INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARANÁ – IFPR – CAMPUS CAPANEMA

PEDRO AUGUSTO GLUSZEWICZ SANTANA

A MATEMÁTICA DA CRIPTOGRAFIA RSA

CAPANEMA - PR

2024

PEDRO AUGUSTO GLUSZEWICZ SANTANA

A MATEMÁTICA DA CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática do Instituto Federal do Paraná, como um dos requisitos parciais de avaliação.

Orientador(a): Dra. Amanda Ferreira de Lima

CAPANEMA

2024

FOLHA DE APROVAÇÃO

PEDRO AUGUSTO GLUSZEWICZ SANTANA

A MATEMÁTICA DA CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso aprovado como requisito parcial para a obtenção do título de Licenciado em Matemática do Instituto Federal do Paraná, formada pela seguinte banca examinadora

Orientadora:

Amanda Ferreira de Lima

Profª. Drª. Amanda Ferreira de Lima

Banca examinadora:

gov.br Documento assinado digitalmente
EVERTON ARTUSO
Data: 26/08/2024 10:18:17-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Everton Artuso

Carina M. Costa

Profª. Drª. Carina Moreira Costa

Capanema, 16 de Agosto de 2024

AGRADECIMENTOS

Primeiramente agradeço a toda minha família pelo apoio e carinho para concluir minha primeira graduação, muita paciência e muitas trocas de ideias que ocorreram principalmente por conta dos meus estudos, em segundo lugar a todos os professores do IFPR Capanema pelo caráter, dedicação, paciência e carinho, vocês com certeza mudaram minha maneira de ver o mundo, sempre costumo dizer que existe um “Pedro” antes de começar essa graduação e um depois, em terceiro lugar vem meus amigos dos quais também me deram incentivo, forças, ótimas ideias e que também ajudaram como podiam para que todos esses anos eu tivesse excelência em meus estudos e aprendizagem, muitas horas de dispêndio de suas vidas para que isso tudo acontecesse.

“Aprender Matemática não é simplesmente compreender a Matemática já feita, mas ser capaz de fazer investigação de natureza matemática. Só assim se pode verdadeiramente perceber o que é a Matemática e a sua utilidade na compreensão do mundo e na intervenção sobre o mundo.” (Braumann, 2002, p.5)

RESUMO

O objetivo deste trabalho é realizar uma investigação bibliográfica sobre a história e os fundamentos matemáticos da criptografia, com um enfoque na criptografia RSA. A criptografia desempenha um papel crucial na segurança das informações transmitidas diariamente através dos sistemas de comunicação modernos. Iniciando com o desenvolvimento da criptografia, desde a sua utilização pelas culturas antigas até o seu papel em guerras e governos que permearam a história até culminar na presença que exerce hoje com o advento das tecnologias. Na sequência, traz a evolução dos métodos criptográficos até chegar à criptografia assíncrona, essa amplamente utilizada em nossos dispositivos atuais. A criptografia RSA, em destaque neste trabalho, é explorada através de seus conceitos matemáticos subjacentes e de uma análise sobre sua segurança, mesmo após mais de quatro décadas de avanços tecnológicos. A dificuldade em quebrar o padrão RSA é discutida, mostrando que este sistema continua a ser uma escolha confiável para a proteção de dados sensíveis. Este estudo também aborda a importância da criptografia na sociedade moderna e sua aplicação prática, fornecendo uma visão abrangente e intrigante sobre o tema.

Palavras-chave: Criptografia, História da Matemática, Criptologia, Criptografia RSA, Álgebra, Teoria dos Números.

SUMÁRIO

Sumário

1. INTRODUÇÃO

A criptografia está onipresente na vida moderna, protegendo as informações que trocamos diariamente, seja ao acessar contas bancárias, realizar compras online ou enviar mensagens através de diversos canais de comunicação. Com o advento da internet e das tecnologias digitais nas últimas décadas, a necessidade por segurança e privacidade de dados tornou-se cada vez mais exacerbada. No entanto, a criptografia não é uma invenção recente. Seu surgimento remonta aos primórdios da civilização, já que utilizada por antigos faraós egípcios para proteger comunicações vitais.

Nesse diapasão, a criptografia teve seu papel central em conflitos e guerras ao longo dos séculos, em especial na Segunda Guerra Mundial, momento em que a quebra de códigos complexos foi crucial na ocorrência de batalhas e estratégias militares. Dada sua importância nos eventos históricos, as técnicas foram evoluindo substancialmente, no entanto ainda permanece a necessidade por seu aprimoramento para o alcance da plenitude da segurança nas informações às quais a sociedade tem acesso. A constante evolução das técnicas criptográficas reflete a necessidade incessante de aprimorar a segurança da informação em resposta aos novos desafios e ameaças. À medida que os métodos de interceptação e decodificação de dados se tornam mais sofisticados, adversários determinados e cibercriminosos lançam desafios contínuos à integridade e confidencialidade das informações. Assim, o desenvolvimento e o aperfeiçoamento das técnicas criptográficas são essenciais para proteger os dados contra essas ameaças em constante evolução.

Neste contexto, se destaca como uma das técnicas a criptografia RSA, desenvolvida em 1977 por Ronald Rivest, Adi Shamir e Leonard Adleman, representando um dos marcos mais significativos da criptografia moderna. Ao introduzir o conceito de criptografia de chave pública, a RSA revolucionou a forma como protegemos dados, uma vez que fez as comunicações digitais se transformarem devido ao significativo nível de segurança que propiciara nelas.

Assim, este trabalho tem por finalidade explorar a trajetória histórica da criptografia desde suas origens até os avanços contemporâneos, com um enfoque detalhado na criptografia RSA. Nele, serão abordados os princípios matemáticos que

sustentam o RSA, demonstrando como a teoria dos números e a álgebra modular se entrelaçam para formar um dos sistemas criptográficos mais robustos da atualidade. Além disso, tem por objetivo evidenciar a relevância contínua da criptografia RSA em um mundo cada vez mais digitalizado e vulnerável a ataques cibernéticos.

Em um cenário global onde a informação é rapidamente difundida e altamente valiosa, compreender e aplicar a criptografia torna-se imperativo. Através deste estudo, almeja-se não apenas traçar a evolução da criptografia mesclada aos princípios matemáticos envolvidos, mas também inspirar uma apreciação mais profunda pela matemática e pela ciência que sustentam a proteção de dados, com vistas a aprimorar a segurança de nações e indivíduos.

2. A EVOLUÇÃO HISTÓRICA DA CRIPTOGRAFIA

A priori vamos expor os conceitos básicos que serão utilizados neste trabalho, a posteriori abordaremos a história da criptografia desde a antiguidade até a contemporaneidade.

2.1 Conceitos Básicos

Vejamos alguns termos:

Cryptos vem do grego e tem seu significado como secreto e oculto.

Código ou Cifra consiste em uma combinação de símbolos e letras de forma sistemática que permite a representação de uma determinada informação. Conforme Singh (2000, p. 47) “Tecnicamente, um código é a substituição de palavras ou frases, enquanto uma cifra é a substituição de letras”. Assim, um código altera a estrutura da mensagem de forma mais complexa que uma cifra.

Criptoanálise é o estudo de métodos para decifrar ou quebrar sistemas criptográficos, com o proposito de desvendar mensagens criptografadas sem precisar do acesso à chave de descriptografia. Técnicas matemáticas, estatísticas e computacionais são aplicadas para encontrar padrões e revelar o conteúdo original. “Ela, no entanto, admite possibilidade de erro, mesmo que racionalizado, sistematizado ou mecanizado” (DuPont 2017, tradução nossa).

Criptografia é o estudo e a prática de técnicas para proteger a comunicação contra terceiros, garantindo que apenas o remetente e o destinatário pretendidos possam ler a mensagem. Segundo Coutinho (2005), "ela é a arte dos códigos secretos, que desde criança já praticamos de alguma forma."

Criptografar (Cifrar ou Codificar) é a técnica de aplicar criptografia para transformar uma mensagem inicial em um criptograma.

Criptograma é a mensagem resultante após ser aplicada uma técnica de criptografia.

Descriptografar (Decodificar) é a técnica de reverter a criptografia, transformando um criptograma de volta na mensagem inicial utilizando a **chave** adequada.

Decifrar ou Quebrar um código refere-se ao processo de criptoanálise para descobrir a mensagem original quando não há acesso à chave de descriptografia.

Nota-se que estamos fazendo uma distinção de dois termos, Decifrar/Quebrar e Descriptografar/Decodificar.

Criptologia é a disciplina científica que engloba a criptografia e a criptoanálise, bem como a esteganografia. Segundo Couto (2008, p.18), "estuda os conhecimentos e as técnicas necessárias para a realização da criptoanálise, criptografia e a esteganografia."

Esteganografia estuda métodos para esconder uma determinada informação em outra mensagem ou objeto físico, por exemplo, usar tinta invisível entre linhas visíveis de um jornal, piscar repetidamente em código Morse, ou ocultar mensagens dentro dos bits de uma foto ou arquivo de som.

Um caso conhecido atualmente é o de Zheng Xiaoqing, cidadão americano que trabalhava no setor de energia da General Eletric Power. Segundo dados da BBC News (2023) “..., ele escondeu arquivos confidenciais roubados do seu empregador no código binário da fotografia digital de um pôr-do-sol, que ele encaminhou para si próprio”. Este pode ser um exemplo de espionagem de dados utilizando esteganografia.

No caso das cifras, podemos classificá-las em Cifras de Substituição e as Cifras de Transposição.

As **Cifras de Transposição** alteram a ordem dos caracteres no texto a ser cifrado. Em vez de substituir letras por outras, como nas cifras de substituição, as cifras de transposição reorganizam as letras ou símbolos, por exemplo por meio de anagramas, da seguinte forma: CARRO pode ser escrito como ARCRO.

Contudo, o método mais usado antigamente era o da Cifra das Colunas:

Exemplo: A mensagem:

Faça_uma_transação_de_mil_reais_da_conta_x_para_outra_conta_y

Colocando-a em um bloco de 8 colunas, obtemos o seguinte bloco:

F	**A**	**Ç**	**A**	_	**U**	**M**	**A**
_	**T**	**R**	**A**	**N**	**S**	**A**	**Ç**
Ã	**O**	_	**D**	**E**	_	**M**	**I**
L	_	**R**	**E**	**A**	**I**	**S**	_
D	**A**	_	**C**	**O**	**N**	**T**	**A**
_	**X**	_	**P**	**A**	**R**	**A**	_
O	**U**	**T**	**R**	**A**	_	**C**	**O**

N	**T**	**A**	**_**	**Y**	**.**	*****	*****

Tabela 1 - Cifra de Transposição - Bloco de 8 colunas

Perceba que, para criar esse bloco, foi preciso adicionar algum símbolo para espaços em branco do bloco com colunas. Isto serve para que não ocorram problemas no processo de descriptografia. Para cifrar esta mensagem, usaremos a cifra (chave): 5 2 8 4 1 6 3 7, ou seja, vamos alternar as colunas na sequência da chave (a quinta coluna será transposta para a primeira, a oitava coluna será transposta para a terceira e assim por diante, resultando na tabela cifrada:

_	**A**	**A**	**A**	**F**	**U**	**Ç**	**M**
N	**T**	**Ç**	**A**	**_**	**S**	**R**	**A**
E	**O**	**I**	**D**	**Ã**	**_**	**_**	**M**
A	**_**	**_**	**E**	**L**	**I**	**R**	**S**
O	**A**	**A**	**C**	**D**	**N**	**_**	**T**
A	**X**	**_**	**P**	**_**	**R**	**_**	**A**
A	**U**	**O**	**R**	**O**	**_**	**T**	**C**
Y	**T**	*****	**_**	**N**	**.**	**A**	*****

Tabela 2 - Cifra de Transposição - Bloco de 8 colunas

Isso resultará na seguinte mensagem cifrada:

_aaafuçmntça_sraeoidã__ma__elirsoaacdn_tax_p_r_aauoro_tcyt*_n.a*

Para descriptografar a mensagem, basta repetir os mesmos passos transpondo as colunas na mesma ordem da chave.

Já no tocante à Cifra de Substituição, esta trabalha com a substituição de uma letra por um símbolo, de acordo com uma determinada tabela de substituição, por exemplo:

A=4	**B=8**	**C=¢**	**D=>**	**E=3**	**F=F**	**G=6**	**H=#**
I=!	**J=J**	**K=K**	**L=1**	**M=¨**	**N=Z**	**O=0**	**P=9**
Q=@	**R=R**	**S=5**	**T=7**	**U=U**	**V=V**	**W=W**	**X=***
Y=Y	**Z=N**	**Ã=ª**	**Ó=º**				

Tabela 3 - Cifra de Substituição - Tabela de Substituição

Exemplo: O criptograma é:

3u zª0 9r3c!50 >3 ¨u!70 94r4 53r f31!n

5º >3 u¨ v!01ã0 3 u¨ 80¨ 50¨ z0 4r
3u c4z70 3 >4nç0 c0¨ @u3¨ @u!53r ¨3 0uv!r
3 46r4>3ç0 4 v!>4 90r ¨3 >3!*4r 50n#4r

Utilizando a tabela de substituição podemos descriptografar a informação e nos mostrará a seguinte mensagem:

Eu não preciso de muito para ser feliz
Só de um violão e um bom som no ar
Eu canto e danço com quem quiser me ouvir
E agradeço a vida por me deixar sonhar

Independentemente do método usado, agora temos noções de como a cifra geralmente possui uma única chave. Isso se enquadra no padrão de **Criptografia Simétrica**, em que o mesmo algoritmo e chave são utilizados tanto para criptografar quanto para descriptografar uma mensagem.

Com efeito, existe uma técnica mais avançada chamada Supercifragem. Nesse caso, é possível utilizar a mistura de métodos para tornar a cifragem ainda mais segura. Isso envolve combinar diferentes algoritmos criptográficos ou aplicar várias etapas de cifragem sequencialmente. A Supercifragem visa aumentar a robustez do sistema, dificultando ainda mais a quebra da criptografia por parte de atacantes.

Entretanto, temos sistemas muito mais seguros, tais como o padrão de **Criptografia Assimétrica**, a qual usa uma chave para criptografar e uma para descriptografar, sendo uma delas a **chave pública**, e a outra, **chave privada**. Por exemplo, quando a pessoa A precisa criptografar uma mensagem, ela usará a chave privada e enviará o criptograma para a pessoa B que usará a chave pública para descriptografar a mensagem. A pessoa B também pode criar um criptograma com a chave pública e enviar para a pessoa A, que fará a descriptografia com a chave privada.

No entanto, seja qual for a chave que possuir, é possível criptografar, mas não se pode descriptografar com a mesma chave, criando assim um sistema de mão única que gera um novo padrão de segurança e integridade do criptograma, pois não se pode calcular uma chave privada vindo de uma chave pública.

2.2 História

2.2.1 Origens Antigas da Criptografia

Na antiguidade, segundo Silva e Martins (2011 pg. 20), o surgimento da criptografia não ocorreu com um propósito específico a ocultar informações, deveras que a própria escrita de um povo pôde ser vista como um padrão criptográfico para outro, a partir de Bezerra, Malagutti e Rodrigues (2010 pg. 15). Podemos efetuar esta observação em duas fontes:

Uma tabuleta de argila encontrada num campo arqueológico da antiga babilônia (Figura 1), datada de cerca de 1800 a.C., trouxe o cálculo sexagesimal da raiz quadrada de 2 com sete casas decimais de precisão, a qual está na Coleção Babilônica de Yale do Museu Yale Peabody (New Haven, Connecticut, Estados Unidos):

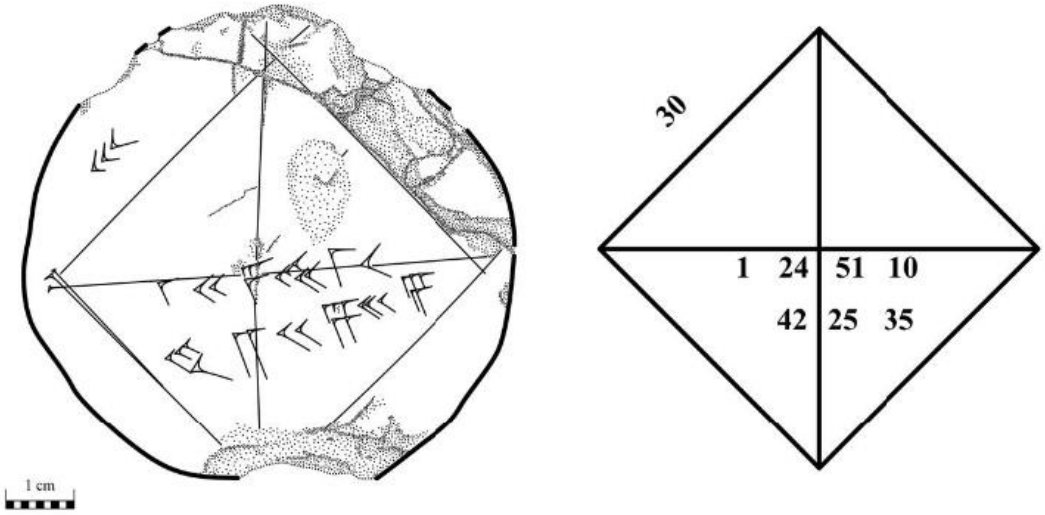

Figura 1 – Tabuleta de argila - YBC 07289, Yale Peabody Museum, BC.021354: (photo by Wagensonner, K., 2022)

Outro é a chamada **Pedra de Roseta** (Figura 2), segundo o British Museum (2017), foi uma descoberta crucial para a decifração dos hieróglifos egípcios, visto que forneceu uma chave que abriu a porta para a compreensão de uma civilização há muito perdida. Esta pedra, inscrita com o mesmo texto, um decreto emitido em Mênfis no Egito datado do século II a.C.-, em três scripts diferentes — hieróglifos egípcios, demótico e grego —, permitiu aos egiptólogos Thomas Young (1803) e Jean-François Champollion (1822), desvendarem o complexo sistema de escrita dos antigos egípcios. Ao comparar as inscrições, os estudiosos puderam correlacionar as formas

hieroglíficas com suas correspondências fonéticas e semânticas nas outras duas línguas, trazendo à tona o significado dos símbolos que haviam permanecido enigmáticos por séculos.

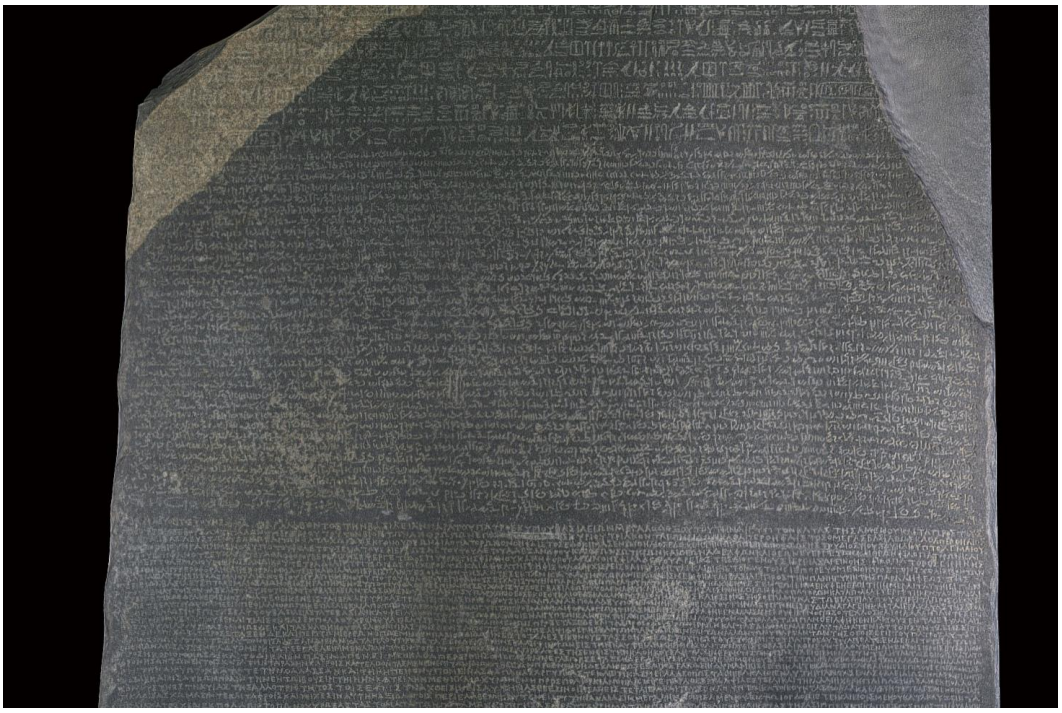

Figura 2 - Pedra de Roseta, Museu Britânico, (capturada da interface 3D em www.britishmuseum.org)

Silva e Martins (2011, p. 20) observaram que, além de serem utilizados em inscrições monumentais e textos religiosos, os hieróglifos desempenhavam um papel importante na vida cotidiana dos egípcios, desde na documentação administrativa até na escrita decorativa em artefatos pessoais e funerários. Essa ubiquidade sublinha a versatilidade e a importância cultural dos hieróglifos na antiga sociedade egípcia.

Embora a decifração dos hieróglifos represente um feito monumental na compreensão de antigos sistemas de escrita, é importante reconhecer que não se trata apenas da criptografia em sentido estrito. Isso porque a Pedra de Roseta não revelava tão somente um código secreto, mas sim todo um sistema de linguagem complexo e sofisticado, inovador para diversas épocas.

Assim, os próximos tópicos abordarão padrões criptográficos que foram desenvolvidos a fim de ocultar informações de maneira intencional e sistemática. Esses métodos não se limitavam à tradução de linguagens, mas introduziam técnicas sofisticadas para garantir a segurança e a privacidade das comunicações. Vamos mergulhar em como essas práticas evoluíram e como impactaram a segurança da informação ao longo da história.

Segundo Paixão (2020 pg. 27, apud Singh, 2007) Heródoto fez o primeiro relato usando criptografia no período do embate da Pérsia e Grécia no século V a.C. Resumindo o relato, um exilado grego que estava na Pérsia, chamado Demarato, teria ouvido os planos de Xerxes para atacar a Grécia. Então, Demarato com sua fidelidade à pátria resolveu enviar uma mensagem para Grécia. Usando tábuas de madeira encerada, ele raspou a cera das tábuas e fez o entalhe, Tendo escrito a mensagem, cobriu novamente as tábuas com cera a fim de conseguir ocultar a mensagem dos guardas persas. Suas informações foram entregues com êxito e a Grécia conseguiu se precaver do ataque persa.

Em outro relato, Heródoto narra o envio de uma mensagem que foi escrita na cabeça de um homem. Foi raspado o seu cabelo, escrita a mensagem em sua cabeça e quando o seu cabelo cresceu enviaram o homem a seu destino. Quando chegou lá, teve sua cabeça raspada novamente, e revelada, assim, a mensagem. Nesse relato, foi possível perceber que a técnica aplicada foi a esteganografia.

Segundo Pinto et al. (2014 pg. 5), ainda no século V a.C., tinha-se o bastão de Licurgo (Figura 3), utilizado pelo general espartano Panasius, o qual constituía-se de um bastão do tipo prisma octogonal em que uma tira de couro era enrolada em torno do bastão e nessa tira, era escrita uma mensagem. Depois, desenrolava-se a tira, que era usada como cinta pelo mensageiro no intuito de a camuflar, e a mensagem era enviada ao seu destinatário, que possuía um mesmo bastão com as mesmas características do bastão do emissor. Esse enrolava a tira no seu bastão e lia o conteúdo da mensagem escrita na tira.

Figura 3 – Bastão de Licúrgo - https://australianscience.com.au/technology/a-scytale-cryptography-of-the-ancient-sparta/

Outro método notável de criptografia da Grécia Antiga é a **Cifra Quadrada de Políbio** (Tabela 4), desenvolvida pelo historiador grego Políbio. Este método utilizava uma técnica de substituição de letras por pares de números, que se baseava em uma matriz de tamanho 5x5. Cada letra do alfabeto era posicionada em uma célula da matriz, e cada célula era identificada por um par de coordenadas — o número da linha e o número da coluna. Por exemplo, na matriz padrão, a letra 'A' poderia ser representada pelo par (1,1), 'B' por (1,2), e assim por diante.

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

Tabela 4 - Cifra de Substituição - Cifra Quadrada de Políbio

Por exemplo ΚΡΥΠΤΟΓΡΑΦΗΣΗ (criptografia em grego), com a tabela o criptograma seria: 2542454144351342112225 22.

A Cifra de Políbio era não só engenhosa, mas também prática, pois permitia a codificação de mensagens em formatos que podiam ser facilmente transmitidos por sinais de fumaça, bandeiras ou outros métodos visuais. Além disso, seu uso de números ao invés de letras ajudava a manter as mensagens cifradas seguras, mesmo quando os métodos tradicionais de interceptação eram empregados.

Este método destacou-se pela sua simplicidade e eficácia, proporcionando uma maneira eficiente de codificar e decodificar mensagens durante a Antiguidade. A **Cifra Quadrada de Políbio** não só teve um impacto significativo na história da criptografia, mas também exerceu uma influência duradoura em métodos posteriores de codificação e segurança de informações. Segundo Silva e Martins (2011, p. 25), seu valor histórico é inestimável, pois a estrutura fundamental da cifra serviu de base para o desenvolvimento de outras técnicas de criptografia. Entre essas técnicas,

destacam-se a **Cifra Playfair** e a **Cifra Campal Germânica**, ambas empregadas durante a Primeira Guerra Mundial.

Outra das cifras mais famosas da Antiguidade é a **Cifra de César**, nomeada em homenagem ao general romano Júlio César, que a utilizava para proteger suas comunicações militares. A Cifra de César é um exemplo clássico de cifra de substituição, onde cada letra do alfabeto é substituída por outra, deslocada para um número fixo de posições. No caso específico de César, ele frequentemente deslocava as letras em três posições para a direita: A se transformava em D, B em E, e assim por diante como mostra a Tabela 5. Assim, a mensagem original era transformada em uma sequência de letras aparentemente sem sentido, que só poderia ser lida se o destinatário soubesse o deslocamento aplicado.

Para aumentar a complexidade e reforçar a segurança da cifra, César às vezes usava letras do alfabeto grego em substituição às letras latinas, dificultando ainda mais a compreensão por parte de inimigos que interceptassem suas mensagens. Esta técnica simples, mas engenhosa, tornou-se um marco na história da criptografia.

Qualquer cifra que baseie sua codificação no deslocamento fixo de letras dentro de um alfabeto é considerada uma variante da Cifra de César. Sua simplicidade e eficácia proporcionaram um método robusto para manter seguras as comunicações na época, e seu legado continua a ser estudado e admirado no campo da criptografia.

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
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

Tabela 5 - Cifra de Substituição - Alfabética Cifra de César

2.2.2 Criptografia na Antiguidade Tardia e na Idade Média

Os hebreus, por volta do século V a VI a.C., também utilizavam a criptografia para seus textos religiosos. Segundo Pinto et al. (2014 pg. 5) eles possuíam cifras ATBASH, ALBAM e ATBAH, que consistia em uma substituição simples monoalfabética de uma letra para outra de seu alfabeto. Com isso, ATBASH (Figura 4) utilizava o seu alfabeto reverso, por exemplo a primeira letra a (aleph) codificada seria a letra t (taw), a letra b (beta) pela letra s (shin) e assim por diante, abaixo temos um diagrama do alfabeto hebreu e suas substituições:

Plaintext Alphabet	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
Ciphertext Alphabet	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

Figura 4 - Atbash Cipher - crypto.interactive-maths.com/atbash-cipher

Em nosso alfabeto se apresentaria desse modo:

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

Figura 5 - Atbash Cipher - crypto.interactive-maths.com/atbash-cipher

No caso das variantes ALBAM e ATBAH, na ALBAM, utilizava-se a transposição de caracteres no alfabeto, ou seja, o alfabeto inicia-se na posição 12, e em ATBAH ocorre uma substituição e transposição, em que os nove últimos caracteres são transpostos de forma decrescente, em seguida os outros nove caracteres, da mesma forma, subsequentemente:

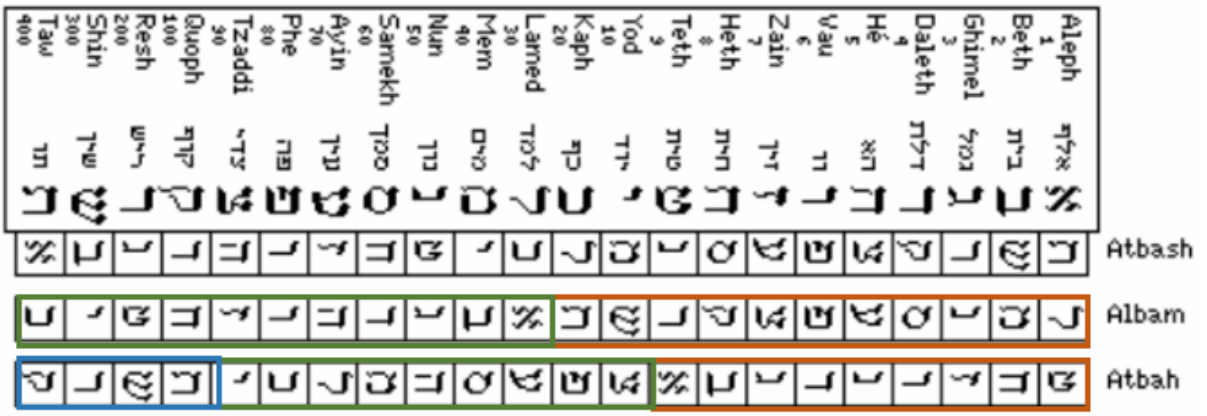

Figura 6 – Atbash, Alban and Atbah Cipher - https://www.apprendre-en-ligne.net/crypto/subst/atbash.html (editado pelo autor)

Durante a Idade Média, os muçulmanos destacaram-se como a civilização de maior avanço intelectual de seu tempo (DuPont, 2017). Por volta de 800 d.C., a fundação da Casa da Sabedoria (Bait al-Hikmah) em Bagdá marcou o início de um florescimento extraordinário de conhecimento. Este centro tornou-se um farol de erudição e um ponto de convergência para ideias de diversas culturas, promovendo uma era de intensa produção científica e cultural. A abertura e a tolerância aos conhecimentos estrangeiros fomentaram avanços significativos nas artes, na medicina e, de maneira notável, na matemática.

Os muçulmanos tiveram um papel essencial no desenvolvimento da criptoanálise, com o estudo da decifração de mensagens cifradas em

correspondências e textos de outras civilizações. Al-Kindi, um eminente filósofo, cientista e matemático conhecido como o “filósofo dos árabes” e o “bisavô da estatística” (Silva e Martins, 2011, p. 26), foi uma figura central nesse campo. Ele produziu cerca de 290 obras sobre uma variedade de assuntos, mas sua contribuição mais notável à criptoanálise só foi descoberta em 1987 nos arquivos da Biblioteca Sulaymaniyya, em Istambul, Turquia. Este acervo contém o maior número de manuscritos islâmicos do mundo.

Dentre eles, encontrou-se o manuscrito intitulado “Um Manuscrito sobre Decifração de Mensagens Criptografadas”, que detalha o uso da análise de frequência para decifrar textos cifrados. Este método, que examina a frequência das letras para identificar padrões no texto, é um marco na criptoanálise. Embora não se saiba com certeza se foi Al-Kindi quem criou a técnica, o manuscrito é o mais antigo registro conhecido desse método (DuPont, 2017), sublinhando a profundidade das contribuições islâmicas para a criptoanálise e a ciência como um todo.

Outra figura notável foi Al-Khalil, que precedeu Al-Kindi. Ele desenvolveu um método inovador conhecido como “Método da Palavra Provável”. Al-Khalil, ao observar que muitos textos antigos do Império Bizantino começavam com a frase “Em nome de Deus”, usou essa regularidade para criar um sistema de decifragem baseado em palavras e frases frequentes. Este método foi uma solução engenhosa para os criptogramas da época e representou um avanço significativo na criptoanálise.

Para muitos estudiosos árabes dessa era, as palavras eram consideradas portadoras de um significado profundo e esotérico. Como DuPont (2017) sugere, para os muçulmanos, a linguagem não era apenas um meio de comunicação, mas também uma entidade sagrada e codificada. Esse reverente enfoque motivou muitos estudiosos a tentarem decifrar os textos do Alcorão em busca de novos entendimentos e conhecimentos ocultos. Nesse contexto, a criptoanálise e a tradução de textos antigos ganharam ainda mais importância e sofisticação, contribuindo significativamente para o avanço intelectual da civilização islâmica.

A partir do século XIII, a criptografia aparece na Europa. Seu uso se difunde principalmente por cientistas e alquimistas a fim de manter suas descobertas em sigilo (Paixão, 2020 pg. 31).

Em meados do século XV a criptoanálise ocidental se desenvolveu, sobretudo com a análise de frequência. Contudo, por mais que existam várias outras evidências históricas, não se sabe se esta proveio dos árabes ou de autoria própria.

Nessa época, a criptografia era muito usada para fins políticos, neste passo ainda era muito utilizado cifras de substituição para comunicação secreta, porém, com os avanços da criptoanálise, começa a ficar evidente de que este tipo de criptografia era ultrapassado.

2.2.3. Renascimento e o Desenvolvimento da Criptografia

Paixão (2020, pg. 31) e Singh (2000, pg. 18) contam a história da Rainha da Escócia chamada Mary, e seu trágico destino, em parte devido ao uso de cifras em suas cartas, constituindo um exemplo clássico da importância da criptografia e das consequências que uma criptoanálise eficaz pode fazer. Mary foi aprisionada pela então Rainha da Inglaterra, Elizabeth I, por quase 19 anos devido às ameaças que ela representava ao trono inglês tanto por suas próprias reivindicações, e por contar, para isso, com o apoio de católicos ingleses e estrangeiros.

Durante seu cativeiro, Mary se envolveu em várias conspirações para escapar e possivelmente usurpar o trono de Elizabeth. Para comunicar-se secretamente com seus aliados, Mary utilizou um sistema de cifra, confiando na segurança desta para esconder seus planos. No entanto, suas mensagens foram interceptadas por Sir Francis Walsingham, o astuto secretário de Elizabeth, que havia organizado uma rede eficaz de espionagem.

Walsingham empregou criptoanalistas habilidosos que conseguiram decifrar as mensagens cifradas de Mary. Uma dessas mensagens interceptadas foi a chave para desmascarar a conspiração de Babington em 1586, na qual Anthony Babington e outros católicos planejavam assassinar Elizabeth e colocar Mary no trono. A prova da participação de Mary nesta conspiração foi obtida através da decifração de suas cartas cifradas.

Apesar de Mary nunca ter se encontrado pessoalmente com os conspiradores, a correspondência decifrada forneceu evidências suficientes para condená-la por traição. Ela foi julgada e executada em 8 de fevereiro de 1587.

Este episódio histórico destaca não apenas a importância da criptografia para a comunicação segura, mas também os riscos associados quando a segurança de um

sistema de cifra é comprometida. A falha de Mary em reconhecer que sua cifra poderia ser quebrada, e a habilidade dos criptoanalistas de Elizabeth, selaram seu destino e serviram como um lembrete precoce da contínua batalha entre criptógrafos e criptoanalistas.

Singh (2000, pg. 13) faz uma analogia interessante sobre a criptografia e a criptoanálise, afirmando que uma bactéria funciona e vive em nosso corpo durante muito tempo, até que as pesquisas médicas conseguem um método para matá-las com o uso de antibióticos. Nesse passo, as bactérias precisam evoluir para se manterem vivas, até que os pesquisadores descubram outro tipo de antibiótico, fazendo com que elas precisem evoluir novamente, e o ciclo assim se repetindo. O mesmo ocorre com a criptografia, que precisou e precisa evoluir constantemente ao passo que os criptoanalistas revelem um novo método de quebrar o método criptográfico evoluído.

Um padrão desenvolvido para tornar o método de substituição mais seguro foi desenvolvido por Leon Battista Alberti, o qual utilizava-se de 2 alfabetos para a substituição. Usando uma tabela com 3 linhas, a primeira possuía o alfabeto original, a segunda possuía um alfabeto criptografado por substituição e a terceira outro alfabeto criptografado por substituição.

Neste caso, a substituição de palavras fazia a cada troca entre o primeiro e segundo alfabeto de substituição, a primeira letra usava o primeiro alfabeto já a segunda letra o segundo alfabeto, na terceira voltava para o primeiro alfabeto e assim por diante. Esse processo aumentava a segurança criptográfica e tornava mais complexo para os criptoanalistas decifrarem por meio da frequência de letras. Este padrão deu início à substituição polialfabética.

Anos mais tarde Blaise de Vigenère aprimorou o método criando o quadrado de Vigenère (Tabela 6). Por meio dessa técnica, era necessário possuir uma palavra chave para codificar e decodificar. A chave criada para codificar identificava, a partir de cada letra, qual alfabeto seria utilizado para a codificação, por exemplo a chave CASA. Como já vimos com Alberti, a cifra de Vigenère propunha que alfabeto utilizar sequencialmente, ou seja, o primeiro alfabeto de substituição seria o C, o segundo alfabeto o A, o terceiro o S e o quarto o A novamente. Na quinta letra, retornava o C e assim por diante.

	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	D
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	C
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	B
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

Tabela 6 - https://giacomel.blogspot.com/2015/11/tabela-de-vigenere.html

Como o quadro era disponibilizado para uso comum a entrada da chave o tornou o chamado “Le Chiffre Indéchiffrable” ou a cifra indecifrável, por não ser possível decifrar com a análise das frequências. Apesar de sua segurança, ela não foi utilizada com muita frequência, pois sua complexidade de criptografar e descriptografar dependendo da chave, tornava o método muito demorado e complexo. Assim, ela serviu bem para diplomatas e espiões que necessitavam de algo praticamente indecifrável. Quando não havia essa necessidade, a cifra de Alberti era mais empregada.

De acordo com Singh (2000, pg. 91), esse padrão de cifragem foi seguro até o século XIX, quando Charles Babbage, e, anos mais tarde Friedrich Kasiski, individualmente, descobriram métodos para quebrar a cifra. Eles perceberam que a repetição na chave poderia levar a padrões repetitivos que poderiam ser explorados no texto cifrado para quebrar a cifra.

2.2.4. Criptografia na Era Moderna

No século XX, com os avanços tecnológicos e matemáticos, a criptografia teve uma grande aliada. Anteriormente tudo se fazia de forma manual, mas, nessa época,

foi possível criar máquinas para criptografar e descriptografar um texto, a exemplo da Máquina Enigma.

A Enigma era uma máquina de cifragem eletromecânica que utilizava um sistema de rotores para embaralhar as letras do alfabeto (Singh 2000, pg. 172). Cada tecla pressionada fazia com que os rotores se movessem, alterando a configuração da cifra para cada letra digitada. Isso resultava em um vasto número de possíveis configurações, tornando a tarefa de decifrar uma mensagem sem conhecer as configurações iniciais dos rotores extremamente desafiadora.

Conforme Singh (2000, pg. 182), o esforço para quebrar a Enigma não foi realizado por um único indivíduo ou mesmo uma única nação. Contribuições significativas vieram de criptoanalistas poloneses, britânicos e franceses. Os poloneses, em particular, conseguiram replicar a máquina Enigma e desenvolver dispositivos, como a "Bomba Criptológica", que ajudaram a testar rapidamente as configurações dos rotores.

No Reino Unido, o matemático Alan Turing e sua equipe em Betchley Park desempenharam um papel crucial ao desenvolver métodos mais avançados para acelerar o processo de decifração das mensagens da Enigma. Turing projetou uma máquina chamada "Bombe", inspirada no dispositivo polonês, que automatizava o processo de busca por configurações de rotores que produziam texto legível em alemão.

A quebra do código da máquina Enigma foi o resultado de uma combinação de genialidade matemática, colaboração internacional, avanços tecnológicos e, também, de algumas boas doses de sorte e oportunismo, com a captura de máquinas e documentos chave. Este esforço coletivo não apenas contribuiu para a vitória dos Aliados na Segunda Guerra Mundial, mas também estabeleceu as bases para a criptografia moderna e a ciência da computação.

2.2.5. A Era da Criptografia Digital

O início da criptografia na era digital representa um marco na história da segurança da informação, marcando a transição de métodos de criptografia analógicos e manuais para sistemas baseados em computadores capazes de processar algoritmos complexos. Este período foi caracterizado pelo desenvolvimento

de novos algoritmos e pela democratização da criptografia, permitindo seu uso em uma escala global sem precedentes.

Com o advento dos computadores na segunda metade do século XX, a criptografia começou a se adaptar às possibilidades oferecidas pela computação digital. A capacidade de processar informações a uma velocidade e escala sem precedentes abriu caminho para o desenvolvimento de algoritmos criptográficos mais avançados e seguros.

O uso de algoritmos de chave simétrica, onde a mesma chave é usada para cifrar e decifrar uma mensagem, tornou-se comum. Exemplos notáveis são colocados por Abdullah (2017), que inclui o Data Encryption Standard (DES) e, posteriormente, o Advanced Encryption Standard (AES), que oferecem níveis de segurança robustos para comunicações seguras.

Segundo Singh (2000, pg. 304) um dos avanços mais significativos foi a introdução da criptografia de chave pública, também conhecida como criptografia assimétrica. Inventada por Whitfield Diffie e Martin Hellman em 1976, essa abordagem revolucionou a criptografia ao permitir que duas partes trocassem mensagens seguras sem a necessidade de compartilhar uma chave secreta com antecedência. O algoritmo RSA, desenvolvido por Ron Rivest, Adi Shamir e Leonard Adleman, é um exemplo proeminente dessa categoria.

A era digital também viu o desenvolvimento de protocolos de segurança para proteger a comunicação em redes, incluindo o Secure Sockets Layer (SSL) e seu sucessor, o Transport Layer Security (TLS). Estes protocolos utilizam criptografia para assegurar a privacidade e integridade dos dados transmitidos pela Internet.

O aumento da capacidade computacional também significou que métodos de criptoanálise se tornassem mais sofisticados, levando a uma corrida contínua entre criptógrafos e criptoanalistas. Isso culminou na necessidade por algoritmos criptográficos que pudessem resistir a análise, mesmo diante de adversários poderosos.

À medida que a sociedade se tornava cada vez mais digitalizada, a criptografia tornou-se fundamental para proteger a privacidade individual, transações financeiras e comunicações governamentais.

Além disso, forneceu base para a segurança da informação moderna, garantindo a confidencialidade, integridade e autenticação de dados no mundo digital.

À medida que entramos em novas eras de tecnologia, como a computação quântica, os princípios da criptografia continuam a evoluir frente aos novos desafios e agindo na proteção de informações contra adversários cada vez mais sofisticados.

3. CRIPTOGRAFIA RSA

3.1 História Da Criptografia RSA

Segundo Coutinho (2005, pg. 3), a criptografia RSA é um marco na evolução da criptografia moderna, uma vez que introduziu um dos primeiros algoritmos de criptografia de chave pública, permitindo a comunicação segura em canais inseguros sem a necessidade de compartilhar uma chave secreta de antemão. Desenvolvida por Ron Rivest, Adi Shamir e Leonard Adleman em 1978, enquanto trabalhavam no Massachussets Institute of Technology (M.I.T.), a criptografia RSA baseia-se na dificuldade matemática de fatorar grandes números compostos, particularmente o produto de dois grandes números primos.

A necessidade de segurança na comunicação digital remonta à criação da ARPAnet em 1969, uma rede precursora da Internet moderna. A ARPAnet foi inicialmente concebida para a transmissão segura de dados sigilosos entre departamentos de pesquisa e instalações militares dos Estados Unidos, visto que foi a pioneira em permitir a transmissão de pacotes de dados a longa distância entre computadores.

Com a expansão dessa rede, tornou-se imperativo desenvolver sistemas criptográficos mais robustos. Até aquele momento, a criptografia simétrica era o padrão. No entanto, essa abordagem apresentava desafios consideráveis: era necessário compartilhar as chaves de criptografia entre todos os destinatários, o que não só complicava a logística, mas também aumentava os riscos de segurança, pois a posse da chave por múltiplas partes potencializava a vulnerabilidade dos dados.

A história da RSA começa com o trio de pesquisadores Whitifield Diffie, Martin Hellman e Ralph Merkle. Diffie e Hellman eram criptógrafos, já Merkle era um matemático que se interessava por problemas de troca de chaves. Juntos, eles buscaram sistemas de mão única para criptografar uma determinada informação.

A priori tentaram utilizar uma função afim, porém esse processo ainda continuava com uma mão dupla (da mesma forma que era possível criar uma chave de criptografia, era possível criar uma mesma chave de descriptografia, utilizando o processo inverso).

Frente à esse desafio, cogitaram então utilizar a aritmética modular para criar um novo método, que se tornou um primeiro ponto de partida próspero para resolver

o problema da chave de mão única. Porém, este método ainda consistia em que a pessoa A e a pessoa B tivessem as primeiras chaves P (um número primo) e Y (uma base) para que efetuassem o cálculo da expressão $Y^x(mod\ P)$. No caso o valor de x era o único que era realmente secreto e cada uma das duas pessoas o escolhia, para ao fim, resolver a chave por completo. Silva e Martins (2011 pg. 53) dão um exemplo: se Y e P fossem respectivamente 5 e 13, e a pessoa A escolhesse o $x_a = 7$, e a pessoa B escolhesse o $x_b = 4$, e colocassem na função acima, chegariam nas respectivas chaves públicas: $A = 5^7(mod 13) = 8\ (mod 13)$ e $B = 5^4(mod 13) = 1(mod 13)$, no momento dessa troca de chaves (chaves A e B) eles utilizariam novamente a expressão e resolveriam cada um com seu x secreto, então a pessoa A pegaria a chave de B e escreveria do seguinte modo respectivamente:

$$B = 1^{x_a}(mod\ 13) = 1^7(mod\ 13) = 1.$$

Já a pessoa B pegaria a chave de A e escreveria do seguinte modo:

$$A = 8^{x_b}(mod\ 13) = 8^4(mod\ 13) = 1.$$

Neste caso as chaves chegando ao mesmo resultado, seriam válidas.

Por mais que estas chaves fossem válidas, permanecia o problema por precisar trocar a informação dessa chave, pois ainda havia o de compartilhamento de chaves no tocante à chave simétrica.

Posteriormente, Diffie estabelece um novo sistema chamado assimétrico, em que a chave de criptografia e chave de descriptografia eram diferentes, ou seja, se a pessoa A possui a chave de criptografia, esta não pode descriptografar com a mesma chave o criptograma. Neste caso temos a chave pública, a qual pode ser enviada para qualquer um que queira enviar mensagens para a pessoa A, já que ela é gerada ao mesmo tempo que sua chave privada, a qual é a chave de descriptografia.

Assim o sistema de mão única foi criado, porém Diffie não conseguira um método para esta implementação, era apenas uma teoria.

A construção de um método funcional foi dada por Riverst, Shamir e Adleman, que utilizando o conceito de Diffie chegaram à utilização de números primos, no caso p e q e o número n que é o produto de p e q, para criptografar uma mensagem utiliza-se o número n, mas para descriptografar é necessário conhecer p e q.

O exemplo de Silva e Martins (2011 pg. 57) elucida a ideia. Se a pessoa A criar n a partir dos primos 1933 e 9419, obtém 18206927. Esta é a chave pública. Para encontrar, porém, a chave privada teria que fatorar esse número, para obter p e q,

algo que utilizando primos pequenos já não é um trabalho muito simples e a torna uma “função de mão única”. Olhando por este ponto, ainda parece que é um trabalho pequeno para quebra da chave privada, porém para o RSA utiliza-se números primos na escala de 10^{65} pelo menos.

Coutinho (2016, pg. 10) vai além dando outra perspectiva. Através da chave RSA, para manter sua segurança, os primos escolhidos necessitam ter acima de 100 algarismos, sendo assim, o produto dos dois primos dará um número de cerca de 200 algarismos, e para fatorar um número desse tamanho, com os computadores atuais seriam necessários vários milhares de anos.

Para dar um exemplo de funcionalidade da criptografia RSA, podemos supor que uma determinada loja possui um sistema online de pagamentos. Esta loja cria as chaves públicas e privadas no padrão RSA, e a chave pública é vinculada a todo o cadastro do cliente. Assim, todos os dados como nome, endereço, CPF, telefone, números do cartão de crédito, são criptografados, criando assim o criptograma. Esse método é realmente muito simples e rápido.

Uma certa pessoa que intercepta esse criptograma, sabe que foi utilizado a criptografia RSA através de dados expostos como a chave pública da loja online, porém somente seria possível descriptografar o criptograma a partir da chave privada e é aí que se torna muito mais complexo.

Paixão (2020, pg. 113) utiliza uma analogia interessante, e que ilustra e compara os dados da pessoa como frutas, a criptografia RSA como um liquidificador e o criptograma como o suco dessas frutas após liquidificado. Nesta analogia, o ato de fazer o suco é simples, porém o ato de tornar o suco em frutas é impossível. Claro que esta analogia é ideal para quando estamos pensando em como este criptograma é estabelecido e não vale para o inverso, já que, mesmo que outro liquidificador fosse a chave privada, não conseguiria transformar suco em fruta, mas tem seu propósito de elucidar o quanto difícil ou mesmo impossível seria nos padrões atuais.

3.2 Pré-Requisitos Matemáticos

À medida que avançamos na exploração da criptografia RSA, é vital considerar os pré-requisitos matemáticos que fundamentam essa técnica criptográfica. Segundo Hefez (2013), em seu livro "Aritmética", a compreensão da

aritmética modular é essencial, pois ela forma a base para operações críticas dentro do algoritmo RSA, como a exponenciação modular utilizada para cifrar e decifrar mensagens. Além disso, Hefez destaca a importância de entender os conceitos de números primos e suas propriedades, visto que a segurança do RSA se apoia na dificuldade de fatorar grandes números em seus componentes primos.

Complementando essa ideia, Paixão (2020) e Araújo (2017) explicam em seus estudos que a familiaridade com a teoria dos números, particularmente com o teorema fundamental da aritmética e a fatoração de números inteiros, é crucial para apreciar a robustez do RSA. Eles argumentam que a habilidade de manipular e trabalhar com grandes números primos não só facilita a implementação do algoritmo, mas também permite uma compreensão mais profunda da sua resistência a ataques criptográficos.

Esses conceitos matemáticos são mais do que meros elementos teóricos; eles são ferramentas práticas que nos permitem aplicar e verificar a eficácia da criptografia RSA em diversos contextos. Diante disso, vamos embasar as demonstrações matemáticas e explicações nos autores Abramo Hefez (2013), Jéssica Shayanne da Paixão (2020) e Paulo Francisco de Araújo (2017).

3.2.1. Propriedade dos Números Inteiros

De forma axiomática podemos delinear uma pequena lista das propriedades básicas e das duas operações com números inteiros, baseado em Paixão (2020):

- A adição e multiplicação são **bem definidas**:

Para todos $a, b, a', b' \in \mathbb{Z}$ se $a = a' e\ b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

- A adição e a multiplicação são **comutativas**:

Para todos $a, b \in \mathbb{Z}, a + b = b + a$ e $a \cdot b = b \cdot a$.

- A adição e a multiplicação são **associativas**:

Para todos $a, b, c \in \mathbb{Z}, (a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

- A adição e a multiplicação possuem **elementos neutros**:

Para todo $a \in \mathbb{Z}, a + 0 = a$ e $a \cdot 1 = a$

- A adição possui **elementos simétricos**:

Para todo $a \in \mathbb{Z}$, existe $b = (-a)$ tal que $a + b = 0$.

- A multiplicação é **distributiva** com relação à adição:

Para todos $a, b, c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

Nos inteiros também valem as seguintes propriedades:

- **Fechamento de $\mathbb{N}$:** O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$.
- **Tricotomia:** Dados $a, b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:
  i) $a = b$;
  ii) $b - a \in \mathbb{N}$;
  iii) $-(b - a) = a - b \in \mathbb{N}$.
- **Princípio da Boa Ordem:** Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

3.2.2. Divisão de Inteiros

Definição 1: Dados dois números a e b, diremos que a *divide* b, escrevendo $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Neste caso, diremos também que a é um *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a ou, se $b \neq 0$, que b é *divisível* por a. Quando não existe nenhum número inteiro c tal que $b = c \cdot a$, denotaremos $a \nmid b$.

A divisão euclidiana assegura que sempre é possível realizar uma divisão entre dois números inteiros, mesmo quando eles não são divisíveis de maneira exata. Em tais casos, podemos executar uma "divisão com um pequeno resto". Esse princípio fundamental, que remonta aos ensinamentos de Euclides, estabelece a base para diversas propriedades cruciais dos números inteiros que serão examinadas a seguir.

Teorema 1 (Divisão Euclidiana). Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

Demonstração: Considere o conjunto $S = \{x = a - b \cdot y : y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.

Existência: Existe $n \in \mathbb{Z}$ tal que $n \cdot (-b) > -a$, logo $a - n \cdot b > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - b \cdot q$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S,

$$\text{pois } s = a - (q \pm 1) \cdot b \in S, \text{ com } s < r.$$

Unicidade: Suponha que $a = b \cdot q + r = b' \cdot q' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que $|b| \cdot |q - q'| = |r - r'| < |b|$, o que só é possível se $q = q'$ e consequentemente, $r = r'$.

■

3.2.3. Máximo Divisor Comum

Definição 2: Sejam dados dois números a e b, distintos ou não. Um número inteiro d será dito um *divisor comum* de a e b se $d|a$ e $d|b$.

Definição 3: Diremos que um número inteiro $d \geq 0$ é um *máximo divisor comum (m.d.c.)* de a e b, se possuir as seguintes propriedades:

i) d é um divisor comum de a e b, e

ii) d é divisível por todo divisor comum de a e b.

A condição (ii) pode ser renunciada do seguinte modo:

ii') Se c é um divisor comum de a e b, então $c|d$.

Denotando o m.d.c. de a e b, quando existe, como (a, b), apresentaremos a seguir o Lema 1, que será utilizado para provar a existência do máximo divisor comum de dois inteiros não negativos.

Lema 1. Sejam $a, b, n \in \mathbb{Z}$. Se existe $(a, b - n \cdot a)$, então, (a, b) existe e $(a, b) = (a, b - n \cdot a)$.

Demonstração: Seja $d = (a, b - n \cdot a)$. Como $d|a$ e $d|(b - n \cdot a)$, segue que $d|b = b - n \cdot a + n \cdot a$.

Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b.

Logo, c é um divisor comum de a e $b - n \cdot a$ e, portanto, $c|d$. Isso prova que $d = (a, b)$.

■

A seguir será apresentada a prova constitutiva da existência do m.d.c. dada por Euclides. Tal algoritmo é um primor do ponto de vista computacional e pouco se conseguiu aperfeiçoá-lo em mais de dois milênios.

3.2.4. Propriedades do Máximo Divisor Comum

Sejam $a, b \in \mathbb{Z}$. Definimos o conjunto

$$I(a, b) = \{xa + yb : x, y \in \mathbb{Z}\}.$$

Note que se a e b não são simultaneamente nulos, então $I(a, b) \cap \mathbb{N} \neq \emptyset$. De fato, temos que $a^2 + b^2 = a \cdot a + b \cdot b \in I(a, b) \cap \mathbb{N}$.

A seguir utilizaremos a notação

$$d\mathbb{Z} = \{Id; I \in \mathbb{Z}\}.$$

O Teorema 2 nos dará outra demonstração da existência do m.d.c. de dois números a e b e da existência dos inteiros m e n tais que $(a, b) = ma + nb$. Porém, ao contrário da prova de Euclides, não nos fornecerá um meio prático para achar o m.d.c. dos dois números, nem os inteiros m e n.

Teorema 2. Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Se $d = min\, I(a, b) \cap \mathbb{N}$, então

i) d é o m.d.c. de a e b; e

ii) $I(a, b) = d\mathbb{Z}$.

Demonstração: (i) Suponha que c divida a e b, logo c divide todos os números naturais da forma $xa + yb$. Portanto, c divide todos os elementos de $I(a, b)$, e, consequentemente, $c|d$.

Agora vamos mostrar que d divide todos os elementos de $I(a,b)$. Seja $z \in I(a,b)$ e suponha, por absurdo, que $d \nmid z$. Logo, pela divisão euclidiana,

$$z = dq + r, \text{ com } 0 < r < d. \text{ (1)}$$

Como $z = xa + yb$ e $d = ma + nb$, para alguns $x, y, m, n \in Z$, segue-se de (1) que

$$r = (x - qm)a + (y - qn)b \in I(a,b) \cap \mathbb{N},$$

o que é um absurdo, pois $d = min\, I(a,b) \cap \mathbb{N}$ e $r < d$. Em particular, $d|a$ e $d|b$.

Assim, provamos que d é o m.d.c. de a e b.

(ii) Dado que todo elemento de $I(a,b)$ é divisível por d, temos que $I(a,b) \subset d\mathbb{Z}$. Por outro lado, para todo $Id \in d\mathbb{Z}$, temos que

$$Id = I(ma + nb) = (Im)a + (In)b \in I(a,b)$$

e, portanto, $d\mathbb{Z} \subset I(a,b)$. Em conclusão, temos que $I(a,b) = d\mathbb{Z}$.

■

A Proposição 1 estabelece uma conexão fundamental entre as estruturas aditivas e multiplicativas dos números naturais. Essa relação é essencial para a demonstração de diversos resultados matemáticos, incluindo o notável teorema conhecido como Lema de Gauss.

Proposição 1. Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.

Demonstração: Suponha que a e b são primos entre si. Logo, $(a,b) = 1$. Pelo Teorema 2, temos que existem números inteiros m e n tais que $ma + nb = (a,b) = 1$, segue a primeira parte da proposição.

Reciprocamente, suponha que existam números inteiros m e n tais que $ma + nb = 1$. Se $d = (a,b)$, temos que $d|(ma + nb)$, o que mostra que $d|1$, e, portanto, $d = 1$.

■

Teorema 3 (Lema de Gauss). Sejam a, b e c números inteiros. Se $a|b \cdot c$ e $(a,b) = 1$, então $a|c$.

Demonstração: Se $a|b \cdot c$, então existe $e \in \mathbb{Z}$ tal que $b \cdot c = a \cdot e$.

Se $(a,b) = 1$, então, pela proposição anterior, temos que existem $m, n \in Z$ tais que

$$ma + nb = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = m \cdot a \cdot c + n \cdot b \cdot c.$$

Substituindo $b \cdot c$ por $a \cdot e$ nesta última igualdade, temos que

$$c = m \cdot a \cdot c + n \cdot a \cdot e = a(mc + ne)$$

e, portanto, $a|c$.

■

3.2.5. Algoritmo de Euclides

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b|a$, já vimos que $(a, b) = b$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever:

$$a = b \cdot q_1 + r_1, \text{ com } 0 < r_1 < b$$

Temos duas possibilidades:

a) $r_1|b$. Em tal caso, $r_1 = (b, r_1)$ e pelo Lema 1 temos que

$$r_1 = (b, r_1) = (b, a - q_1 b) = (b, a) = (a, b),$$

E o algoritmo termina.

b) $r_1 \nmid b$. Em tal caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1$$

Novamente, temos duas possibilidades:

A') $r_2|r_1$. Nesse caso, $r_2 = (r_1, r_2)$ e novamente pelo Lema 1:

$$r_2 = (r_1, r_2) = (r_1, b - q_2 r_1) = (r_1, b) = (a - q_1 b, b) = (a, b),$$

E paramos, pois termina o algoritmo.

B') $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtendo:

$$r1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Continuamos esse procedimento até que pare. Isso sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $B > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n|r_{n-1}$, o que implica que $(a, b) = r_n$.

O algoritmo acima pode ser sintetizado e realizado na prática como mostramos a seguir.

Inicialmente, efetuamos a divisão $a = bq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
a	b	
r_1		

A seguir, continuamos efetuando a divisão $b = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n	0	

Por exemplo, calcular o m.d.c. de 372 e 162:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6	0	

Portanto, (372,162) = 6.

Note que conseguimos, através do uso do Algoritmo de Euclides de trás para a frente, escrever 6 = (372,162) como uma soma de um múltiplo de 162 e um múltiplo de 372. De fato, observando o exemplo acima, o Algoritmo de Euclides nos fornece:

$$6 = 18 - 1 \cdot 12$$

$$12 = 48 - 2 \cdot 18$$

$$18 = 162 - 3 \cdot 48$$

$$48 = 372 - 2 \cdot 162.$$

Donde segue que

$$6 = 18 - 1 \cdot 12 =$$

$$= 18 - 1 \cdot (48 - 2 \cdot 18) =$$

$$= 3 \cdot 18 - 48 =$$
$$= 3 \cdot (162 - 3 \cdot 48) - 48 =$$
$$= 3 \cdot 162 - 10 \cdot 48 =$$
$$= 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) =$$
$$= 23 \cdot 162 - 10 \cdot 372.$$

Com isso, temos que

$$(372{,}162) = 6 = 23 \cdot 162 + (-10) \cdot 372.$$

3.2.6. Números Primos

Como já citamos na introdução deste capítulo, o princípio das chaves assimétricas baseia- se na relativa facilidade em encontrar números primos grandes e, ao mesmo tempo, na enorme dificuldade prática em fatorar o produto de dois desses números.

Assim, estudaremos nesta seção os números primos e algumas de suas propriedades a fim de melhorar nossa compreensão da criptografia RSA.

3.2.6.1. Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética nos garante que os números primos são suficientes para gerar todos os números naturais, logo, todos os inteiros não nulos. Para entender este teorema, precisamos definir as propriedades que fazem um número ser primo.

Definição 4. Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de **número primo**.

Dados dois números primos *p* e *q* e um número inteiro *a* qualquer, decorrem da definição acima os seguintes fatos:

i) Se $p|q$, então $p = q$.

De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii) Se $p \nmid a$, então $(p, a) = 1$.

De fato, se $(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Definição 5. Um número maior do que 1 e que não é primo será dito **composto**.

A seguir, estabelecemos um resultado fundamental de Euclides, chamado Lema de Euclides.

Proposição 1 (Lema de Euclides). Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|a \cdot b$, então $p|a$ ou $p|b$.

Demonstração: Se $p|a \cdot b$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, temos que $(p, a) = 1$, e o resultado segue-se do Teorema 3, também conhecido como Lema de Gauss.

■

Para provar o Teorema Fundamental da Aritmética precisaremos do Corolário 1 a seguir:

Corolário 1. Se $p, p_1, \dots, p_n$ são números primos e, se $p|p_1 \cdot \dots \cdot p_n$, então $p = p_i$ para algum $i = 1, \dots, n$.

Demonstração: Demonstra-se o resultado por indução sobre n .Se $n = 2$, o resultado vale pela Proposição 1. Como hipótese de indução suponha que o resultado vale para $n - 1$. Agora se, $p|p_1 \dots p_n$ tem-se que $p|p_1 \dots p_{n-1}$ ou $p|p_n$. Se $p|p_n$ o resultado segue. Se $p \nmid p_n$ então $p|p_1 \dots p_{n-1}$ e, pela hipótese de indução $p = p_i$ para algum $i = 1, \dots, n - 1$.

■

Teorema 4 (Teorema Fundamental da Aritmética). Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração: Usaremos a segunda forma do Princípio da Indução sobre o número natural n. Se $n = 2$, o resultado é verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1 \ldots, q_s$ tais que $n_1 = p_1 \ldots p_r$ e $n_2 = q_1 \ldots q_s$. Portanto, $n = p_1 \ldots p_r \cdot q_1 \ldots q_s$.

Vamos provar a unicidade da escrita. Suponha que tenhamos $n = p_1 \ldots p_r = q_1 \ldots q_s$, , onde os p_i e os q_j são números primos. Como $p_1 | q_1 \ldots q_s$, pelo Corolário 1, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto, $p_2 \ldots p_r = q_2 \ldots q_s$.

Como $p_2 \ldots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

■

3.2.6.2. Distribuição dos Números Primos

Para demonstrar a existência de infinitos números primos, apresentaremos a prova elaborada por Euclides, através de uma demonstração por absurdo.

Teorema 5. Existem infinitos números primos.

Demonstração: Suponha que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Considere o número natural

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1.$$

Pelo Teorema 4 (Fundamental da Aritmética), o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Mas isto implica que p divide 1, o que é absurdo.

■

Um dos métodos mais antigos para a construção de uma tabela de primos é o **Crivo de Eratóstenes**, que permite determinar todos os números primos até a

ordem que se desejar. Embora a técnica funcione, não é muito eficiente para determinar números primos de ordem muito elevada.

Faremos a seguir a construção do Crivo de Eratóstenes até o número 120. Para isso, será interessante usarmos o lema a seguir.

Lema 2. Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 < n$, então ele é primo.

Demonstração: Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n, então, $n = q \cdot n_1$, com $q \leq n_1$. Segue daí que $q^2 \leq q \cdot n_1 = n$.

Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo.

■

Para a construção da tabela escrevemos todos os números naturais de 2 a 120 (Tabela 7). Riscam-se, de modo sistemático, todos os números compostos da tabela, seguindo o roteiro abaixo.

Risque todos os múltiplos de 2 acima de 2, já que nenhum deles é primo.

O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3, pois esses não são primos.

O terceiro número não riscado que aparece é 5, que é primo. Risque todos os múltiplos de 5 maiores do que 5, pois esses não são primos.

O quarto número não riscado que aparece é 7, que é primo. Risque todos os múltiplos de 7 maiores do que 7, pois esses não são primos.

Não necessitamos ir além do número primo 7, pois, segundo o Lema 2 temos que o próximo número primo seria o 11, cujo quadrado supera 120.

Crivo de Eratóstenes

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~

~~-91-~~	~~-92-~~	~~-93-~~	~~-94-~~	~~-95-~~	~~-96-~~	97	~~-98-~~	~~-99-~~	~~-100-~~
101	~~-102-~~	103	~~-104-~~	~~-105-~~	~~-106-~~	107	~~-108-~~	109	~~-110-~~
~~-111-~~	~~-112-~~	113	~~-114-~~	~~-115-~~	~~-116-~~	~~-117-~~	~~-118-~~	~~-119-~~	~~-120-~~

Tabela 7 - Hefez (2014, p. 151).

3.2.6.3. Pequeno Teorema de Fermat

Os chineses, desde 500 anos antes da Era Comum, já sabiam que, se p é um número primo, então $p|2^p - 2$. Coube a Pierre Fermat, no século XVII, generalizar esse resultado, enunciando um pequeno, mas notável teorema.

Lema 3. Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração: O resultado vale trivialmente para $i = 1$. Podemos, então, supor $1 < i < p$.

Nesse caso, $i!\,|p(p-1)\ldots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i!\,|(p-1)\ldots(p-i+1)$, e o resultado segue, pois $\binom{p}{i} = p\frac{(p-1)\ldots(p-i+1)}{i!}$.

■

Teorema 6 (Pequeno Teorema de Fermat). Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.

Demonstração: Se $p = 2$, o resultado é óbvio já que $a^2 - a = a(a-1)$ é par. Suponhamos que p seja ímpar.

Nesse caso, claramente basta mostrar o resultado para $a > 0$. Vamos provar o resultado por indução sobre a.

O resultado vale claramente para $a = 0$, pois $p|0$.

Supondo válido para a, iremos prová-lo para $a + 1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a.$$

Como, pelo Lema 3 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o resultado se segue.

■

O Corolário 2 também será chamado de **Pequeno Teorema de Fermat**.

Corolário 2. Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.

Demonstração: Como, pelo Pequeno Teorema de Fermat (Teorema 6), $p|a(a^{p-1} - a)$ e como $(a, p) = 1$, segue-se, imediatamente, que p divide $a^{p-1} - 1$.

■

É importante ressaltar que o Pequeno Teorema de Fermat nos fornece um teste de não primalidade. De fato, dado $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m não é primo.

Definição 6: Dizemos que dois números inteiros positivos são primos entre si, ou relativamente primos, se não possuírem divisores comuns além de 1.

Observe que a e b são primos entre si se, e somente se, $(a, b) = 1$.

3.2.7. Congruências

Definição 7: Seja m um número natural. Diremos que dois números inteiros a e b são *congruentes* módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se $a \equiv b \, mod \, m$.

Quando a relação $a \equiv b \, mod \, m$ for falsa, diremos que a e b não são congruentes ou que são incongruentes, módulo m. Escrevemos, nesse caso, $a \not\equiv b \, mod \, m$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os restos. É suficiente aplicar o seguinte resultado:

Proposição 2. Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \, mod \, m$ se, e somente se, $m|b - a$.

Demonstração: Sejam $a = m \cdot q + r$, com $0 \leq r < m$ e $b = m \cdot q' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b \, mod \, m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m|b - a$, já que $|r - r'| < m$.

■

Proposição 3. Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que:

i) $a \equiv a \, mod \, m$,

ii) Se $a \equiv b \, mod \, m$, então $b \equiv a \, mod \, m$,

iii) Se $a \equiv b \, mod \, m$, e $b \equiv c \, mod \, m$, então $a \equiv c \, mod \, m$.

Demonstração:

i) $a \equiv a \, mod \, m$:

$$m|0 \Longrightarrow m|a - a \Longrightarrow \ a \equiv a \, mod \, m.$$

ii) Se $a \equiv b \, mod \, m$, então $b \equiv a \, mod \, m$ o que implica que $m|b - a$.

Logo, existe um $k \in \mathbb{Z}$ tal que $m \cdot k = b - a$. Usando a propriedade dos números inteiros, garantimos a existência do elemento simétrico a k, o $-k$. Assim, $m(-k) = -(b - a) = a - b$ o que implica $m|a - b$ e, portanto $b \equiv a \, mod \, m$.

iii) Se $a \equiv b \, mod \, m$, e $b \equiv c \, mod \, m$, então $a \equiv c \, mod \, m$.

Como $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$, temos $m|b - a$ e $m|c - b$, logo, existem $k, k' \in \mathbb{Z}$ tais que:

1) $m \cdot k = b - a$ e
2) $m \cdot k' = c - b$.

De (1) temos que $b = m \cdot k + a$. Substituindo em (2) temos $m \cdot k' = c - (m \cdot k + a)$. Portanto,

$$m \cdot k' + m \cdot k = c - a \Longrightarrow m(k + k') = c - a$$

Assim, $m|c - a$ e, portanto, $a \equiv c \; mod \; m$.

■

Decorre da proposição anterior que a congruência, módulo inteiro fixado m, é uma relação de equivalência.

Note que todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0,1, \dots, m - 1$. Além disso, dois desses números distintos não são congruentes módulo m.

Portanto, para encontrar o resto da divisão de um número a por m, basta achar o número natural r dentre os números $0, \dots, m - 1$ que seja congruente a a módulo m.

O que torna a noção de congruência útil e poderosa é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 4. Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

i) Se $a \equiv b \; mod \; m$ e $c \equiv d \; mod \; m$, então $a + c \equiv b + d \; mod \; m$.

ii) Se $a \equiv b \; mod \; m$ e $c \equiv d \; mod \; m$, então $a \cdot c \equiv b \cdot c \; mod \; m$

Demonstração:

Suponhamos que $a \equiv b \; mod \; m$ e $c \equiv d \; mod \; m$. Logo, temos que $m|b - a$ e $m|d - c$.

i) Basta observar que $m|(b - a) + (d - c)$ e, portanto, $m|(b + d) - (a + c)$, o que prova essa parte do resultado.

ii) Basta notar que $b \cdot d - a \cdot c = d(b - a) + a(d - c)$ e concluir que $m|b \cdot d - a \cdot c$.

■

Corolário 3. Para todos $n \in \mathbb{N}, a, b \in \mathbb{Z}$, se $a \equiv b \; mod \; m$, então tem-se que $a^n \equiv b^n \; mod \; m$.

Demonstração: Faremos a demonstração por indução sobre n. Se $n = 1$ o resultado é válido por hipótese.

Como hipótese de indução suponhamos que o resultado vale para n, ou seja, $a^n \equiv b^n \; mod \; m$. Queremos provar que vale para $n+1$. Basta observar que

$$b^{n+1} - a^{n+1} = b^n \cdot b - a^n \cdot a$$

Como $a \equiv b \; mod \; m$ e $a^n \equiv b^n \; mod \; m$, pela hipótese, temos pela proposição 4 item (ii), o resultado desejado.

■

3.2.8. Função φ de Euler

Um **sistema reduzido de resíduos** módulo m é um conjunto de números inteiros $r_1, \dots, r_s$ tais que:

a) $(r_i, m) = 1$, para todo $i = 1, \dots, s$;

b) $r_i \not\equiv r_j \; mod \; m$, se $i \neq j$;

c) Para cada $n \in \mathbb{Z}$ tal que $(n, m) = 1$, existe i tal que $n \equiv r_i \; mod \; m$.

Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de elementos naturais entre 0 e $m-1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define uma importante função:

$$\varphi: \mathbb{N} \to \mathbb{N},$$

chamada de **função fi de Euler.**

Pela definição, temos que $\varphi(m) \leq m - 1$, para todo $m \geq 2$.

Além disso, se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um número primo.

Teorema 7. Sejam $m, n \in \mathbb{N}$ com $(m, n) = 1$. Então

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Demonstração: O resultado é facilmente verificado se $m = 1$ ou $n = 1$. Então, vamos supor $m > 1$ e $n > 1$. Assim, consideremos a tabela abaixo formada pelos números naturais de 1 até $n \cdot m$.

1	$m+1$	...	$(n-1)m+1$
2	$m+2$	...	$(n-1)m+2$
3	$m+3$	...	$(n-1)m+3$
...	...	...	...

m	$2m$	...	$n \cdot m$

Observe que a tabela acima forma um sistema completo de resíduos módulo $n \cdot m$. Mas, estamos interessados no sistema reduzido de resíduos módulo $n \cdot m$, ou seja, queremos determinar todos os números de 1 a $n \cdot m$ que são primos com $n \cdot m$. Assim, queremos determinar t, tal que $(t, n \cdot m) = 1$. Mas,

$$(t, n \cdot m) = 1 \Leftrightarrow (t, n) = (t, m) = 1.$$

Dessa forma, para calcular $\varphi(m \cdot n)$ devemos determinar na tabela acima os inteiros que são primos com n e m ao mesmo tempo. Assim, se na r-ésima linha tivermos $(m, r) = d > 1$ então nenhum termo dessa linha será primo com $m \cdot n$ pois, todos os termos são da forma $k \cdot m + r$, onde $0 \leq k \leq n - 1$ e estes são todos divisíveis por d. Logo, os elementos que são primos com m estão necessariamente nas colunas restantes e, num total de $\varphi(m)$ elementos. Agora, vejamos quais são os elementos primos com n em cada uma dessas linhas.

Como $(n, m) = 1$, os elementos da linha $k, m + k, \ldots, (n - 1)m + k$ são todos primos com n e formam um sistema completo de resíduos módulo n. Logo, cada uma dessas linhas possui uma quantidade de $\varphi(n)$ elementos primos com n e, consequentemente primos com $n \cdot m$. Logo, o número de elementos simultaneamente primos com n e m é $\varphi(n) \cdot \varphi(m)$.

Portanto, $\varphi(m \cdot n) = \varphi(n) \cdot \varphi(m)$.

■

Observemos que, pela definição da função φ e pelo teorema anterior temos que, se p e q são ambos primos, então $\varphi(p \cdot q) = (p - 1) \cdot (q - 1)$, que será fortemente utilizado na codificação de mensagens utilizando o método RSA.

3.3 A Criptografia RSA

Aqui, vamos abordar como a Criptografia RSA funciona e o que torna o algoritmo tão interessante. Para tanto, serão utilizados três autores, Severino Coutinho (2005), Abramo Hefez (2013) e Paulo Francisco de Araújo (2017).

No livro Números Inteiros e Criptografia RSA, Severino Coutinho oferece uma abordagem didática e rigorosa da criptografia RSA. Coutinho inicia com uma introdução à teoria dos números, preparando o leitor para entender os fundamentos matemáticos que sustentam o algoritmo RSA. Ele destaca a importância da escolha de grandes números primos e da utilização de operações modulares para garantir a segurança do sistema. Coutinho enfatiza que a robustez do RSA está na dificuldade de fatorar números grandes, tornando a criptografia uma aplicação prática e poderosa da matemática pura.

Em sua dissertação *Aplicações de Criptografia no Ensino Médio*, Paulo Francisco de Araújo foca na implementação e aplicação didática da criptografia RSA. Araújo contextualiza o RSA dentro da educação, mostrando como conceitos matemáticos abstratos podem ser aplicados de maneira prática e relevante. Ele explora a importância do RSA no cotidiano digital e explica os passos básicos da criptografia e decriptação, destacando a importância da chave pública e privada para a segurança dos dados. Araújo usa exemplos práticos para ilustrar como o RSA pode ser integrado ao currículo de ensino médio, tornando a matemática mais interessante e aplicável para os estudantes.

No capítulo "As Origens da Criptografia" do livro *Aritmética*, Abramo Hefez aborda a criptografia RSA dentro do contexto histórico e teórico da criptografia. Hefez detalha a evolução da criptografia desde os métodos antigos até a moderna criptografia de chave pública. Ele descreve o RSA como uma inovação significativa, resultante da combinação de teorias matemáticas complexas com a necessidade prática de segurança nas comunicações. Hefez destaca a elegância do RSA ao utilizar propriedades da teoria dos números, como a dificuldade de fatoração, para criar um sistema criptográfico robusto e eficaz. Ele também enfatiza a importância do RSA no cenário global de segurança da informação, especialmente com o advento da internet e das comunicações digitais.

A criptografia RSA é amplamente reconhecida por sua contribuição significativa à segurança digital. Através das abordagens de Coutinho, Araújo e Hefez,

podemos apreciar as diferentes perspectivas sobre a importância, implementação e aplicação do RSA. Cada autor contribui de maneira única para a compreensão deste método criptográfico, seja através de uma análise teórica rigorosa, de aplicações educacionais práticas ou de um contexto histórico detalhado. Essas abordagens complementares enriquecem o entendimento do RSA e sua relevância no mundo contemporâneo.

3.3.1. O Advento dos Computadores

A chegada dos telégrafos e finalmente dos computadores revolucionou a Teoria da Informação. Com a disseminação dos computadores, foi necessário buscar uma uniformização nos procedimentos. Como os computadores utilizam códigos binários, foi preciso transformar todas as informações nesse código. Assim, nasce o American Standard Code for Information Interchange, abreviado por ASCII, cujo significado é Código Padrão Americano para o Intercâmbio de Informação.

Essa codificação, desenvolvida a partir de 1960, não é um método de decifragem. Ela é apenas uma tradução à linguagem binária dos símbolos mais corriqueiros. Atribui significados específicos aos $2^7 = 128$ números binários (formados por 0 e 1) de sete dígitos. Os 32 primeiros e o último são caracteres de controle, não imprimíveis, e os outros, que são imprimíveis, constituem dados na Tabela 8.

Um grande desafio para a computação é a questão da privacidade na troca de informações e na uniformização dos padrões. Estabelecido o código ASCII, um próximo passo foi a busca, de uniformização no uso dos sistemas criptográficos.

Após intensa busca, em 1973, o National Bureau of Standards, órgão governamental americano, escolheu o sistema criptográfico Data Encryption Standard (DES), desenvolvido pela IBM, para ser o sistema oficial americano.

Este sistema, utilizado até 1999, era bastante complexo e funcionava com uma distribuição de chaves simétricas. Ou seja, um número (a chave) é acertado entre duas partes para definir os parâmetros da função cifragem que é a mesma para a decifragem. Como o segredo das mensagens é garantido através da manutenção do segredo das chaves, isso criou um enorme problema logístico de distribuição de chaves, uma verdadeira “operação de guerra”. Hoje em dia são utilizados outros

sistemas como o Advanced Encryption Standard (AES) ou o Skipjack, esse último desenvolvido pela U.S. National Security Agency.

Urgia então resolver de modo mais racional o problema da troca de chaves entre correspondentes. Por muito tempo pairou sobre a comunidade dos criptologistas o paradigma da impossibilidade da troca de senhas sem a intermediação de um portador. Coube a três norte-americanos, Whitfield Diffie, Martin Hellman e Ralph Merkle, quebrar esse paradigma. É aí que começa a entrar no campo da criptografia, timidamente, mas de modo irreversível, a Teoria dos Números através da noção de congruências.

Ronald Rivest, Adi Shamir e Leonard Adleman, do Laboratório de Ciência da Informação do Massachusetts Institute of Technology (MIT) deram em 1978 o passo decisivo para a implementação do primeiro sistema criptográfico com chaves assimétricas, idealizado por Diffie. O princípio baseia-se na relativa facilidade em encontrar números primos grandes, ao passo que havia uma enorme dificuldade prática em fatorar o produto de dois desses números, além do uso de propriedades relativamente elementares da Teoria dos Números, como a Função φ de Euler.

Vamos aos detalhes matemáticos dessa descoberta. Recordando, estamos à procura de um sistema criptográfico com duas chaves, uma pública e outra privada, para que qualquer pessoa possa cifrar uma mensagem previamente codificada em ASCII e somente o seu legítimo destinatário possa decifrá-la.

3.3.2. Codificação de mensagens com RSA

Suponhamos, por simplicidade, que a mensagem original é um texto onde não há números, apenas palavras. Para explicarmos o funcionamento do método RSA, ao invés de trabalharmos com mensagens codificadas em ASCII, utilizaremos a tabela de conversão abaixo.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 8 - Tabela de Conversão para o método RSA

Nesse método, não faremos distinção de letras maiúscula e minúscula e desconsideraremos também acentos de palavras. Além disso, os espaços entre as palavras serão substituídos pelo número 99.

Existe a importância de representar cada letra do alfabeto com dois dígitos ao converter uma mensagem em uma sequência numérica para evitar ambiguidades. Por exemplo, se a letra A fosse representada pelo número 1 e a letra B pelo número 2, e a letra L fosse o número 12, o que seria o mesmo que a sequência numérica para AB. Isso causaria confusão ao decifrar a mensagem, pois não seria claro se 12 representa AB ou apenas L.

A seguir, apresentaremos um passo a passo de como criptografar mensagens utilizando o método RSA, seguido de um exemplo de aplicação deste método.

1) Convertemos a mensagem a ser criptografada em uma sequência numérica conforme a tabela de conversão acima.
2) Escolhemos dois números primos distintos quaisquer, suficientemente grandes, que chamaremos de p e q.
3) Determinamos n o primeiro parâmetro a ser utilizado na cifragem, de forma que $n = p \cdot q$.
4) Calculamos o valor de $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$.
5) Determinamos e o segundo parâmetro que será utilizado na codificação de tal forma que e seja relativamente primo com $\varphi(n)$, ou seja, $\big(e, \varphi(n)\big) = 1$ e $1 < e < \varphi(n)$.
6) Quebramos a mensagens em blocos de tamanho $M < n$.
7) Codificamos cada bloco da mensagem utilizando a seguinte relação:

   $$C(b) \equiv b^e \ mod \ n.$$

   Onde b é o bloco da mensagem original e $C(b)$ é o bloco cifrado.

   Observação: O par (n, e) é a chave pública ou chave de cifragem.

Exemplo: Vamos criptografar a mensagem IFPR CAPANEMA.

Seguindo os passos acima, teremos:

1) A sequência numérica ficará da seguinte forma:

   $$18\ 15\ 25\ 27\ 99\ 12\ 10\ 25\ 10\ 23\ 14\ 22\ 10$$

2) Sejam $p = 7$ e $q = 11$
3) $n = p \cdot q = 77$
4) $\varphi(n) = \varphi(77) = (7-1)(11-1) = 60$

5) Vamos considerar $e = 7$ e, observe que $(7,60) = 1$
6) Como $n = 77$, devemos quebrar a mensagem em blocos de tamanho aleatório, desde que o valor numérico de cada bloco seja menor do que $n = 77$. Assim, quebrando a mensagem em blocos, obtemos:

$$1 - 8 - 1 - 52 - 52 - 7 - 9 - 9 - 1 - 2 - 1 - 10 - 2 - 5 - 10 - 2 - 31 - 4 - 2 - 2 - 10$$

Para escolher os blocos na criptografia, é importante evitar que um bloco comece com 0, pois isso pode causar problemas na decodificação. Além disso, os blocos devem ser formados de maneira que não correspondam a nenhuma unidade linguística como palavras ou letras específicas. Isso dificulta a decodificação por análise de frequência, tornando-a praticamente impossível, a menos que corresponder a um 0 solto ou que comece com 0.

7) Para o primeiro bloco, ou seja, para $b = 1$, temos:

$$C(1) \equiv 1^7 \ mod\ 77$$

Logo $C(1) = 1$

Para o próximo bloco, $b = 8$, temos:

$$C(8) \equiv 8^7 \ mod\ 77$$

Logo $C(8) = 57$

Para o próximo bloco, para $b = 1$, temos

$$C(1) \equiv 1^7 \ mod\ 77$$

Logo $C(1) = 1$

Para o próximo bloco, para $b = 52$, temos

$$C(52) \equiv 52^7 \ mod\ 77$$

Logo $C(52) = 24$

E assim por diante, continuando esse mesmo raciocínio chegaremos aos seguintes blocos criptografados:

$$1 - 57 - 1 - 24 - 24 - 28 - 37 - 37 - 1 - 51 - 1 - 10 - 51 - 47 - 10 - 51 - 59 - 60 - 51 - 51 - 10$$

3.3.3. Decifrando a Mensagem

Para decodificar a mensagem recebida, seguiremos um passo a passo, similar ao processo de codificação. Em seguida, decodificaremos a mensagem do exemplo acima.

1) Determinar d, tal que $d \cdot e \equiv 1\ mod\ \varphi(n)$

Observe que o valor de d pode ser calculado utilizando o Algoritmo de Euclides descrito na seção 3.2.4, como veremos abaixo.

2) Decodificamos cada bloco da mensagem utilizando a relação:

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

onde a é um bloco da mensagem codificada.

Observação: O par (n, d) é a chave privada ou chave de decodificação.

Enunciaremos logo abaixo um teorema que garante que o RSA funciona.

Teorema 8. Sejam $C(b)$ um bloco qualquer da mensagem criptografada e $D(a)$ um bloco da mensagem decodificada. Então, $D\big(C(b)\big) = b$.

Demonstração: Das relações $C(b) \equiv b^e\ mod\ n$ e $D(a) \equiv a^d mod\ n$, temos:

$$D\big(C(b)\big) \equiv D(b^e) \equiv (b^e)^d \equiv b^{e\cdot d}\ mod\ n.$$

Como d é o inverso de e módulo $\varphi(n)$, temos que $e \cdot d \equiv 1\ mod\ \varphi(n)$ e, daí que, existe um inteiro k tal que $e \cdot d = k\varphi(n) + 1$. Mas, $\varphi(n) = (p-1)(q-1)$. Assim, temos: $e \cdot d = k(p-1)(q-1) + 1$ e, substituindo na fórmula anterior, temos:

$$D\big(C(b)\big) \equiv b^{k(p-1)(q-1)+1}\ mod\ n.$$

E como $n = p \cdot q$, temos:

$$D\big(C(b)\big) \equiv b^{k(p-1)(q-1)+1}\ mod\ (p \cdot q).$$

Observe que, pelo fato de p e q serem primos, basta mostrar:

1) $b^{k(p-1)(q-1)+1} \equiv b\ mod\ p$
2) $b^{k(p-1)(q-1)+1} \equiv b\ mod\ q$.

De fato, se (1) e (2) são verdadeiras, pela proposição 2 de Congruência, temos $p|b - b^{k(p-1)(q-1)+1}$ e $q|b - b^{k(p-1)(q-1)+1}$, o que implica que

$p \cdot q|b - b^{k(p-1)(q-1)+1}$, e assim $b^{k(p-1)(q-1)+1} \equiv b\ mod\ (p \cdot q)$.

Vamos provar (1):

(1) Se $p|b$ então $0 \equiv b \equiv b^{k(p-1)(q-1)+1}\ mod\ (p \cdot q)$

Se $p \nmid b$ então pelo Pequeno Teorema de Fermat, temos:

$$b^{p-1} \equiv 1\ mod\ p.$$

Daí, $(b^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1\ mod\ p.$

Multiplicando esta equivalência por b, obtemos

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

Analogamente provamos (2).

Portanto, $D\big(C(b)\big) = b$ para todo bloco $C(b)$ da mensagem criptografada.

■

Agora vamos descriptografar a mensagem:

$$1-57-1-24-24-28-37-37-1-51-1-10-51-47-10-51-59$$
$$-60-51-51-10$$

Seguindo o procedimento descrito acima, temos:

1) Sabendo que $n = 77$, $e = 7$ e $\varphi(n) = 60$. Daí, como $d \cdot e \equiv 1\ mod\ \varphi(n)$, vamos encontrá-lo usando o Algoritmo de Euclides:

	8	1	1	3
$\varphi(77) = 60$	$e = 7$	4	3	1
4	3	1	0	

Então, temos:

$$60 = 8 \cdot 7 + 4$$
$$7 = 1 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

Isolando os restos, temos:

$$4 = 60 - 8 \cdot 7$$
$$3 = 7 - 1 \cdot 4$$
$$1 = 4 - 1 \cdot 3$$

Vamos utilizar os três restos encontrados como uma combinação linear de 60 e 7:

$$4 = 60 - 8 \cdot 7$$
$$3 = 7 - 1 \cdot 4$$
$$= 7 - 1 \cdot (60 - 8 \cdot 7)$$
$$= (-1) \cdot 60 + 9 \cdot 7.$$

Então,

$$1 = 4 - 1 \cdot 3$$
$$= (60 - 8 \cdot 7) - 1 \cdot [(-1) \cdot 60 + 9 \cdot 7]$$
$$= 2 \cdot 60 + (-17) \cdot 7.$$

Então chegamos a nosso resultado esperado:

$$1 = 2 \cdot 60 + (-17) \cdot 7$$

Como $-17 \equiv 43\ mod\ 60$, então $43 \cdot 7 \equiv 1\ mod\ 60$, e portanto, $d = 43$.

2) Decodificando o primeiro bloco, $D(1) = 1^{43}$, da mensagem, temos:

$$D(1) \equiv 1^{43}\ mod\ 77$$
$$\equiv 1\ mod\ 77$$

Logo, $D(1) = 1$.

Decodificando o segundo bloco, $D(57) = 57^{43}$, da mensagem, temos:

$$D(57) \equiv 57^{43}\ mod\ 77$$
$$\equiv \{[(57)^2]^{21} \cdot 57\}\ mod\ 77$$
$$\equiv \{[15]^{21} \cdot 57\}\ mod\ 77$$
$$\equiv \{[(15)^2]^{10} \cdot 57 \cdot 15\}\ mod\ 77$$
$$\equiv \{[71]^{10} \cdot 57 \cdot 15\}\ mod\ 77$$
$$\equiv \{[(71)^2]^5 \cdot 57 \cdot 15\}\ mod\ 77$$
$$\equiv \{[36]^5 \cdot 57 \cdot 15\}\ mod\ 77$$
$$\equiv \{[(36)^2]^2 \cdot 57 \cdot 15 \cdot 36\}\ mod\ 77$$
$$\equiv \{[64]^2] \cdot 57 \cdot 15 \cdot 36\}\ mod\ 77$$
$$\equiv \{15 \cdot 57 \cdot 15 \cdot 36\}\ mod\ 77$$
$$\equiv 8\ mod\ 77$$

Logo, $D(57) = 8$.

Decodificando o quarto bloco, $D(24) = 24^{43}$, da mensagem, temos:

$$\begin{aligned} D(24) &\equiv 24^{43}\ mod\ 77 \\ &\equiv \{[(24)^2\ ]^{21} \cdot 24\}\, mod\ 77 \\ &\equiv \{[37]^{21} \cdot 24\}\ \ mod\ 77 \\ &\equiv \{[(37)^2\ ]^{10} \cdot 24 \cdot 37\}\ \ mod\ 77 \\ &\equiv \{[60]^{10} \cdot 24 \cdot 37\}\ \ mod\ 77 \\ &\equiv \{[(60)^2]^5 \cdot 24 \cdot 37\}\ \ mod\ 77 \\ &\equiv \{[58]^5 \cdot 24 \cdot 37\}\ \ mod\ 77 \\ &\equiv \{[(58)^2]^2 \cdot 24 \cdot 37 \cdot 58\}\ \ mod\ 77 \\ &\equiv \{[53]^2] \cdot 24 \cdot 37 \cdot 58\}\ \ mod\ 77 \\ &\equiv \{37 \cdot 24 \cdot 37 \cdot 58\}\, mod\ 77 \\ &\equiv 52\ mod\ 77 \end{aligned}$$

Logo, $D(24) = 52$.

Seguindo com procedimento análogo para os demais blocos da mensagem criptografada, determinaremos os blocos da mensagem original e, utilizando a tabela de conversão, conseguiremos ler a mensagem que nos foi enviada.

3.3.4. Por que o método RSA é seguro?

O algoritmo RSA é amplamente reconhecido por sua segurança robusta, fundamentada em princípios matemáticos sólidos e na dificuldade prática de resolver certos problemas numéricos. O RSA é um método de mão única, o que significa que qualquer usuário pode codificar uma mensagem usando a chave pública (n, e). No entanto, a segurança do RSA depende da dificuldade de calcular a chave privada d a partir de apenas n e e. Na prática, só é possível calcular d aplicando o algoritmo euclidiano estendido a $\phi(n)$ e e. Contudo, calcular $\phi(n)$ exige a fatoração de n para descobrir os primos p e q, tarefa que, para números suficientemente grandes, é computacionalmente inviável com as tecnologias atuais.

Uma característica essencial do processo de criptografia no RSA é a injetividade da transformação que ele aplica às mensagens dentro de seu domínio

específico. Isso significa que não existem dois valores distintos x_1 e x_2 que resultem no mesmo valor cifrado y. Em termos matemáticos, a transformação realizada pelo RSA age como uma permutação sobre o conjunto dos inteiros modulares, garantindo que cada entrada produza uma saída única e distinta. A injetividade é crucial para assegurar que cada criptograma produzido seja único, eliminando a possibilidade de colisões que poderiam comprometer a integridade e a segurança do sistema.

Essa injetividade fortalece a segurança do RSA ao garantir que o processo de codificação seja reversível apenas pelo detentor da chave privada, preservando a confidencialidade das comunicações. Combinada à dificuldade da fatoração de grandes números, essa propriedade forma o alicerce sobre o qual a segurança do RSA é construída.

Em resumo, a segurança do RSA deriva da dificuldade matemática inerente ao problema da fatoração de números grandes e da robustez dos procedimentos matemáticos que sustentam o algoritmo. Mesmo com os avanços tecnológicos, quebrar um sistema RSA devidamente implementado requer um esforço computacional que, com os métodos atuais, levaria milhares de anos. Portanto, o RSA continua a ser uma escolha segura e confiável para a criptografia de dados sensíveis.

4. CONSIDERAÇÕES FINAIS

Neste trabalho, investigamos a história e os fundamentos matemáticos que sustentam a criptografia, com ênfase na criptografia RSA. Através da apresentação de elementos históricos, traçamos a evolução da criptografia desde suas origens antigas até os métodos utilizados atualmente.

O método de criptografia RSA, destaca-se por sua robustez e segurança, fundamentada na dificuldade de fatoração de números inteiros grandes. Esse problema matemático continua a desafiar pesquisadores, garantindo a confiabilidade do RSA mesmo após décadas de avanços tecnológicos.

Atualmente, não existem algoritmos eficientes que possam quebrar a segurança oferecida pelo RSA, tornando-o uma escolha confiável para a proteção de dados sensíveis.

Além de seu valor prático, a criptografia RSA serve como um exemplo significativo da aplicação da matemática em problemas reais, demonstrando a relevância da teoria dos números e da álgebra na segurança da informação. Este trabalho espera não apenas contribuir para a compreensão da criptografia, mas também inspirar futuras investigações e aplicações no campo.

Por fim, é importante ressaltar que, mesmo com avanços contínuos em tecnologia, a base matemática sólida sobre a qual o RSA foi construído garante sua permanência como um método seguro e eficaz de criptografia. A aplicação de conceitos matemáticos avançados na resolução de problemas práticos reflete a importância da matemática na nossa sociedade moderna, destacando seu papel fundamental na proteção de informações e na manutenção da segurança digital.

Referências e literatura revisadas ao longo deste trabalho forneceram uma base sólida para futuras pesquisas e aplicações.

Esperamos que este trabalho sirva como um recurso valioso tanto para estudantes quanto para profissionais da área, promovendo uma maior compreensão e apreciação da criptografia e da matemática que a fundamenta.

5. REFERÊNCIAS

ABDULLAH, Ako Muhammad **Advanced Encryption Standard (AES)** Algorithm to Encrypt and Decrypt Data, Cryptography and Network Security. 2017.

ARAUJO, Paulo Francisco. **Aplicações de criptografia no ensino médio**. Portugal, Universidade de Évora, 2002.

BRAUMANN, Carlos A., **Divagações sobre investigação matemática e o seu papel na aprendizagem da matemática**, João Pessoa - PB, Out 2010.

BEZERRA, Debora de Jesus, MALAGUTTI, Pedro Luiz, RODRIGUES, Vânia Cristina da Silva, **Aprendendo Criptologia de Forma Divertida, V Bienal SBEM**, João Pessoa - PB, Out 2010.

BRITISH MUSEUM. **Everything you ever wanted to know about the Rosetta Stone.** 2017, Disponível em: https://www.britishmuseum.org/blog/everything-you-ever-wanted-know-about-rosetta-stone.Acessado em: 19 de novembro de 2023.

COUTINHO, Severino Collier, **Números Inteiros e Criptografia RSA**. 2ª ed, Rio de Janeiro, IMPA, 2005.

COUTINHO, Severino Collier, **Criptografia**. Rio de Janeiro, IMPA, 2016.

COUTO, Sérgio Pereira. **Códigos & Cifras**: da antiguidade à era moderna. Rio de Janeiro (RJ): Novaterra, 2008.

DUARTE, Felipe De Almeida. **A Álgebra Na Criptografia.** Cornélio Procópio, UTFPR, 2015.

DUPONT, Quinn. **The Cryptological Origins Of Machine Translation. From al-Kindi to Weaver**, Amodern, 2017.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**. Lisboa, Universidade de Lisboa, 2010.

HEFEZ, Abramo. **Aritmética.** Rio de Janeiro, SBM, 2013.

MÜLLER, Didier. **Les Chiffres Hébreux.** 2004, Disponível em: https://www.apprendre-en-ligne.net/crypto/subst/atbash.html. Acessado em: 19 de novembro de 2023.

PAIXÃO, Jéssica Shayanne. **Criptografia: história, atividades e divulgação científica**. São Carlos, USP, 2020.

PINTO, Nilmara de Jesus Biasca Pinto. et al. **PET - 10º Brincando de Matemático: Criptografia.** Curitiba, UFPR, 2014.

SANTOS, Maria Camilla da Silva. **Criptografia RSA.** Arapiraca**,** Universidade Federal de Alagoas, 2018.

SEABRA, Diego Felipe Silveira. **Criptologia: uma abordagem histórica e matemática**. São Carlos, Universidade de São Carlos, 2010.

SILVA, Alexandre Ferreira. MARTINS, Renato Marinho. **Criptografia: aspectos históricos e matemáticos**. Belém, Universidade do Estado do Pará, 2011.

SINGH, Simon. **The Code Book.** New York, Anchor Books, 2000.

YBC 2743; Old Babylonian. Clay, Tabuleta redonda, cálculo da raiz quadrada de 2. Yale Peabody Museum. 2022, Disponível em: https://collections.peabody.yale.edu/search/Record/YPM-BC-021354. Acessado em: 19 de novembro de 2023.

YONG, Nicholas. **Espionagem industrial: como a China conseguiu segredos tecnológicos dos EUA.** BBC News. 2023, disponível em https://www.bbc.com/portuguese/internacional-64336494. Acessado em: 19 de novembro de 2023.