UM MÉTODO CRIPTOGRÁFICO BASEADO EM FUNÇÕES DE Z_n

LUCIANO PAULO DO NASCIMENTO
ROBSON PEREIRA DE SOUSA

rfb editora

RFB Editora
CNPJ: 39.242.488/0001-07
91985661194
www.rfbeditora.com
adm@rfbeditora.com
Tv. Quintino Bocaiúva, 2301, Sala 713, Batista Campos, Belém - PA, CEP: 66045-315

Editor-Chefe
Prof. Dr. Ednilson Ramalho
Diagramação, revisão e capa
Autores

Bibliotecária
Janaina Karina Alves Trigo Ramos-CRB 8/9166
Produtor editorial
Nazareno Da Luz

Dados Internacionais de Catalogação na Publicação (CIP)

N235m

Um método criptográfico baseado em funções de Zn / Luciano Paulo do Nascimento, Robson Pereira de Sousa. – Belém: RFB, 2024.

Livro em pdf.
32p.

ISBN 978-65-5889-736-1
DOI 10.46898/rfb.2f049199-dc27-410b-84cd-309d468da108

Criptografia. 2. Funções matemáticas. 3. Teoria dos números. I. Nascimento, Luciano Paulo do. II. Sousa, Robson Pereira de. III. Título.

CDD 005.82

Índice para catálogo sistemático:
Criptografia: Métodos baseados em funções matemáticas. 2. Teoria dos números: Aplicações em criptografia.

Nossa missão é a difusão do conhecimento gerado no âmbito acadêmico por meio da organização e da publicação de livros científicos de fácil acesso, de baixo custo financeiro e de alta qualidade!

Nossa inspiração é acreditar que a ampla divulgação do conhecimento científico pode mudar para melhor o mundo em que vivemos!

Equipe RFB Editora

rfb editora

DEDICATÓRIA

Eu Luciano Paulo, dedico esse trabalho ao meu pai, José Roberto, que nunca estará ausente pois a memória dos seus entes queridos sempre o fará presente.

AGRADECIMENTOS

Este livro é fruto de um trabalho de conclusão de curso. Neste caso, cabe aqui, eu Luciano Paulo tecer alguns agradecimentos

Em primeiro lugar gostaria de agradecer a ajuda no desenvolvimento deste trabalho ao professor e orientador, Robson Pereira de Sousa, por suas orientações e apoio diferenciado durante todas as etapas do processo. Agradeço a Joao Victor por sua contribuição com conhecimentos técnicos que foram bastante relevantes para o término da escrita.

Devo gratidão a minha esposa, Lenyedna Farias, pelo apoio e paciência nessa caminhada da graduação. Agradeço a minha mãe, Aleite Paulo, por ter sempre me incentivado nas diversas etapas da graduação. Agradeço a Teodoro Augusto, Daniel Lima e Davi Jose, amigos de longa data, pela força dada em algum momento desse trajeto.

SUMÁRIO

1 - Prefácio

A criptografia é uma presença constante em nosso cotidiano, manifestando-se de diversas formas, todas com o propósito de manter o sigilo de informações sensíveis. Ela se faz presente em transações comerciais online, como compras com cartão de crédito, na troca de mensagens em aplicativos de mensagens instantâneas, entre outras situações. Seu objetivo fundamental é garantir que apenas pessoas autorizadas possam compreender o conteúdo das comunicações.

Essa prática de escrever de maneira a manter o sigilo para terceiros é ancestral e evoluiu significativamente ao longo da história. Esse processo de refinamento contínuo da criptografia conta com a integração da matemática, especialmente da Teoria dos Números, que introduz conceitos fundamentais como divisão, números primos, congruências, classes de restos, entre outros.

Diante desse contexto, este trabalho propõe-se a apresentar a criptografia por meio de uma análise histórica e de alguns criptossistemas, explorando sua interação com a Teoria dos Números. Por meio de uma abordagem bibliográfica e exploratória, buscamos coletar informações relevantes que atendam aos objetivos estabelecidos, filtrando e organizando os elementos necessários para a construção deste texto.

Inicialmente, oferecemos uma visão panorâmica da criptografia, acompanhada de definições básicas e conceitos essenciais. Em seguida, estruturamos a base teórica, apresentando os principais conceitos, propriedades e teoremas da Teoria dos Números, incluindo a definição do conjunto $\mathbb{Z}_n$ das classes de congruência módulo n.

Inicialmente, exploramos o desenvolvimento histórico da criptografia, destacando métodos clássicos que permitem ao leitor familiarizar-se com o tema. oferecendo uma visão panorâmica, acompanhada de definições básicas e conceitos essenciais. No segundo capítulo, estruturamos a base teórica, apresentando os principais conceitos, propriedades e teoremas da Teoria dos Números, incluindo a definição do conjunto $\mathbb{Z}_n$ das classes de congruência

módulo n. Já no terceiro capítulo, introduzimos elementos que servirão de base para a formalização de modelos de criptossistemas, exemplificando algumas possibilidades de modelos criptográficos.

Por fim, apresentamos as considerações finais, onde refletimos sobre os resultados obtidos e delineamos possíveis caminhos para futuras pesquisas nesse campo tão vasto e dinâmico da criptografia.

Os autores.

2 - A CRIPTOGRAFIA AO LONGO DA HISTÓRIA

Nesta seção apresentaremos um resumo da história da criptografia ao longo dos séculos. Nela estará contida algumas definições e alguns exemplos de sistemas de criptografia que surgiram ao longo da história.

2.1 UM BREVE HISTÓRICO

A comunicação é algo de extrema importância na sociedade de hoje. Porém, a necessidade de se comunicar é algo que vem desde a antiguidade. Não obstante ao todo, mas de forma particular, o envio e o recebimento de mensagens tiveram diversas mudanças ao longo do percurso histórico. Singh (2020) comenta que em momentos específicos, foi indispensável a ocultação dessas mensagens pelos mais diversos motivos. Diz ainda que a criptografia foi decisiva para o resultado de batalhas e com isso provocando a morte de reis e rainhas. Nessa paisagem de ocultação, podemos citar a esteganografia.

Segundo Fiarresga (2010), a ocultação de mensagens poderia ser realizada através da esteganografia e esse nome deriva do grego e significa escrita coberta. Como o próprio nome sugere, a técnica consiste em ocultar a existência de uma mensagem. Diferentes formas dessa técnica foram utilizadas ao longo da história. Entre as mais diversas maneiras da esteganografia estavam mensagens escrita em ovos, os mensageiros engoliam bolas de cera com mensagens, cabeça raspada, tinta invisível em baixas temperaturas, entre outras. O artifício oferece certa segurança, mas pode se tornar vulnerável a uma vigilância mais rigorosa. Encontrando a mensagem oculta o seu conteúdo fica explícito a qualquer leitor, pois a técnica consiste apenas em ocultar a mensagem. Com essa falha de segurança abre espaço para o surgimento da criptografia.

De acordo com Galdino (2014), uma das primeiras informações sobre a criptografia é do ano de 480 a.C. e tratava de conflitos entre Gregos e Persas. Para Coutinho (2014), a criptografia estuda os processos para codificação de uma mensagem de forma que apenas o destinatário legítimo tenha condições de interpretar o conteúdo escrito.

Segundo Singh (2020), o objetivo da criptografia não era ocultar a existência de uma mensagem. A finalidade era esconder o significado – esse procedimento é chamado de encriptação. Embora a esteganografia e criptografia fossem técnicas distintas, existe a possibilidade de aliar as duas técnicas para tentar aumentar o nível de segurança da mensagem. Essa combinação gerava dois obstáculos. O primeiro seria descobrir que existia uma mensagem oculta e o segundo seria, caso houvesse acesso ao conteúdo, entender o seu teor.

Na criptografia, para tornar uma mensagem incompreensível, o texto era alterado seguindo um protocolo particular, esse já previamente conhecido pelo transmissor e receptor. Dessa maneira,

mesmo a mensagem sendo interceptada, na teoria, o conteúdo não faria sentido algum para o intermediário.

Alguns conceitos são importantes na criptografia. De acordo com Stewart (2016) podemos definir alguns termos:

- Texto original: a mensagem original.
- Texto cifrado: a versão codificada ou encriptada da mensagem original.
- Algoritmo de encriptação: o método usado para converter a mensagem original para o texto cifrado.
- Algoritmo de desencriptação: o método usado para converter o texto cifrado para o texto original.
- Chave: informação necessária para encriptar ou desencriptar a mensagem

Além disso, Coutinho (2014) definia o decifrar como a descoberta da chave por um leitor não lícito da mensagem. O decifrar é a tarefa mais complexa e poderá se tornar ainda mais de acordo com a complexibilidade do algoritmo de encriptação empregado no processo.

A processo de encriptação, segundo Fiarresga (2010), pode ser realizado conforme cifras de transposição e cifras de substituição. A primeira consiste em cada letra utilizada ser mantida na mensagem, todavia ela muda de posição. Enquanto isso, na cifra de substituição cada letra mantém a sua posição, mas é substituída por outra letra ou símbolo.

A utilização da criptografia aparece em diversos recortes e das mais variadas maneiras ao longo da história da humanidade. O Citale espartano é um exemplo clássico de uma forma de encriptar. De acordo com Ganassoli e Schankoski (2015), o Citale era um instrumento militar do século V a.C., e utilizava a cifra de transposição. Esse instrumento era constituído de uma fita de couro ou pergaminho envolto em um bastão de madeira. Para confeccionar a mensagem era preciso escrever na fita envolvida no bastão. Após desenrolar a fita do bastão, as letras eram misturadas. O destinatário recebia a fita e para ler a mensagem era preciso envolver a fita em um bastão de mesmo diâmetro.

Figura 1 – Citale Espartano

Fonte: GANASSOLI; SCHANKOSKI (2015, p.8)

Essa outra modalidade de cifrar um texto, método de substituição, tem um destaque quando

se fala da história da criptografia. Relata Singh (2020) que, no primeiro século antes de Cristo, César utilizava um método que consistia em substituir uma letra por outra que estivesse em três posições à frente na sequência do alfabeto. Desse jeito, ajustando para o nosso alfabeto, podemos colocar o alfabeto natural em cima e abaixo como o deslocamento de três unidades. Conforme tabela abaixo:

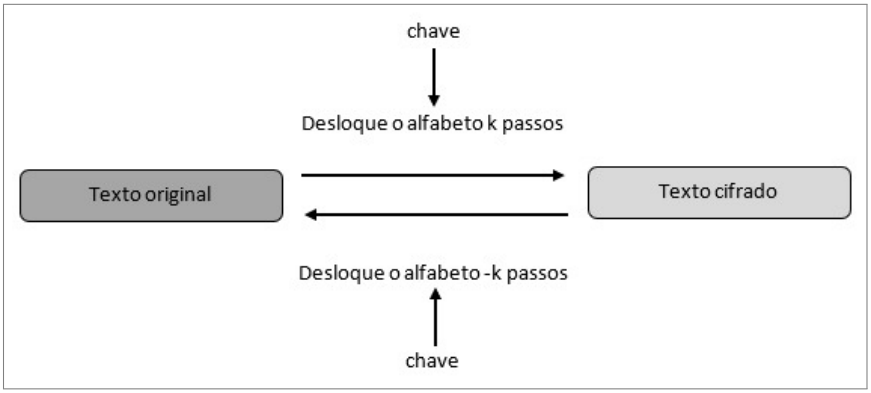
Tabela 1 – Correspondência da Cifra de César

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

Fonte: Elaboração própria em 2022

A Cifra de César é um caso particular de um método. Porém a cifra pode ser generalizada para um deslocamento de X unidades, onde esse X vai ser um número natural partindo de 1 até o máximo de números de letras do alfabeto utilizado menos uma unidade. Stewart (2016) diz que, em uma cifra de César, a chave é o número de passos que o alfabeto é deslocado. O algoritmo de encriptação indica a deslocar o alfabeto X passos e a desencriptação é o deslocamento de X passos no sentido inverso. A imagem abaixo sintetiza a cifra de César para um deslocamento qualquer.

Figura 2 – Síntese da Cifra de César



Fonte: STEWART (2016, p.311)

Podemos perceber que essa cifra de César é algo bem rudimentar. De acordo com Jesus (2013), esse modelo era pouco seguro pois apresenta poucas possibilidades, e um estudo de frequência de letras da língua do alfabeto poderia ajudar na ação de decifrar uma mensagem.

A criptografia evoluiu de acordo com a necessidade de mais segurança para as mensagens cifradas. E essa evolução foi gerando sistemas mais seguros para que terceiros não autorizados não conseguissem interpretar um texto codificado. Como fruto de uma dessas evoluções ao longo do tempo, temos uma cifra bastante conhecida da história, a cifra de Vigenère. O nome foi em

homenagem ao francês Blaise de Vigenère que viveu no século XVI. Segundo Singh (2020) foi o francês que montou a cifra baseada em ideias de antecessores. Misturou elas para formar essa nova cifra. Ganassoli e Schankoski (2015) definem esse modelo como uma cifra polialfabética, que consiste na utilização de dois ou mais alfabetos cifrados, usados alternadamente, de modo a aumentar consideravelmente a dificuldade de pessoas não autorizadas terem acesso as informações do texto encriptado.

Na cifra de Vigenère, tabela abaixo, podem ser utilizados quaisquer alfabetos desse quadro. A quantidade será determinada no momento da montagem do algoritmo de encriptação. Por exemplo, seria possível cifrar a primeira letra da mensagem com o alfabeto 22, a segunda de acordo com alfabeto 12, a terceira com o alfabeto 7, e assim por diante. Dessa maneira haveria 26 possibilidades de alfabeto disponíveis para essa tarefa. Singh (2020) relata que essa cifra foi bastante utilizada por muito tempo pela sua característica de segurança.

Tabela 2 – Quadrado de Vigenère

Alfabeto correto	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	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
26	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

Fonte: SINGH (2020, p.86)

Todavia, em algum momento esse tipo de modelo não se tornou mais tão seguro. E a criptografia seguiu evoluindo através dos embates entre quem formulava os algoritmos de encriptação e os criptoanalistas. Esses últimos, são os responsáveis por decifrar mensagens criptografadas sem conhecer a chave. Nisso, vão surgindo diversos modelos com a finalidade de aumentar o sigilo da informação enviada.

Um fato bastante relevante foi o uso da criptografia durante a Segunda Guerra Mundial. De acordo com Singh (2020), a criptografia aliada ao advento das máquinas teve grande relevância

em acontecimentos históricos e decisivos na guerra. Segundo Ganassoli e Schankoski (2015) isso abriu caminho para o uso de computadores na criptografia. Os computadores ajudavam a tornar os códigos mais difíceis e complexos. Essa constante evolução foi seguindo no decorrer dos anos, através dos mais variados personagens e suas contribuições. Ainda segundo Ganassoli e Schankoski (2015), nesse desenvolvimento no decorrer do tempo e com a entrada da aritmética modular foi desenvolvido o método RSA, o qual é utilizado até hoje.

Diante desse panorama histórico rápido, conseguimos ter noção do que seja a criptografia e alguns modelos clássicos. No método RSA a matemática se faz presente de forma clara. Porém esse não é o objetivo desse trabalho.

Perante esse breve relato da história surge a pergunta: Onde a matemática pode se inserir nesse simples modelo de criptografia? Como transformar isso em um modelo matemático e onde poderemos ter uma conexão com a Teoria do Números?

A ideia é selecionar alguns desses recortes históricos e verificar que eles podem ser descritos como modelos de criptografia através de funções de $\mathbb{Z}_n$ em $\mathbb{Z}_n$. Para isso, na próxima etapa iremos apresentar alguns conceitos que servirão de base para definir esses modelos. Serão apresentados conceitos iniciais, propriedades e teoremas da Teoria dos Números. Dessa forma conseguiremos realizar uma associação entre a criptografia e a Teoria dos números.

3 - O CONJUNTO Z_n

Neste capítulo apresentaremos definições, proposições e teoremas da Teoria dos Números que serão essenciais à compreensão do capítulo seguinte. Todavia, os resultados não serão demonstrados, o leitor interessado poderá consultá-los em Polcino e Coelho (2001) ou Filho (1981). Além disso, o leitor familiarizado com tais conceitos pode, se desejar, avançar para o capítulo seguinte.

3.1 Divisibilidade

Nesta seção estudaremos alguns resultados do conjunto dos números inteiros

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Vale ressaltar que para as nossas pretensões iremos considerar o conjuntos dos números naturais como sendo o conjunto

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

Vamos começar definindo um conceito importante dos números inteiros: divisibilidade.

Definição 3.1.1. *Sejam a e b números inteiros. Diz-se que b divide a (ou que b é um divisor de a ou, ainda, que a é um múltiplo de b) se existe um inteiro c tal que $bc = a$.*

Usaremos a notação $b \mid a$ para indicar que b divide a. A negação dessa afirmação será indicada por $b \nmid a$.

Lema 3.1.1. *Sejam a e b inteiros, tais que $a \geq 0$ e $b > 0$. Então, existem q e r, tais que $a = bq + r$ e $0 \leq r < b$.*

Teorema 3.1.1. ***(Algoritmo da Divisão)*** *Sejam a e b inteiros com $b \neq 0$. Então, existem inteiros q e r, únicos, tais que $a = bq + r$ e $0 \leq r < |b|$.*

Definição 3.1.2. *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo d ($d > 0$) que satisfaz as condições:*

1. *$d \mid a$ e $d \mid b$*
2. *se $c \mid a$ e se $c \mid b$, então $c \leq d$*

Vamos designar o máximo divisor comum de a e b por mdc(a,b).

Definição 3.1.3. *Sejam a e b dois inteiros não conjuntamente nulos. Diz-se que a e b são primos entre si se, e somente se, o mdc(a,b) = 1.*

Teorema 3.1.2. ***(Teorema de Bézout)*** *Sejam a, b inteiros e d = mdc(a, b). Então, existem inteiros r e s tais que $d = ra + sb$.*

3.2 Congruências

Definição 3.2.1. *Seja $n \neq 0$ um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulo n se n divide $a - b$.*

Neste caso, escrevemos $a \equiv b \pmod{n}$

Proposição 3.2.1. *Seja n um inteiro fixo. Dois inteiros a e b são congruentes módulo n se, e somente se, eles têm como resto o mesmo inteiro quando dividimos por n.*

Proposição 3.2.2. *Sejam $n > 0$ um inteiro fixo, e a, b, c, d inteiros arbitrários. Então, valem as seguintes propriedades:*

1. $a \equiv a \pmod{n}$.
2. Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$
3. Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$
4. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv c + d \pmod{n}$
5. Se $a \equiv b \pmod{n}$, então $a + c \equiv b + c \pmod{n}$
6. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $ac \equiv bd \pmod{n}$
7. Se $a \equiv b \pmod{n}$, então $a^m \equiv b^m \pmod{n}$, para todo inteiro positivo m
8. Se $a + c \equiv b + c \pmod{n}$, então $a \equiv b \pmod{n}$

Definição 3.2.2. *Para cada inteiro $n \geq 1$, indicaremos por $\Phi(n)$ o número de inteiros positivos, menores ou iguais a n, que são relativamente primos com n. A função assim definida chama-se função Φ de Euler.*

Teorema 3.2.1. *Se $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ é a decomposição canônica do inteiro positivo $n \geq 1$, então:*

$$\Phi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \dots (p_r^{k_r} - p_r^{k_r - 1}).$$

Teorema 3.2.2. *Sejam a e n inteiros com $n \geq 1$, tais que mdc(a, n) = 1. Então,*

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

3.3 Classes de congruências

Definição 3.3.1. *Seja a um inteiro. Chama-se classe de congruência de a módulo n o conjunto formado por todos os inteiros que são congruentes a a módulo n. Denotaremos esse conjunto por $\overline{a}$. Temos, então,*

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$$

Definição 3.3.2. *Chamaremos de conjunto dos inteiros módulo n, e denotaremos por $\mathbb{Z}_n$, o conjunto das classes de congruências módulo n, dado por*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}.$$

Definição 3.3.3. *Em $\mathbb{Z}_n$ estão definidas duas operações: soma e produto. Mais explicitamente, definimos soma e produto em $\mathbb{Z}_n$ por*

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$e$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Proposição 3.3.1. *Em $\mathbb{Z}_n$ valem as seguintes propriedades:*

1. *Propriedade associativa: Para toda terna $\overline{a}$, $\overline{b}$, $\overline{c}$ de inteiros módulo n, tem-se que*

$$\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}.$$

2. *Existência do Neutro: Existe um único elemento em $\mathbb{Z}_n$, que é precisamente $\overline{0}$, a classe do elemento 0, tal que*

$$\overline{a} + \overline{0} = \overline{a} \text{ para todo } \overline{a} \in \mathbb{Z}_n.$$

3. *Existência do Oposto: Para cada inteiro módulo n, $\overline{a}$, existe um único elemento em $\mathbb{Z}_n$, que chamaremos oposto de $\overline{a}$ e indicaremos por $-\overline{a}$, tal que*

$$\overline{a} + (-\overline{a}) = \overline{0}.$$

4. *Propriedade Comutativa Aditiva: Para todo par $\overline{a}$, $\overline{b}$ de elementos de $\mathbb{Z}_n$, tem-se que*

$$\overline{a} + \overline{b} = \overline{b} + \overline{a}.$$

5. *Propriedade Associativa: Para toda terna $\overline{a}$, $\overline{b}$, $\overline{c}$ de inteiros módulo n, tem-se que*

$$\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}.$$

6. *Existência do Neutro: Existe um único elemento em $\mathbb{Z}_n$, que é precisamente $\overline{1}$, tal que*

$$\overline{a} \cdot \overline{1} = \overline{a}.$$

7. *Propriedade Comutativa Multiplicativa: Para todo par $\overline{a}$, $\overline{b}$ de elementos de $\mathbb{Z}_n$, tem-se que*

$$\overline{a}\overline{b} = \overline{b}\overline{a}$$

8. Propriedade Distributiva: Para toda terna $\overline{a}$, $\overline{b}$, $\overline{c}$ de elementos de $\mathbb{Z}_n$, tem-se que

$$\overline{a}(\overline{b}+\overline{c}) = \overline{a}\overline{b} + \overline{a}\,\overline{c}$$

Definição 3.3.4. *Um elemento $\overline{a} \in \mathbb{Z}_n$ diz-se inversível se existe $\overline{a'} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{a'} = \overline{1}$. Um elemento $\overline{a'}$ nessas condições diz-se um inverso de $\overline{a}$.*

Proposição 3.3.2. *Se $\overline{a}$ é inversível em $\mathbb{Z}_n$, então seu inverso é único.*

Proposição 3.3.3. *Seja $\overline{a}$ um elemento não-nulo de $\mathbb{Z}_n$. Então, $\overline{a}$ é inversível se, e somente se, mdc(a,n) = 1.*

Definição 3.3.5. *Um elemento não-nulo $\overline{a}$ de $\mathbb{Z}_n$ diz-se um divisor de zero se existe $\overline{b} \in \mathbb{Z}_n$, também não nulo, tal que $\overline{a}\overline{b} = \overline{0}$.*

Proposição 3.3.4. *Se $\overline{a}$ não é um divisor de zero em $\mathbb{Z}_n$, então $\overline{a}^{\Phi(n)} = \overline{1}$.*

Note que esse resultado afirma, em particular, que o inverso de $\overline{a}$ pode ser obtido como uma potência [1] de $\overline{a}$, já que $\overline{a} \cdot \overline{a}^{\Phi(n)-1} = \overline{1}$, donde $\overline{a}^{\Phi(n)-1}$ é o inverso de $\overline{a}$.

Proposição 3.3.5. *Um elemento não nulo $\overline{a}$ de $\mathbb{Z}_n$ é divisor de zero se, e somente se, mdc(a, n) $\neq 1$.*

[1] Através da Definição 3.3.3 conclui-se que $\overline{a} \cdot \overline{a} \cdot \ldots \cdot \overline{a} = \overline{a}^n$, em que n é natural diferente de zero.

4 - UM MÉTODO DE CRIPTOGRAFIA VIA FUNÇÕES DE Z_n EM Z_n

Nesta etapa, tendo como base os capítulos anteriores, apresentaremos uma introdução à criptografia através de funções de $\mathbb{Z}_n$ em $\mathbb{Z}_n$.

4.1 Elementos iniciais do Cripto-sistema

Quando falamos no processo de criptografia pensamos em um texto original e um texto codificado. Eles podem ser escritos em um alfabeto qualquer e com a quantidade determinada de caracteres que esses alfabetos possuem. Porém, aqui, iremos utilizar o alfabeto latino com 26 caracteres. O alfabeto latino é dado pelos seguintes caracteres: a, b, c, ..., x, y, z.

Temos ciência de que um número de letras dispostas em uma determinada ordem forma uma mensagem simples e essa será única. Para cada mensagem simples haverá uma correspondente codificada que também será única. Isso deve ocorrer para não haver a possibilidade de falha na comunicação. Dessa maneira, poderemos visualizar o processo de codificação como uma função, fazendo uma associação de cada mensagem simples, que chamaremos de s, para uma mensagem codificada, que chamaremos de c.

De forma mais abrangente, vamos definir X como o conjunto de todas as possibilidades de mensagens simples e definir Y como o conjunto de todas as possibilidades de mensagens codificadas. Assim, cada uma das possíveis mensagens codificadas, que são os elementos do conjunto Y, terá uma mensagem simples, única e correspondente no conjunto X. Acrescentamos ainda que para quaisquer mensagens simples distintas, teremos mensagens codificadas diferentes. Com isso podemos afirmar que essa correspondência entre esses dois conjuntos é uma bijeção de X em Y.

Segundo Lima (2013), um cripto-sistema, ou sistema de criptografia, é um conjunto de elementos e procedimentos que permitem a criptografia. De acordo com isso, vamos perceber que a bijeção de X em Y é um cripto-sistema.

Definindo X como o conjunto de todas as mensagens simples possíveis e Y o conjunto de todas as mensagens codificadas. De forma geral, podemos entender o processo de codificação da seguinte forma:

$$f\text{: X} \to \text{Y, tal que } f(s) = c$$

Já no processo de decodificação teremos a função inversa de f, que denotamos por f^{-1}, dada por:

$$f^{-1} : \mathrm{Y} \to \mathrm{X}, \text{ tal que } f^{-1}(c) = s$$

Na antiguidade foram usados diversos cripto-sistemas. Um deles que é bastante conhecido é a Cifra de César, que vimos anteriormente no capítulo três. O sistema consistia em substituir cada letra do alfabeto pela terceira letra a direita da sequência desse mesmo alfabeto. A letra A é substituída pela letra D, a B é substituída pela E, e assim por diante. Por fim, o Y é substituído pelo B e o Z pelo C. Para exemplificar, iremos codificar através da Cifra de César a mensagem a seguir:

OCULTAR DE TERCEIROS UMA INFORMAÇÃO

Para facilitar a visualização, usemos a Tabela 1 – Correspondência da Cifra de César. De acordo com a tabela faremos a substituição de cada letra. Dessa maneira a letra O será trocada pela letra R. A letra C deverá ser substituída pelo F e assim por diante. Após realizar a substituição de todas as letras da mensagem, obteremos a seguinte mensagem cifrada:

RFXOWDU GH WHUFHLURV XPD LQIRUPDFDR

Mais adiante explicaremos matematicamente uma possibilidade de representação desse cripto-sistema.

A partir de agora, vamos acrescentar um símbolo para o espaço entre as palavras. Escolheremos o asterisco (símbolo: *). Com isso, vamos definir o nosso alfabeto, onde chamaremos apenas de Ω (ômega). Ele será definido da seguinte forma: Ω = {a, b, c, ..., x, y, z, *}. Perceba que agora o nosso conjunto Ω terá 27 elementos. Como trabalharemos com funções de $\mathbb{Z}_n$ em $\mathbb{Z}_n$ e com o intuito de montar um cripto-sistema, faremos uma associação com o conjunto das classes de congruências módulo 27, ou seja,

$$\mathbb{Z}_{27} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, ..., \overline{24}, \overline{25}, \overline{26}\}.$$

A correspondência entre Ω e $\mathbb{Z}_{27}$ está expressa na tabela abaixo:

Tabela 3 – Correspondência de Ω com $\mathbb{Z}_{27}$

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	*
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$	$\overline{18}$	$\overline{19}$	$\overline{20}$	$\overline{21}$	$\overline{22}$	$\overline{23}$	$\overline{24}$	$\overline{25}$	$\overline{26}$

Fonte: Elaboração própria em 2022

4.2 Construção do cripto-sistema

No que segue, iremos mostrar uma possibilidade de construção de um cripto-sistema. O teorema abaixo vai servir de base para que isso aconteça.

Teorema 4.2.1. *Seja a função $f : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $f(x) = ax + b$, com $a,b \in \mathbb{Z}_n$ e $a \neq 0$. Se o mdc$(a,n) = 1$, então a função f é um cripto-sistema.*

Demonstração. Por hipótese temos que mdc$(a,n) = 1$. Como a é um elemento não-nulo de $\mathbb{Z}_n$, então existe $a^{'}$ único em $\mathbb{Z}_n$, de acordo com a Proposição 3.3.2, tal que $a^{'} \cdot a = \overline{1}$. Assim, teremos

$$f^{-1}(x) = a^{'}x - a^{'}b.$$

De fato, f^{-1} é a função inversa de f:

$$f(f^{-1}(x)) = a(a'x - a'b) + b = (aa')x - (aa')b + b = \overline{1}x - \overline{1}b + b = x - b + b = x$$

e

$$f^{-1}(f(x)) = a'(ax + b) - a'b = (a'a)x + a'b - a'b = \overline{1}x = x.$$

Portanto, concluímos que f é um cripto-sistema. ■

Vale ressaltar que qualquer cripto-sistema f nas condições do Teorema 4.2.1 pode ser decodificado, isto é, retornar à mensagem original, através da expressão

$$f^{-1}(x) = a^{'}x - a^{'}b.$$

Além disso, o inverso de a, que chamamos de a', pode ser calculado através da expressão $a^{\Phi(n)-1}$, isto é, $a' = a^{\Phi(n)-1}$, como podemos ver na Proposição 3.3.4. A exigência é que a não seja um divisor de zero, o que de fato vai acontecer pois sempre mdc(a, n) = 1, de acordo com o que foi descrito no Teorema 4.2.1.

Agora poderemos descrever a cifra de César através de uma função de $\mathbb{Z}_n$ em $\mathbb{Z}_n$. Baseado no teorema acima, fazendo a associação com a Tabela 3 e percebendo a cifra como

$$f(x) = ax + b, \text{ com } a = \overline{1} \text{ e } b = \overline{3}.$$

Temos o seguinte cripto-sistema que descreve a cifra:

$$f : \mathbb{Z}_{27} \to \mathbb{Z}_{27}, \text{ onde } c(x) = x + \overline{3}.$$

Exemplo 4.2.1. *Vamos utilizar o cripto-sistema acima para cifrar a palavra CRIPTOGRAFIA.*

Utilizando a Tabela 3, verificamos que o C corresponde ao $\overline{2}$, o R corresponde ao $\overline{17}$ e assim por diante. Com esses elementos elencados, podemos codificar aplicando-os na função. Com a imagem obtida, faremos novamente a correspondência com a Tabela 3, e assim codificaremos a mensagem.

$$f(\overline{2}) = \overline{2} + \overline{3} = \overline{5} = \text{f}$$
$$f(\overline{17}) = \overline{17} + \overline{3} = \overline{20} = \text{u}$$
$$f(\overline{8}) = \overline{8} + \overline{3} = \overline{11} = \text{l}$$
$$\vdots$$
$$f(\overline{8}) = \overline{8} + \overline{3} = \overline{11} = \text{l}$$
$$f(\overline{0}) = \overline{0} + \overline{3} = \overline{3} = \text{d}$$

Desse processo conseguimos a mensagem cifrada

FULSWRJUDILD

Para decodificar a mensagem basta utilizar a função inversa $f^{-1}(x) = x - \overline{3}$ com os elementos da mensagem codificada.

Exemplo 4.2.2. *Vamos utilizar a correspondência da Tabela 3 e o cripto-sistema*

$$g : \mathbb{Z}_{27} \to \mathbb{Z}_{27}, \text{onde } g(x) = \overline{8}x + \overline{7}$$

para cifrar a mensagem

AS CLASSES DE CONGRUÊNCIAS

Com efeito,

$$g(\overline{0}) = \overline{8} \cdot \overline{0} + \overline{7} = \overline{7} = \text{h}$$
$$g(\overline{18}) = \overline{8} \cdot \overline{18} + \overline{7} = \overline{151} = \overline{16} = \text{q}$$
$$g(\overline{26}) = \overline{8} \cdot \overline{26} + \overline{7} = \overline{215} = \overline{26} = *$$
$$\vdots$$
$$g(\overline{0}) = \overline{8} \cdot \overline{0} + \overline{7} = \text{h}$$
$$g(\overline{18}) = \overline{8} \cdot \overline{18} + \overline{7} = \overline{151} = \overline{16} = \text{q}$$

Com isso, através do cripto-sistema escolhido, conseguimos a seguinte mensagem criptografada:

*HQ*XOHQQMQ*EM*XLDBIFMDXRHQ*

Podemos também decodificar a mensagem. Para isso, vamos utilizar a função inversa de g. Sabemos que a função inversa de $f(x) = ax + b$ é dada por $f^{-1}(x) = a'x - a'b$. Neste caso, temos que encontrar o inverso de $\overline{8}$. Com efeito, $\overline{a} = \overline{8}$ e $n = 27$, e então o inverso de $\overline{8}$ é dado por $\overline{8}^{\Phi(27)-1}$. Temos, pelo Teorema 3.2.1, que

$$\Phi(27) = \Phi(3^3) = 3^3 - 3^2 = 18.$$

Logo,

$$\overline{8}^{\Phi(27)-1} = \overline{8}^{18-1} = \overline{8}^{17}.$$

Agora devemos encontrar o correspondente a $\overline{8}^{17}$ em $\mathbb{Z}_{27}$. Ora, $8^3 \equiv 26 \pmod{27}$. Mas $26 \equiv -1 \pmod{27}$. Portanto,

$$8^3 \equiv -1 \pmod{27} \Longrightarrow 8^{15} \equiv -1 \pmod{27} \Longrightarrow 8^{17} \equiv -64 \pmod{27}.$$

Como $-64 \equiv 17 \pmod{27}$, concluímos que

$$8^{17} \equiv 17 \pmod{27}.$$

Disso, temos que

$$g^{-1}(x) = \overline{17}x - \overline{17} \cdot \overline{7} = \overline{17}x - \overline{119} = \overline{17}x + 16.$$

Novamente usaremos a Tabela 3 e faremos a correspondência com os elementos da mensagem codificada utilizando g^{-1}.

$$\begin{gathered} g^{-1}(\overline{7}) = \overline{17} \cdot \overline{7} + \overline{16} = \overline{135} = \overline{0} = \text{a} \\ g^{-1}(\overline{16}) = \overline{17} \cdot \overline{16} + \overline{16} = \overline{288} = \overline{18} = \text{s} \\ g^{-1}(\overline{26}) = \overline{17} \cdot \overline{26} + \overline{16} = \overline{458} = \overline{26} = * \\ \vdots \\ g^{-1}(\overline{16}) = \overline{17} \cdot \overline{16} + \overline{16} = \overline{288} = \overline{18} = \text{s} \end{gathered}$$

Com isso, decodificamos a mensagem criptografada e retornamos para a mensagem original

AS CLASSES DE CONGRUÊNCIAS

É fácil perceber que cada cripto-sistema da forma do Teorema 4.2.1 gera uma permutação do alfabeto determinado. Para exemplificar, apresentaremos a permutação gerada pelo cripto-sistema g através da tabela

Tabela 4 – Permutação gerada por g

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	*
h	p	x	e	m	u	b	j	r	z	g	o	w	d	l	t	a	i	q	y	f	n	v	c	k	s	*

Fonte: Elaboração própria em 2022

Para conseguir essa permutação do alfabeto, basta aplicar todos os caracteres em g. Vale ressaltar que, pelo princípio fundamental da contagem [2], existem $n!$ possíveis cripto-sistemas,

[2] O leitor poderá consultar esse resultado em Morgado et al. (2006, p.28)

em que n é número de caracteres do alfabeto escolhido. Em particular, para

$$\Omega = \{\text{a}, \text{b}, \text{c}, ..., \text{x}, \text{y}, \text{z}, *\}$$

existem $27!$ cripto-sistemas.

4.3 Cripto-sistema em blocos

Tratamos até este momento de associações entre um caractere e um elemento do conjunto da classe de congruência $\mathbb{Z}_{27}$. Cada um desses caracteres sozinho é um bloco formado por um elemento. Contudo, esses blocos não precisam ser de apenas um símbolo. Os blocos podem ter k símbolos, onde k é um natural maior que 1. Neste caso, quanto maior a quantidade de caracteres por bloco mais segurança terá o cripto-sistema.

De forma geral, nesse modelo de criptografia com funções de $\mathbb{Z}_n$ em $\mathbb{Z}_n$, em um alfabeto de n caracteres, faremos a associação desses blocos com a classe de congruência

$$\mathbb{Z}_{n^k} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n^k - 1}\},$$

onde k representa o número de blocos escolhido no modelo.

Com isso, cada bloco B_i de k símbolos terá o seu correspondente em $\mathbb{Z}_{n^k}$ de modo que $B_i = (x_k, x_{k-1}, ..., x_2, x_1)$, onde cada x_i é um caractere do alfabeto devendo ser associado ao $\mathbb{Z}_n$ utilizado. Neste caso, B_i corresponde a $(x_k n^{k-1} + x_{k-1} n^{k-2} + ... + x_2 n + x_1)$, que pertence a $\mathbb{Z}_{n^k}$.

Uma observação pertinente consiste no fato de que o texto a ser criptografado não tem uma quantidade de símbolos que seja múltipla do número k de elementos do bloco. Quando acontecer esse fato, completaremos ao final com a quantidade mínima necessária de símbolos para que a quantidade total de caracteres seja múltipla de k.

Exemplo 4.3.1. *Utilizando a Tabela 3, vamos exemplificar como ficaria a correspondência dos blocos de 4 símbolos formados da palavra MATEMÁTICA e o conjunto $\mathbb{Z}_{n^k}$.*

Como a palavra em questão tem 10 caracteres e não é um múltiplo de 4, vamos preencher a quantidade mínima necessária para que o número seja múltiplo. Vamos determinar que preencheremos com a letra A os espaços restantes de agora em diante. Nesse caso, vamos acrescentar duas letras A. A palavra a ser codificada seria MATEMÁTICAAA.

Vamos separar em blocos de 4. Teremos

MATE MATI CAAA

Como teremos blocos de 4, associaremos os blocos aos elementos do conjunto

$$\mathbb{Z}_{27^4} = \mathbb{Z}_{531441} = \{\overline{0}, 1, \overline{2}, ..., \overline{531440}\}.$$

Para fazer essa associação usaremos

- *(M, A, T, E) = (*$\overline{12}$,$\overline{0}$,$\overline{19}$,$\overline{4}$*) = (*$\overline{12} \cdot \overline{27^3} + \overline{0} \cdot \overline{27^2} + \overline{19} \cdot \overline{27} + \overline{4}$*) =* $\overline{236713}$
- *(M, A, T, I) = (*$\overline{12}$,$\overline{0}$,$\overline{19}$,$\overline{8}$*) = (*$\overline{12} \cdot \overline{27^3} + \overline{0} \cdot \overline{27^2} + \overline{19} \cdot \overline{27} + \overline{8}$*) =* $\overline{236717}$
- *(C, A, A, A) = (*$\overline{2}$,$\overline{0}$,$\overline{0}$,$\overline{0}$*) = (*$\overline{2} \cdot \overline{27^3} + \overline{0} \cdot \overline{27^2} + \overline{0}.\overline{27} + \overline{0}$*) =* $\overline{39366}$

Exemplo 4.3.2. *Vamos utilizar o cripto-sistema*

$$h : \mathbb{Z}_{27^3} \to \mathbb{Z}_{27^3}, \text{ dada por } h(x) = \overline{40}x + \overline{14},$$

e codificar a palavra CRIPTOGRAFIA. Vamos utilizar o $k = 3$*, ou seja, blocos de 3 símbolos.*

A palavra escolhida para codificação tem um número de símbolos múltiplo de k*. Assim, não precisaremos do ajuste de completar com símbolos A. Agora vamos dividir a palavra em grupos de 3 símbolos e fazer a correspondência com a Tabela 3. Disso, obteremos:*

CRI PTO GRA FIA

Neste caso,

- *O bloco CRI corresponde a* $\overline{2} \cdot \overline{27^2} + \overline{17} \cdot \overline{27} + \overline{8} = \overline{1925}$
- *O bloco PTO corresponde a* $\overline{15} \cdot \overline{27^2} + \overline{19} \cdot \overline{27} + \overline{14} = \overline{11462}$
- *O bloco GRA corresponde a* $\overline{6} \cdot \overline{27^2} + \overline{17} \cdot \overline{27} + \overline{0} = \overline{4833}$
- *O bloco FIA corresponde a* $\overline{5} \cdot \overline{27^2} + \overline{8} \cdot \overline{27} + \overline{0} = \overline{3861}$

Com isso, aplicaremos esses valores em $h(x)$*.*

- $h(\overline{1925}) = \overline{40} \cdot \overline{1925} + \overline{14} = \overline{77014} = \overline{17965} = \overline{24} \cdot \overline{27^2} + \overline{17} \cdot \overline{27} + \overline{10}$*; realizando a correspondência com a tabela em relação ao* $\overline{24}$*,* $\overline{17}$ *e* $\overline{10}$ *obtemos o YRK*
- $h(\overline{11462}) = \overline{40} \cdot \overline{11462} + \overline{14} = \overline{458494} = \overline{5785} = \overline{7} \cdot \overline{27^2} + \overline{25} \cdot \overline{27} + \overline{7}$*; analogamente ao item anterior obteremos o HZH*
- $h(\overline{4833}) = \overline{40} \cdot \overline{4833} + \overline{14} = \overline{193334} = \overline{16187} = \overline{22} \cdot \overline{27^2} + \overline{5} \cdot \overline{27} + \overline{14}$*; obteremos WFO*
- $h(\overline{3861}) = \overline{40} \cdot \overline{3861} + \overline{14} = \overline{154454} = \overline{16673} = \overline{22} \cdot \overline{27^2} + \overline{23} \cdot \overline{27} + \overline{14}$*; obteremos WXO*

Disso, a mensagem criptografada é

YRKHZHWFOWXO

Agora, vamos calcular a inversa de h. Todavia não usaremos o método utilizado anteriormente que envolvia o cálculo de $\Phi(n)$, visto que, no caso em questão, $\Phi(27^3) = 13122$ e, neste caso, teríamos que encontrar o correspondente a $\overline{40}^{13121}$ em $\mathbb{Z}_{27^3}$.

Com efeito, veja que mdc$(40, 27^3)$ = 1. Pelo Teorema de Bézout 3.1.2, existem inteiros r e s tais que

$$1 = 40r + 27^3 s \text{ ou } 1 = 40r + 19683s.$$

Utilizando classes, temos que

$$\overline{1} = \overline{40}\overline{r} + \overline{19683}\overline{s}.$$

Como $\overline{19683} = \overline{0}$, então

$$\overline{1} = \overline{40}\overline{r}.$$

Neste caso, $\overline{r}$ é o inverso de $\overline{40}$. Uma solução [3] possível para a equação $1 = 40r + 19683s$ é

$$1 = 40 \cdot 6397 + 19683 \cdot (-13).$$

Veja que, utilizando classes, obteríamos

$$\overline{1} = \overline{40} \cdot \overline{6397}.$$

Dessa forma, $\overline{6397}$ é o inverso de $\overline{40}$ em $\mathbb{Z}_{27^3}$.

Deste modo,

$$h^{-1}(x) = \overline{6397}x + \overline{8857}.$$

De forma análoga ao processo para transformar a mensagem simples em criptografada, faremos para transformar a mensagem criptografada em mensagem simples:

YRK HZH WFO WXO

YRK corresponde a $\overline{24} \cdot \overline{27^2} + \overline{17} \cdot \overline{27} + \overline{10} = \overline{17965}$. Da mesma forma, HZH corresponde a $\overline{5785}$, WFO é o $\overline{16187}$ e WXO é $\overline{16673}$.

Agora temos os valores para aplicação em $h^{-1}(x)$.

$$h^{-1}(\overline{17965}) = \overline{6397} \cdot \overline{17965} + \overline{8857} = \overline{114930962} = \overline{1925} = \overline{2} \cdot \overline{27^2} + \overline{17} \cdot \overline{27} + \overline{8},$$

que corresponde ao bloco CRI.

Da mesma forma, aplicando os outros valores em h^{-1}, obtemos $h^{-1}(\overline{5785})$ correspondente ao bloco PTO, $h^{-1}(\overline{16187})$ é o GRA e $h^{-1}(\overline{16673})$ é FIA. Com isso, naturalmente, voltamos para a mensagem simples

CRIPTOGRAFIA

[3] É possível encontrar essa solução particular através de divisões sucessivas utilizando o algoritmo de Euclides. O leitor interessado poderá consultar Polcino e Coelho (2001, p.71 - 73)

4.4 Criptografia com a Cifra de Vigenère

Outro modelo de criptografar bastante destacado na história é a cifra de Vigenère. Conforme dito anteriormente, esse modelo é uma variação da Cifra de César e foi criado no sentido de proporcionar mais segurança ao sistema. Na Cifra de César determina-se um deslocamento de n casas. Partindo disso, o método de criptografar vai ser realizado usando essa única alteração do alfabeto. Porém, na Cifra de Vigenère são utilizados mais de um deslocamento, ou seja, mais de um alfabeto com deslocamentos distintos. Os deslocamentos possíveis estão descritos no quadrado de Vigenère (Tabela 2). O uso do alfabeto será determinado através de uma senha estabelecida através de uma palavra. Dessa maneira escolhe-se uma palavra $X_1X_2X_3...X_n$, onde X_n representa a enésima letra da palavra. Com isso, a primeira letra do texto simples a ser cifrado seria realizada com o alfabeto que tenha X_1 na segunda coluna do quadrado de Vigenère modificado, que será apresentado em seguida, a segunda letra através do alfabeto que tenha X_2 na segunda coluna, e assim sucessivamente. Com isso, de maneira geral, usaremos o cripto-sistema abaixo:

$$v : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dado por } v_n(x) = x + \overline{b},$$

onde $\overline{b}$ é o elemento correspondente a X_n da classe de congruência de acordo com o alfabeto utilizado.

Tabela 5 – Quadrado de Vigenère modificado

Alfabeto correto	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	*
$\overline{0}$	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	*
$\overline{1}$	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
$\overline{2}$	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
⋮													⋮														⋮
$\overline{24}$	Y	Z	*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
$\overline{25}$	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
$\overline{26}$	*	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

Fonte: Elaboração própria em 2022

Exemplo 4.4.1. *Usaremos a tabela modificada do quadrado de Vigenère e definiremos como senha a palavra NATAL. Com o cripto-sistema $v_n(x)$, vamos codificar o texto*

ROBSON É O PROFESSOR

De acordo com a Tabela 4 e a senha teremos a seguinte correspondência:

(N, A, T, A, L) implicaria em ($\overline{13}$, $\overline{0}$, $\overline{19}$, $\overline{0}$, $\overline{11}$)

Com isso usaremos:

- $v_1(x) = x + \overline{13}$, *para os elementos nas posições* $5a + 1$, *com* a *pertencente aos naturais*
- $v_2(x) = x + \overline{0}$, *para os elementos nas posições* $5a + 2$, *com* a *pertencente aos naturais*
- $v_3(x) = x + \overline{19}$, *para os elementos nas posições* $5a + 3$, *com* a *pertencente aos naturais*
- $v_4(x) = x + \overline{0}$, *para os elementos nas posições* $5a + 4$, *com* a *pertencente aos naturais*
- $v_5(x) = x + \overline{11}$, *para os elementos nas posições* $5a$, *com* a *pertencente aos naturais*

Agora realizando a correspondência de cada caractere do texto simples e aplicando na função $v(x)$, *vamos obter:*

- *R, corresponde a* $v_1(\overline{17}) = \overline{17} + \overline{13} = \overline{30} = \overline{3}$, *que representa o D*
- *O, corresponde a* $v_2(\overline{14}) = \overline{14}$, *que representa o O*
- *B, corresponde a* $v_1(\overline{1}) = \overline{1} + \overline{19} = \overline{20}$, *que representa o U*

$\vdots$

- *S, corresponde a* $v_3(\overline{18}) = \overline{18} + \overline{19} = \overline{37} = \overline{10}$, *que representa o K*
- *O, corresponde a* $v_4(\overline{14}) = \overline{14}$, *que representa o O*
- *R, corresponde a* $v_5(\overline{17}) = \overline{17} + \overline{11} = \overline{28} = \overline{1}$, *que representa o B*

Disso, obtemos a mensagem criptografada

*DOUSZ**X*ZMPJOQRSKOB*

O receptor da mensagem cifrada vai ter a senha escolhida. Com isso, ele conseguirá determinar a inversa de $v_n(x)$ para trazer a mensagem criptografada para a simples. Como temos a senha NATAL, a inversa será dada por:

- $v_1^{-1}(x) = x - \overline{13}$, para os elementos nas posições $5a + 1$, com a pertencente aos naturais
- $v_2^{-1}(x) = x$, para os elementos nas posições $5a + 2$, com a pertencente aos naturais
- $v_3^{-1}(x) = x - \overline{19}$, para os elementos nas posições $5a + 3$, com a pertencente aos naturais;
- $v_4^{-1}(x) = x$, para os elementos nas posições $5a + 4$, com a pertencente aos naturais
- $v_5^{-1}(x) = x - \overline{11}$, para os elementos nas posições $5a$, com a pertencente aos naturais

Outra possibilidade para o cripto-sistema baseado na Cifra de Vigenère seria a junção com os blocos de mais de um elemento. Vamos apresentar um exemplo dessa possibilidade.

Exemplo 4.4.2. *Utilizando-se, mais uma vez, da tabela modificada do quadrado de Vigenère, vamos escolher a senha XVI e trabalhar com blocos de três elementos. Com o cripto-sistema* $v_n(x)$, *iremos criptografar o texto simples*

O BLAISE VIGENÈRE NASCEU NA FRANÇA

A senha XVI implica em $(\overline{23}, \overline{21}, \overline{8})$*, neste caso teremos*

$$v_n : \mathbb{Z}_{27^3} \to \mathbb{Z}_{27^3}$$

em que

- $v_1(x) = x + \overline{23}$*, para os elementos nas posições* $3a + 1$*, com* a *pertencente aos naturais*
- $v_2(x) = x + \overline{21}$*, para os elementos nas posições* $3a + 2$*, com* a *pertencente aos naturais*
- $v_3(x) = x + \overline{8}$*, para os elementos nas posições* $3a$*, com* a *pertencente aos naturais*

Agora vamos dividir o texto simples em grupos de 3 símbolos e fazer a correspondência com o alfabeto Ω*. Obteremos*

*O*B LAI SE* VIG ENÈ ... ANÇ AAA*

Como o número de símbolos não é um múltiplo de 3, completamos com o mínimo de letras A possível para formar um múltiplo de 3. Nesse caso foram duas letras A. Agora iremos ver o que cada bloco representa em $\mathbb{Z}_{27^3}$:

- *O*B é representado por* $\overline{14} \cdot \overline{27^2} + \overline{26} \cdot \overline{27} + \overline{1} = \overline{10909}$
- *LAI é representado por* $\overline{11} \cdot \overline{27^2} + \overline{0} \cdot \overline{27} + \overline{8} = \overline{8027}$
- *SE* é representado por* $\overline{18} \cdot \overline{27^2} + \overline{4} \cdot \overline{27} + \overline{26} = \overline{13256}$

$\vdots$

- *ANÇ é representado por* $\overline{0} \cdot \overline{27^2} + \overline{13} \cdot \overline{27} + \overline{2} = \overline{353}$
- *AAA é representado por* $\overline{0} \cdot \overline{27^2} + \overline{0} \cdot \overline{27} + \overline{0} = \overline{0}$

Agora temos os valores para aplicação em $v_n(x)$

- $v_1(\overline{10909}) = \overline{10909} + \overline{23} = \overline{10932} = \overline{14} \cdot \overline{27^2} + \overline{26} \cdot \overline{27} + \overline{24}$*, que corresponde ao bloco O*Y*
- $v_2(\overline{8027}) = \overline{8027} + \overline{21} = \overline{8048} = \overline{11} \cdot \overline{27^2} + \overline{1} \cdot \overline{27} + \overline{2}$*, que corresponde ao bloco LBC*
- $v_3(\overline{13256}) = \overline{13256} + \overline{8} = \overline{13264} = \overline{18} \cdot \overline{27^2} + \overline{5} \cdot \overline{27} + \overline{7}$*, que corresponde ao bloco SFH*

Após realizar esse procedimento teremos a mensagem criptografada

*O*YLBCSFHVJBENZRFHNBODFO*NI*GNANXAAI*

Fazendo o processo inverso em blocos de três e sabendo a senha conseguimos facilmente transformar a mensagem criptografada em mensagem simples.

Finalmente, considerando tudo o que vimos neste trabalho, finalizamos o que gostaríamos de produzir. Apesar disso, não esgotamos todas as virtudes que esses resultados nos dão. Neste capítulo, em particular, conseguimos apresentar elementos iniciais sobre a criptografia onde foi possível abordar um modelo de cripto-sistema. Além disso, conseguimos apresentar modelos clássicos de sistemas de criptografia em que estabelecemos uma relação com o cojunto das classes de congruências. O leitor será capaz, portanto, de reconhecer a ideia por trás do processo de criptografar e desencriptar, ao mesmo tempo que experimenta diferentes tipos de modelos de criptografia.

5 - Considerações Finais

Neste trabalho foi possível conhecer um pouco da história da criptografia, desde a sua importância, sendo inclusive a ser decisiva na guerra. Além disso, conhecemos sua evolução ao longo do tempo desde o modelo mais rudimentar de encriptar até o modelo RSA que é utilizado até hoje. Conhecemos alguns modelos clássicos que surgiram ao longo da história, dando destaque à Cifra de César e ao modelo de Vigènere. Foram apresentados os conceitos fundamentais de teoria dos números que são relevantes para o entendimento dos Cripto-sistemas via funções onde o domínio e o contradomínio eram conjuntos de classes de congruências. Foi definido matematicamente uma possibilidade de montagem de cripto-sistema, a partir disso, foi realizada a conexão de sistemas clássicos com a teoria matemática vista. Tendo como base o que foi apresentado, mostramos algumas exemplificações de cripto-sistemas e algumas variações deles com o advento dos blocos de dois ou mais elementos.

Durante a realização do trabalho foi percebido que a história da criptografia nos apresentou um rico caminho e nele foi possível observar que ainda existe bastante espaço para exploração de outros diversos pontos ao longo do período histórico. Além disso, experimentamos uma aplicação direta da matemática, mais precisamente, da Teoria dos Números, em um tema comum no dia a dia e atual.

Com o exposto, conseguimos atingir os objetivos traçados inicialmente e ficou percebido de forma clara que o assunto é abundantemente abrangente, instigante e contemporâneo. Sendo assim desperta interesse para pesquisas posteriores. Um ponto que pode ser viável é estudar alguma maneira de formatar este trabalho de modo a transformar ele em um produto que seja acessível para estudantes do ensino básico, além de outras possibilidades que trabalhar com a criptografia nos possibilita.

Referências

COUTINHO, S. C. **Números inteiros e criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2014.

FIARRESGA, V. M. C. Criptografia e matemática. Tese de Doutorado. Faculdade de Ciências da Universidade de Lisboa, 2010. Disponível em: <http://hdl.handle.net/10451/3647>. Acesso em: 19 de abr. de 2022.

FILHO, E. d. A. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

GALDINO, U. A. Teoria dos números e criptografia com aplicações básicas. Universidade Estadual da Paraíba, 2014. Disponível em: <http://tede.bc.uepb.edu.br/jspui/handle/tede/2266>. Acesso em: 19 de abr. de 2022.

GANASSOLI, A. P.; SCHANKOSKI, F. R. Criptografia e matemática. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT/UFPR). Curitiba, 2015. Disponível em: <http://www.educadores.diaadia.pr.gov.br/arquivos/File/fevereiro2016/matematica_dissertacoes/dissertacao_fernanda_ricardo_scankoski.pdf>. Acesso em: 19 de abr. de 2022.

JESUS, A. L. N. D. Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes. Mestrado Profissional em Matem´atica em Rede Nacional PROFMAT/UNIVASF. Bahia, 2013. Disponível em: <https://portais.univasf.edu.br/profmat/dissertacoes/andre_luis_neris_de_jesus_turma_2011.pdf>. Acesso em: 19 de abr. de 2022.

MORGADO, A. C. et al. **Análise Combinatória e Probabilidade**. 9. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006.

POLCINO, C.; COELHO, S. **Números: Uma Introdução à Matemática**. 3. ed. São Paulo: Editora da Universidade de São Paulo, 2001.

SINGH, S. **O livro dos códigos**. Tradução: Jorge Calife. 12. ed. Rio de Janeiro: Record, 2020.

STEWART, I. **O Fantástico Mundo dos Números: a matemática do zero ao infinito**. Tradução: George Schlensinger. Rio de Janeiro: Zahar, 2016.

SOBRE OS AUTORES

LUCIANO PAULO

LICENCIADO EM MATEMÁTICA PELO INSTITUTO FEDERAL DO RIO GRANDE DO NORTE. ATUALMENTE É PROFESSOR DE MATEMÁTICA DO MUNICÍPIO DE MONTE ALEGRE - RN.

ROBSON SOUSA

LICENCIADO EM MATEMÁTICA PELA UNIVERSIDADE ESTADUAL DA PARAÍBA E MESTRE EM MATEMÁTICA PURA PELA UNIVERSIDADE FEDERAL DA PARAÍBA. É PROFESSOR DE CÁLCULO E ÁLGEBRA DO INSTITUTO FEDERAL DO RIO GRANDE DO NORTE, CAMPUS NATAL CENTRAL DESDE 2009.

RESUMO

A CRIPTOGRAFIA É O PROCESSO QUE TEM A FINALIDADE DE CODIFICAR O CONTEÚDO DE MENSAGENS PARA QUE PESSOAS NÃO AUTORIZADAS NÃO TENHAM CONDIÇÕES DE INTERPRETAR O TEOR DO TEXTO. ESSE PROCEDIMENTO VEM SE DESENVOLVENDO AO LONGO DO TEMPO E SENDO RELEVANTE EM DIVERSOS MOMENTOS DA HISTÓRIA DA HUMANIDADE. ESTE TEXTO, ALÉM DE APRESENTAR UM BREVE RESUMO DA HISTÓRIA DA CRIPTOGRAFIA TRÁS ALGUNS MODELOS DE CRIPTO-SISTEMAS QUE SÃO DEFINIDOS ATRAVÉS DE FUNÇÕES, CUJO DOMÍNIO E O CONTRADOMÍNIO SÃO CONJUNTOS DE CLASSES DE CONGRUÊNCIA. COM ESSAS FUNÇÕES TEREMOS UM MODELO DE CRIPTOGRAFIA QUE EM SUA CONSTITUIÇÃO ESTÁ PRESENTE A ASSOCIAÇÃO ENTRE A CRIPTOGRAFIA E A TEORIA DOS NÚMEROS.

RFB Editora
CNPJ: 39.242.488/0001-07
91985661194
www.rfbeditora.com
adm@rfbeditora.com
Tv. Quintino Bocaiúva, 2301, Sala 713, Batista Campos,
Belém - PA, CEP: 66045-315

9 786558 897361 >

rfb editora