma grande confiabilidade.

REFERÊNCIAS

CARNEIRO, Framilson José Ferreira. **Criptografia e Teoria dos Números**. Rio de Janeiro: Ciência Moderna LTDA, 2017.

COUTINHO, Severino Collier. **Criptografia**. Rio de Janeiro: IMPA, 2013.

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2023. Decifrando Textos em Português. Disponível em: . Acesso em 03 de outubro de 2024.

GARCIA, Allyson da Silva. **Teoria dos Números e Criptografia**. Revista Matemática e Educação / Uni-FACEF Centro Universitário Municipal de Franca. v.1, n.10 (2020), p. 193-216. Franca: Uni-FACEF, 2020.

HEFEZ, Abramo. **Iniciação á Aritmética**. Rio de Janeiro: IMPA, 2015.

KAHN, David. **The Code-breakers:** The Comprehensive History of Secret Communication from Ancient Times to the Internet. Nova Iorque: Scribner, 1996.

PAIXÃO, Jéssica Shayanne da. **Criptografia:** história, atividades e divulgação científica. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. São Carlos -SP. 2020.

PROGRAMA DE INICIAÇÃO CIENTÍFICA DA OBMEP. **Aritmética - Aula 21 - Algoritmo de Euclides revisitado.** YouTube, 01 de agosto de 2013. 21min48s. Disponível em: . Acesso em 03 de outubro de 2024.

PROGRAMA DE INICIAÇÃO CIENTÍFICA DA OBMEP. **Aritmética - Aula 54 - Pequeno Teorema de Fermat.** YouTube, 09 de junho de 2014. 13min52s. Disponível em: . Acesso em 03 de outubro de 2024.

SANTOS, José Plinio de Oliveira. **Introdução à Teoria dos Números**. Rio de Janeiro: SBM,1998.

SILVA, Willian Wallace de Matteus. **A evolução da criptografia e suas técnicas ao longo da história**. Trabalho de conclusão de curso (bacharelado em sistemas de informação) – Instituto Federal Goiano. Ceres – GO. 2019.

SIMON, Singh. **O livro dos códigos:** a ciência do sigilo – do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. São Paulo: Pearson Education do Brasil, 2015. 47 Tabula Recta. Disponível em: . Acesso em 03/10/2024.