UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS FLORIANÓPOLIS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL-PROFMAT

Elídio Louzada Gomes Júnior

QUADRADOS LATINOS E CRIPTOGRAFIA

Florianópolis

2022

Elídio Louzada Gomes Júnior

QUADRADOS LATINOS E CRIPTOGRAFIA

Dissertação submetida ao Programa de Mestrado Profissional de Matemática em Rede Nacional - PROFMAT da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do Grau de Mestre em Matemática. Com área de concentração no Ensino de Matemática.
Orientadora: Prof^{a}. Dr^{a}. Maria Inez Cardoso Gonçalves.

Florianópolis

2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Gomes Júnior, Elídio
QUADRADOS LATINOS E CRIPTOGRAFIA / Elídio Gomes Júnior ; orientador, Maria Inez Cardoso Gonçalves, 2022.
95 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas, Programa de Pós-Graduação em Matemática, Florianópolis, 2022.

Inclui referências.

1. Matemática. 2. Quadrado latino. 3. Criptografia. 4. Cifra de Vigenère. I. Cardoso Gonçalves, Maria Inez. II. Universidade Federal de Santa Catarina. Programa de Pós Graduação em Matemática. III. Título.

Elídio Louzada Gomes Júnior

QUADRADOS LATINOS E CRIPTOGRAFIA

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Dr. Wagner Barbosa Muniz
UFSC

Prof. Dr. Eliezer Batista
UFSC

Prof. Dr. Sérgio Tadao Martins
UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Matemática.

Documento assinado digitalmente
Maria Inez Cardoso Goncalves
Data: 25/08/2022 16:02:51-0300
CPF: 908.897.119-68
Verifique as assinaturas em https://v.ufsc.br

Profª. Drª. Maria Inez Cardoso Gonçalves
Coordenadora do Programa

Documento assinado digitalmente
Maria Inez Cardoso Goncalves
Data: 25/08/2022 16:03:35-0300
CPF: 908.897.119-68
Verifique as assinaturas em https://v.ufsc.br

Profª. Drª. Maria Inez Cardoso Gonçalves.
Orientadora

Florianópolis, 25 de Agosto 2022.

Dedico este trabalho à minha esposa, minha filha e aos meus pais.

AGRADECIMENTOS

Em oração por estar aqui!

À minha família pelo companheirismo e pela paciência.

Aos meus pais, incansáveis no apoio que sempre me deram.

Aos meus irmãos, é bom ter vocês ao meu lado, sinto saudades.

Aos colegas do PROFMAT, Acmon, Alexsandro, Bruna, Carol, Giorgio, Jéssica, Leonardo, Luiz Felipe, Mayara, Virgínia e Tadeu.

Aos professores do Profmat e especialmente a minha orientadora Profª. Drª. Maria Inez Cardoso Gonçalves, pela deferência, dedicação, paciência e conselhos.

"Por uma questão de brevidade, nós sempre representaremos o número $2,718281828459\ldots$ *pela letra e".*

(Leonhard Paul Euler)

RESUMO

Qual a relação entre quadrados latinos e criptografia? Na presente dissertação investigaremos os quadrados latinos, mostrando alguns tipos, enfatizando suas características, especialmente aquelas interessantes e úteis à criptografia. Veremos como Leonhard Euler contribuiu para o estudo do conceito de quadrados latinos. Apresentamos também cifras baseadas em quadrados latinos (principalmente a Cifra de Vigenère) que se constituíram, durante séculos, em métodos seguros de proteção e privacidade de mensagens e dados confidenciais, sendo que atualmente a criptografia tornou-se uma das principais linhas de pesquisa da computação moderna e da matemática na proteção de comunicação de informação. Além de sugerirmos atividades inspiradas sobretudo em quadrados latinos.

Palavras-chave: Quadrado latino. Cifra de Vigenère. Criptografia.

ABSTRACT

What is the relationship between Latin squares and cryptography? In the present dissertation we will investigate Latin squares, showing some types, emphasizing their characteristics, especially those interesting and useful to cryptography. We will see how Leonhard Euler contributed to the study of the concept of Latin squares. We also present the ciphers based on Latin squares (mainly the Vigenère Cipher) that have been, for centuries. secure methods of protecting and privacy of confidencial messages and data, and currently cryptography has become one of the main lhes of research in computing modem technology and mathematics in the protection of information communication. In addition, we suggest activities inspired mainly by Latin squares.

Keywords: Latin square. Vigenere cipher. Cryptography.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Nesse trabalho, o objeto de estudo são os quadrados latinos e a sua aplicação na criptografia. Os tipos de cifras desenvolvidas no decorrer da história da criptografia, que apresentam características encontradas em quadrados latinos.

Os quadrados latinos, inicialmente, eram usados para jogos de quebra-cabeça, quadrados mágicos, amuletos ou ornamentos místicos. A partir dos estudos realizados por Leonhard Euler, no século XVIII. Descobriu-se que eram relevantes para campos como combinatória e álgebra. Mais recentemente, dentre as aplicações modernas dos quadrados latinos, estão pesquisas e aplicações em agricultura, geometria finita, estatística, planejamento de experimentos, telecomunicações, teoria dos códigos e criptografia. Alguns trabalhos, incluindo propostas didáticas, que elencamos a seguir:

- Cifrador simétrico de blocos: projeto e avaliação (LAMBERT, 2004).
- Princípios sobre delineamentos em experimentação agrícola (DUARTE, 1996).
- Quadrados Latinos com aplicações em engenharia de software (SáNCHEZ, 2011).
- Matemática e estatística na análise de experimentos e no melhoramento genético (RESENDE, 2007).
- Um modelo para o ensino de Controle Estatístico da Qualidade (REIS et al., 2001).
- Quadrados latinos e quadrados mágicos - uma proposta didática (FARIAS et al., 2017).

Na pesquisa de criptografia, vimos que esta foi usada como um instrumento para proteger segredos e estratégias de ações militares, de serviços diplomáticos e de governos em geral. Com a proliferação de computadores e sistemas de comunicação na década de 1960, ocorreu um rápido crescimento da demanda dos setores privados e públicos por meios para salvaguardar as informações em formato digital e fornecer serviços de segurança.

Para concatenar essas informações, primeiramente, selecionamos, para a materialização dessa dissertação, os seguintes livros: Combinatorics: Ancient & Modern de Robin Wilson e John Watkins (WILSON; WATKINS, 2013); Introduction to combinatorics de Walter Wallis e John George (WALLIS; GEORGE, 2016) e Latin squares and their applications de Donald Keedwell e József Dénes (KEEDWELL; DÉNES, 2015). A partir dessas leituras, no capítulo 2, serão abordados aspectos históricos dos quadrados latinos, seus conceitos básicos, suas principais características, a contribuição de Leonhard Euler para

a disseminação do seu estudo e aplicações em design experimental e códigos de correção de erros.

No terceiro capítulo, trataremos sobre criptografia, descrevendo seus conceitos básicos, relatando evidências históricas, com atenção especial para a Cifra de Vigenère e os aspectos criptográficos encontrados em livros de autores como Edgar Allan Poe (POE, 2012) e Arthur Conan Doyle (CROWE, 2018).

E no último capítulo, sugerimos atividades para sala de aula inspiradas sobretudo em quadrados latinos, tais como o quebra-cabeça KenKen, o jogo das dezesseis cartas de baralho, o Sudoku, quadrados mágicos e Erdös Latino.

2 QUADRADOS LATINOS

Neste capítulo, iniciamos com um curto relato histórico sobre os quadrados latinos, aludindo como se deu a contribuição de Euler para o desenvolvimento dos estudos relacionados aos quadrados latinos. Apresentamos a conjectura feita por Euler em 1782 sobre a existência de um certo tipo de quadrado latino, a qual motivou o estudo por parte de matemáticos como G. Tarry, E. T. Parker, R. C. Bose, S. S. Shrikhande, F. Yates e outros a descobrir a sua eventual resolução, cerca de um século depois. Depois, falaremos sobre os conceitos básicos, características e aplicações de quadrados latinos em design experimental e códigos de correção de erro.

Um **quadrado latino** é um arranjo de n símbolos em n linhas e n colunas, na forma de um tabuleiro de xadrez, de modo que cada símbolo apareça uma única vez em cada linha e uma única vez em cada coluna. Vemos, abaixo, um quadrado latino de ordem 4 (quatro linhas e quatro colunas, preenchido com as letras A, B, C e D).

A	B	C	D
B	C	D	A
C	D	A	B
D	A	B	C

2.1 ORIGEM

Antes do matemático Leonhard Euler se interessar por quadrados latinos e dar início ao desenvolvimento teórico do assunto em 1779, acredita-se que os quadrados latinos apareceram inicialmente em amuletos (Figura 1) e em ritos em certas comunidades árabes e indianas, possivelmente, a partir do ano 1000.

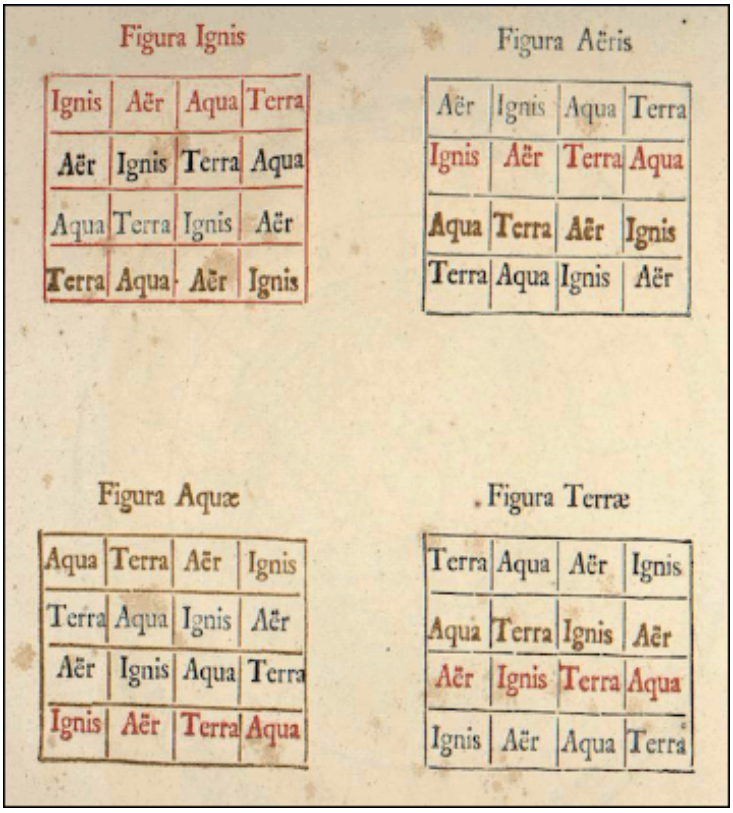
Como podemos ver em dois exemplos de publicações mediaveis nos quais aparecem quadrados latinos. O primeiro, trata-se do missionário catalão Ramon Llull (1232-1316) que fez um resumo sistemático de todos os ramos do conhecimento de seu tempo, baseado na arte combinatória. Entre seus desenhos há quatro tabelas, dos quatro elementos (água, ar, fogo e terra) ordenados como quadrados latinos (Figura 2).

E o segundo, aparece em um livro famoso, Shams al-Ma'arif al-Kubra (O Sol do Grande Conhecimento), que foi escrito no Egito no século XIII por um místico e mago sufi[1] de origem argelina, Ahmad Al-Buni (ou Shihab al-Din Ahmad ibn Ali ibn Yusuf

[1]Praticante ou estudante do Sufismo, conhecida como a corrente mística e contemplativa do Islã.

Fonte: https://exhibitions.kelsey.lsa.umich.edu/pearls/objects/teardrop.html, acesso em 05 jun. 2021

Figura 1: Um amuleto de prata de Damasco; na esquerda, os nomes dos sete dorminhocos de Éfeso (que, segundo a lenda, dormiram em uma caverna por duzentos anos a partir do ano 250) e à direita um **quadrado latino**.



Fonte: https://plato.stanford.edu/entries/llull/, acesso em 05 jun. 2022

Figura 2: Quadrados latinos desenhados por Ramon Llull.

al-Buni al-Maliki al-Amazighi, seu nome completo), que se acredita ter morrido em 1225. Este livro contém muitos quadrados latinos (além de muitos outros quadrados mágicos), incluindo o quadrado 5×5 na Figura 3, o primeiro quadrado latino do livro e possivelmente

o mais antigo quadrado latino conhecido, de acordo com (WILSON; WATKINS, 2013, p. 254).

Os quadrados latinos de al-Buni parecem servir a dois propósitos: primeiro, se acreditava que eles tinham certos poderes mágicos, alguns deles relacionados a um planeta específico; e em segundo lugar, eles parecem ser cruciais na *construção de quadrados mágicos*. De fato, há fortes evidências de que al-Buni e outros autores árabes antigos conheciam métodos para isso, que foram posteriormente adotados por matemáticos do século XVIII, entre eles Leonhard Euler.

فلان	الرحيم	الرحمن	الله	بسم
بسم	فلان	الرحيم	الرحمن	الله
الله	بسم	فلان	الرحيم	الرحمن
الرحمن	الله	بسم	فلان	الرحيم
الرحيم	الرحمن	الله	بسم	فلان

Fonte: (WILSON; WATKINS, 2013).

Figura 3: Possivelmente o mais antigo quadrado latino conhecido.

Não se sabe ao certo a origem do conceito de quadrados latinos, no entanto (WILSON; WATKINS, 2013, p. 255) diz que eles também aparecem em um antigo problema com cartas de um baralho (Figura 4), o qual consiste em distribuir as dezesseis cartas figuradas (ás, rei, dama, valete) em um arranjo 4×4 de modo que cada linha, cada coluna e cada diagonal contenha um ás, um rei, uma rainha e um valete, todos de naipes diferentes; assim, tanto os naipes quanto as figuras formem, isoladamente, quadrados latinos.

2.1.1 A contribuição de Euler.

Apesar dos quadrados latinos terem aparecido ao longo dos anos em amuletos, livros e problemas, como vimos anteriormente, acredita-se que a sua definição matemática formal, bem como a sua nomenclatura, foram introduzidas somente no final do século XVIII, pelo matemático suíço Leonhard Paul Euler. Em 1782, quando tinha 75 anos, Euler publicou um artigo sobre um novo tipo de quadrado mágico intitulado: *"Recherches sur une nouvelle espèce de quarres magiques"* (Investigações sobre um novo tipo de quadrados

Fonte: (WILSON; WATKINS, 2013).

Figura 4: Arranjo 4×4 com dezesseis cartas figuradas de um baralho.

mágicos) (EULER, 1782). Ele iniciou o artigo apresentando o problema que o motivou a desenvolver seus estudos. Abaixo apresentamos a tradução do texto escrito por Euler.

"Uma questão muito curiosa, que durante algum tempo exigiu a sagacidade de muitas pessoas, induziu-me a realizar as seguintes pesquisas, que parecem abrir uma nova carreira em Análise e em particular na área de combinatória. Esta questão diz respeito a um grupo de 36 oficiais de 6 patentes diferentes, oriundos de 6 regimentos diferentes, que deveriam ser dispostos num quadrado de modo que em cada linha e em cada coluna, haja seis oficiais, cada um de uma patente e de um regimento diferente, mas, depois de muito esforço para resolver este problema, fomos obrigados a reconhecer que tal arranjo é absolutamente impossível, embora não possamos dar uma prova rigorosa."

Euler mostrou que o problema dos n^2 oficiais pode ser resolvido se n for um número natural ímpar ou se n for um número natural divisível por 4. Ele também mostrou que não existe solução para $n = 2$. Sem conseguir obter uma demonstração para os demais casos, Euler conjecturou, como em (WILSON; WATKINS, 2013, p. 264), que para $n = 4k+2$, com $k \in \mathbb{N}$, o problema não possuia solução.

Conjectura 2.1. *Não existe par de quadrados latinos ortogonais de lado n, para $n = 4k + 2$, com $k \in \mathbb{N}$.*

Para tentar resolver o problema, Euler se esforçava para encontrar dois quadrados latinos de mesma ordem, mas com símbolos diferentes, de tal maneira que, quando so-

brepostos formassem um novo quadrado mágico especial (com entradas, combinação de símbolos, únicas entre si), também chamado de quadrado greco-latino ou quadrado de Euler. Quadrados latinos com essa característica são chamados de ortogonais (ver Definição 2.2.3). Se no problema fossem "4" ao invés de "6" oficiais, uma possível solução seria o modelo da Figura 4.

Abaixo, conforme (WILSON; WATKINS, 2013, p. 259), vemos a representação do primeiro quadrado latino a receber este nome. Neste quadrado, cada número de 1 a 7 ocorre exatamente uma vez em cada linha e em cada coluna, tanto na base como no expoente, e cada par ordenado ocorre exatamente uma vez. Referindo-se ao seu uso anterior de letras latinas e gregas, Euler usava dois quadrados, escrevia letras latinas em um quadrado e letras gregas no outro (como na Tabela 10 na página 32).

1^1	2^6	3^4	4^3	5^7	6^5	7^2
2^2	3^7	1^5	5^4	4^1	7^6	6^3
3^3	6^1	5^6	7^5	1^2	4^7	2^4
4^4	5^2	6^7	1^6	7^3	2^1	3^5
5^5	1^3	7^1	2^7	6^4	3^2	4^6
6^6	7^4	4^2	3^1	2^5	5^3	1^7
7^7	4^5	2^3	6^2	3^6	1^4	5^1

Fonte: (WILSON; WATKINS, 2013).

Tabela 1: Primeiro quadrado latino a receber esse nome.

Na Tabela 1, o quadrado contém dois quadrados latinos ortogonais de ordem 7 (o quadrado latino formado pelas bases e o outro pelos expoentes), mostrando que Euler poderia resolver um problema idêntico àquele dos trinta e seis oficiais, caso tivesse quarenta e nove oficiais. Da mesma forma, o problema das cartas, na Figura 4, pede dois quadrados latinos ortogonais de ordem 4, e a solução apresentada mostra que tais quadrados latinos ortogonais existem.

Em (WILSON; WATKINS, 2013, p. 264), vemos que um século depois, o matemático francês Gaston Tarry (TARRY, 1900)), após análise exaustiva, provou que nenhuma solução era possível no caso do problema dos 36 oficiais, ou seja, quando $n = 6$. E quase 60 anos mais tarde, em 1959, os matemáticos Ernest Tilden Parker, Raj Chandra Bose e Sharadchandra Shankar Shrikhande, (BOSE; SHRIKHANDE, 1959), provaram a existência de quadrados latinos ortogonais de ordens $10, 14, 18, \ldots$, ou seja, $n = 4k + 2$, com $k > 1$ (ver Tabela 2), estabelecendo que a conjectura de Euler era equivocada.

No início do capítulo, trouxemos uma ideia do que seria um quadrado latino, no entanto para prosseguirmos com o trabalho, precisamos apresentar as definições de quadrado latino; de quadrado latino reduzido, para calcularmos o total de quadrados

00	47	18	76	29	93	85	34	61	52
86	11	57	28	70	39	94	45	02	63
95	80	22	67	38	71	49	56	13	04
59	96	81	33	07	48	72	60	24	15
73	69	90	82	44	17	58	01	35	26
68	74	09	91	83	55	27	12	46	30
37	08	75	19	92	84	66	23	50	41
14	25	36	40	51	62	03	77	88	99
21	32	43	54	65	06	10	89	97	78
42	53	64	05	16	20	31	98	79	87

Fonte: (FRISINGER, 1981, 59).

Tabela 2: Exemplo de par de quadrados latinos ortogonais de ordem 10.

latinos de ordem n; de quadrados latinos mutuamente ortogonais, para construções de quadrados mágicos, por exemplo, como Euler e autores árabes antigos fizeram e o Teorema da existência de quadrado latino para todo número natural n.

2.2 QUADRADOS LATINOS.

Definição 2.2.1 (Quadrado latino)**.** *Um quadrado latino de ordem n é uma matriz $n \times n$ baseada em algum conjunto S de n símbolos (ou letras, ou números), com a propriedade de que cada linha e cada coluna contém cada símbolo exatamente uma vez. Em outras palavras, cada linha e cada coluna é uma permutação de S.*

Abaixo, temos exemplos de quadrados latinos de ordens 3, 4 e 5, respectivamente.

ρ	σ	τ
σ	τ	ρ
τ	ρ	σ

Fonte: Elaborado pelo autor.

Tabela 3: Quadrado latino de ordem 3.

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Fonte: Elaborado pelo autor.

Tabela 4: Quadrado latino de ordem 4.

A	B	C	D	E
B	C	D	E	A
C	D	E	A	B
D	E	A	B	C
E	A	B	C	D

Fonte: Elaborado pelo autor.

Tabela 5: Quadrado latino reduzido de ordem 5.

Corolário 2.0.1. *[Existência de quadrado latino] Para todo número natural n, existe pelo menos um quadrado de ordem (ou tamanho) n.*

Demonstração. Para provar o teorema, consideremos que a primeira linha de um quadrado $n \times n$ seja formada pelos os números naturais $1, 2, 3, \ldots, n-2, n-1, n$. Na segunda linha, permutamos estes números uma posição à esquerda, de modo que a segunda linha seja escrita como $2, 3, 4, \ldots, n-1, n, 1$.

Procedendo desse modo em todas as linhas; na linha $n-1$, vamos obter $n-1, n, 1, \ldots, n-4, n-3, n-2$. E na n-ésima linha, $n, 1, 2 \ldots, n-3, n-2, n-1$. Formando um quadrado latino de ordem n, conforme a Figura abaixo.

1	2	3	$\ldots$	$n-2$	$n-1$	n
2	3	4	$\ldots$	$n-1$	n	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	n	1	$\ldots$	$n-4$	$n-3$	$n-2$
n	1	2	$\ldots$	$n-3$	$n-2$	$n-1$

□

Uma questão que podemos avaliar é se para todo n natural existe um quadrado latino de ordem n, quantos quadrados distintos existem para cada ordem? Verificamos que um grupo de matemáticos contribuiu para responder esse questionamento e mostramos isso na Tabela 6, porém é necessário que introduzamos a definição de quadrado reduzido e qual a sua relevância para calcular a quantidade de quadrados latinos distintos por ordem.

Definição 2.2.2 (Quadrado latino reduzido, normalizado ou padrão)**.** *Um quadrado latino de ordem N é dito reduzido, normalizado ou padrão, se as letras estiverem dispostas em ordem alfabética na primeira linha e na primeira coluna, ou se os seus números estiverem em ordem crescente na primeira linha e na primeira coluna.*

Corolário 2.0.2. *qualquer quadrado latino pode ter suas linhas e colunas reorganizadas e o resultado também será um quadrado latino. Ou seja, qualquer quadrado latino pode ser reestruturado em uma "forma padrão", como um quadrado latino reduzido.*

Nas Tabelas 3, 4 e 5 temos exemplos de quadrados latinos reduzidos.

E é possível especular que existam muitos quadrados latinos distintos de ordem n, no entanto para determinar isto, vamos, inicialmente, denotar por $\boldsymbol{QL_n}$ o número de quadrados latinos distintos de ordem n e por $\boldsymbol{l_n}$ a quantidade total de quadrados latinos reduzidos de ordem n.

Teorema 2.1. *Para todo $n \geq 2$, o total de quadrados latinos de ordem n, é dado por*

$$QL_n = l_n \cdot n!(n-1)!.$$

Demonstração. Dado um quadrado latino de ordem n. As colunas podem permutadas de $n!$ modos distintos, ainda assim, cada uma das permutações mantem a matriz $n \times n$ como um quadrado latino, distintos entre si. Fixamos a primeira linha obedecendo a ordem $1, 2, 3, \ldots, n$. De maneira análoga, após permutar as colunas, permutaremos as $(n-1)$ linhas de $(n-1)$ maneiras. Novamente, cada uma das matrizes $n \times n$ são quadrados latinos, distintos entre si e ainda cada quadrado latino desses será distinto dos anteriores gerados nas permutações das linhas, pois lembremos que a primeira linha está fixa. Então, iniciando com um quadrado latino reduzido de ordem n, a permutação das $(n-1)$ linhas e das $n!$ colunas produz exatamente $n!\cdot(n-1)!$ quadrados latinos de ordem n e, precisamente, um desses quadrados latinos é reduzido, pois no Corolário 2.0.1 é dito que existe pelo menos um quadrado latino de ordem n, com n natural e como qualquer quadrado latino pode ser reestruturado como um quadrado latino reduzido, segue o resultado. □

Neste momento, temos outra questão, para obtermos o número QL_n, precisamos calcular o valor de l_n. E como determinamos quantos quadrados latinos reduzidos ou normalizados existem? A resposta não é simples, pois não foi estabelecida uma fórmula para o cálculo de l_n. De (KEEDWELL; DÉNES, 2015), (FARIAS et al., 2017, p. 10) e (MORGADO, 2012, p. 4), vemos que muitos matemáticos contribuíram para se estabelecer alguns valores, por isso para encadear esses dados de modo conciso, organizamos uma tabela que mostra as descobertas das quantidades de quadrados reduzidos (l_n) por ordem (n) e pelos seus respectivos autores.

Atualmente, para cada ordem n são conhecidos somente valores exatos de l_n (conforme Tabela 6) para $2 \leq n \leq 11$, pois para $12 \leq n \leq 15$ existem estimativas obtidas através de métodos computacionais.

Definição 2.2.3 (Quadrados latinos mutuamente ortogonais)**.** *Se existirem dois quadrados latinos que, quando sobrepostos, apresentam coordenadas totalmente diferentes (ou seja, todas as coordenadas possíveis ocorrem exatamente uma vez), eles são chamados*

n	l_n	Autor
2	1	
3	1	
4	4	
5	56	Euler (1782); Cayley (1890); McMahon (1915).
6	9408	Frolov (1890); Tarry (1900).
7	16942080	Frolov (1890); Norton (1939); Sade (1948); Saxena (1951).
8	535281401856	Wells (1967).
9	377597570964258816	Bammel e Rothstein (1975).
10	75807214831601338114892800	Mckay e Rogoyski (1995).
11	536393777327737129811967354077184 0	Mckay e Wanless (2005).
12	$1,62 \cdot 10^{44}$	Mckay e Rogoyski (1995).
13	$2,52 \cdot 10^{56}$	Mckay e Rogoyski (1995).
14	$2,53 \cdot 10^{70}$	Mckay e Rogoyski (1995).
15	$1,56 \cdot 10^{86}$	Mckay e Rogoyski (1995).

Fonte: (FARIAS et al., 2017, p. 10).

Tabela 6: Valores de quadrados latinos reduzidos e seus respectivos autores.

de quadrados latinos mutuamente ortogonais, ou pela sigla em inglês MOLS (Mutually Orthogonal Latin Squares).

Observação*: "Uma contribuição importante de Euler para o progresso da teoria algébrica dos quadrados latinos, foi a definição de quadrados latinos ortogonais", segundo (SANTOS et al., 2018, p. 46).*

Nos exemplos de quadrados latinos que veremos a seguir, denotamos por $\wedge$, a operação de sobreposição[2] das entradas de dois quadrados latinos $n \times n$ (MOLS) formando um terceiro quadrado (ou seja, um quadrado greco-latino ou quadrado de Euler) com as n^2 entradas distintas entre si.

Exemplo 2.2.1. *Sejam os quadrados latinos QL_1 e QL_2 de ordem 4 conforme mostrado na Tabela 7.*

O conceito de ortogonalidade mútua pode se estender a um conjunto de mais de dois quadrados, sendo cada quadrado mutuamente ortogonal entre si. A **Tabela 8**, resultado da sobreposição dos quadrados QL_1 e QL_2, serviu de modelo para montar o arranjo da **Figura 4**. E na Tabela 9, elaboramos uma representação de dois quadrados mutuamente ortogonais de ordem 4 na construção de um "quadrado de Euler" 4×4.

[2]Sobreposição, neste contexto, é o efeito de colocar um símbolo (letra ou número) ao lado de outro símbolo (letra ou número) na mesma coordenada (ou entrada) de um quadrado de Euler.

$$QL_1 = \begin{array}{|c|c|c|c|}\hline \heartsuit & \clubsuit & \diamondsuit & \spadesuit \\ \hline \clubsuit & \heartsuit & \spadesuit & \diamondsuit \\ \hline \diamondsuit & \spadesuit & \heartsuit & \clubsuit \\ \hline \spadesuit & \diamondsuit & \clubsuit & \heartsuit \\ \hline \end{array} \quad \text{e} \quad QL_2 = \begin{array}{|c|c|c|c|}\hline \alpha & \beta & \gamma & \delta \\ \hline \delta & \gamma & \beta & \alpha \\ \hline \beta & \alpha & \delta & \gamma \\ \hline \gamma & \delta & \alpha & \beta \\ \hline \end{array}$$

Fonte: Elaborado pelo autor.

Tabela 7: Quadrados latinos mutuamente ortogonais (**MOLS**).

$$QLO = QL_1 \wedge QL_2 = \begin{array}{|c|c|c|c|}\hline \heartsuit\,\alpha & \clubsuit\,\beta & \diamondsuit\,\gamma & \spadesuit\,\delta \\ \hline \clubsuit\,\delta & \heartsuit\,\gamma & \spadesuit\,\beta & \diamondsuit\,\alpha \\ \hline \diamondsuit\,\beta & \spadesuit\,\alpha & \heartsuit\,\delta & \clubsuit\,\gamma \\ \hline \spadesuit\,\gamma & \diamondsuit\,\delta & \clubsuit\,\alpha & \heartsuit\,\beta \\ \hline \end{array}$$

Fonte: Elaborado pelo autor.

Tabela 8: Quadrado greco-latino ou quadrado de Euler formado por MOLS.

$$\begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline \end{array} \wedge \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 3 & 2 & 1 & 0 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 00 & 11 & 22 & 33 \\ \hline 13 & 02 & 31 & 20 \\ \hline 21 & 30 & 03 & 12 \\ \hline 32 & 23 & 10 & 01 \\ \hline \end{array}$$

Fonte: Elaborado pelo autor.

Tabela 9: Exemplo numérico de dois quadrados latinos mutuamente ortogonais 4×4.

$$Q_L = \begin{array}{|c|c|c|c|c|}\hline \text{a} & \text{b} & \text{c} & \text{d} & \text{e} \\ \hline \text{b} & \text{c} & \text{d} & \text{e} & \text{a} \\ \hline \text{c} & \text{d} & \text{e} & \text{a} & \text{b} \\ \hline \text{d} & \text{e} & \text{a} & \text{b} & \text{c} \\ \hline \text{e} & \text{a} & \text{b} & \text{c} & \text{d} \\ \hline \end{array} \wedge Q_G = \begin{array}{|c|c|c|c|c|}\hline \epsilon & \delta & \gamma & \beta & \alpha \\ \hline \alpha & \epsilon & \delta & \gamma & \beta \\ \hline \beta & \alpha & \epsilon & \delta & \gamma \\ \hline \gamma & \beta & \alpha & \epsilon & \delta \\ \hline \delta & \gamma & \beta & \alpha & \epsilon \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|}\hline \text{a}\,\epsilon & \text{b}\,\delta & \text{c}\,\gamma & \text{d}\,\beta & \text{e}\,\alpha \\ \hline \text{b}\,\alpha & \text{c}\,\epsilon & \text{d}\,\delta & \text{e}\,\gamma & \text{a}\,\beta \\ \hline \text{c}\,\beta & \text{d}\,\alpha & \text{e}\,\epsilon & \text{a}\,\delta & \text{b}\,\gamma \\ \hline \text{d}\,\gamma & \text{e}\,\beta & \text{a}\,\alpha & \text{b}\,\epsilon & \text{c}\,\delta \\ \hline \text{e}\,\delta & \text{a}\,\gamma & \text{b}\,\beta & \text{c}\,\alpha & \text{d}\,\epsilon \\ \hline \end{array}$$

Fonte: Elaborado pelo autor.

Tabela 10: Quadrados latinos mutuamente ortogonais 5×5.

Na Tabela 10 mostramos a construção de um quadrado de Euler 5×5 a partir de dois quadrados latinos mutuamente ortogonais de ordem 5. Para isso, denotamos Q_L um quadrado com letras latinas e Q_G um quadrado com letras gregas. E aqui podemos notar nas Tabelas 9 e 10 que todas as entradas (ou coordenadas) dos quadrados resultantes são distintas.

No decorrer do trabalho, mencionaremos algumas áreas de aplicações da teoria dos quadrados latinos, por exemplo, combinatória, álgebra, geometria finita, engenharia de software, controle estatístico da qualidade e criptografia. Na próxima subseção nos limitaremos a relatar sobre as seguintes aplicações: design de experimentos e teoria dos

códigos, em particular em códigos de correção de erros. No entanto, antes de continuarmos vejamos através de (ARANDA; JUNG; CATEN, 2008, p. 119) o que é design de experimentos ou planejamento de experimentos, cujo pioneiro foi Ronald Fisher.

> O Planejamento de Experimentos (Design of Experiments, DOE) é uma técnica utilizada para se planejar experimentos, ou seja, para definir quais dados, em que quantidade e em que condições devem ser coletadas durante um determinado experimento, buscando, basicamente, satisfazer dois grandes objetivos: a precisão estatística possível na resposta e o menor custo. Atualmente, essa técnica vem sendo utilizada em grande escala.

2.2.1 Aplicações de quadrados latinos

2.2.1.1 **Design experimental.**

Ronald Aylmer Fisher (1890-1962), estatístico e geneticista britânico, foi pioneiro na aplicação de procedimentos estatísticos ao projeto de experimentos científicos. Em 1925 dedicou a última seção da primeira edição de seus "Métodos estatísticos para pesquisadores" (Statistical Methods for Research Workers (FISHER, 1958) ao uso de quadrados latinos em experimentos de campo, de acordo com (DéNES; KEEDWELL, 1991, p. 323). Ainda conforme (FRISINGER, 1981, p. 57), a partir de 1926, Fisher estudou esses quadrados e os aplicou ao projeto de experimentos de campo na agricultura. Os princípios de experimentação introduzidos por ele encontraram, a posteriori, um amplo campo de aplicação em áreas como biologia, medicina e indústria.

Além disso, Fisher e Frank Yates, (FISHER; YATES et al., 1934), enumeraram todos os **quadrados latinos de ordem 6** para verificar se não havia pares ortogonais dessa ordem e, em 1938, eles forneceram tabelas de pares de quadrados latinos ortogonais de ordens 3 a 12 (exceto 6 e 10, com um par de ordem 10 incluído em edições posteriores), bem como conjuntos completos de MOLS de ordem 3, 4, 5, 7, 8 e 9. Raj Chandra Bose (Subseção 2.1.1) escreveu que o trabalho de Fisher e Yates mostrou que tais quadrados são de fundamental importância no projeto experimental, como ilustramos a seguir.

Exemplo 2.2.2. *De acordo com (RIBEIRO; CATEN, 2001, p. 62), "a vantagem do Quadrado Latino é que se trata de um experimento que exige poucos ensaios, e isso representa economia de tempo e dinheiro".*

E para que tenhamos um exemplo simplificado e semelhante aos experimentos agrícolas com quadrados latinos de Ronald Fisher, suponhamos que queremos determinar a eficiência de cinco fertilizantes diferentes (F_1, F_2, F_3, F_4, F_5) sobre o desenvolvimento de um tipo de lavoura. Para isso, um terreno é dividido em um arranjo de 5×5 porções de terra (sendo que, nem o terreno e nem as porções precisam ser, necessariamente, quadradas). E considerando apenas os fertilizantes, um arranjo como um Quadrado Latino pode ser usado para inibir os efeitos de algum gradiente[3] *natural que exista no terreno. Segundo (RIBEIRO; CATEN, 2001, p. 62), esses efeitos poderiam ser virtualmente eliminados usando o planejamento na Tabela 11:*

Exemplo 2.2.3. *Neste exemplo podemos utilizar um arranjo do tipo Quadrado Greco-*

[3]Conjunto de variáveis ambientais encontradas no solo, como umidade, acidez, composição química, nutrientes e etc.

Tabela de aplicação de fertilizantes					
	Coluna 1	Coluna 2	Coluna 3	Coluna 4	Coluna 5
Linha 1	F_1	F_3	F_5	F_2	F_4
Linha 2	F_2	F_4	F_1	F_3	F_5
Linha 3	F_3	F_5	F_2	F_4	F_1
Linha 4	F_4	F_1	F_3	F_5	F_2
Linha 5	F_5	F_2	F_4	F_1	F_3

Fonte: Baseado em (RIBEIRO; CATEN, 2001, p. 62).

Tabela 11: Tabela de aplicação de fertilizantes em um arranjo de 5×5.

Latino[4] *para avaliar o ganho em um processo químico. Selecionamos como os principais fatores a concentração de ácido (1, 2, 3, 4, 5), a concentração de catalisador (α, β, γ, δ, ϵ) e o tempo de espera (A, B, C, D, E). Para executar os ensaios planejados, são usados cinco lotes de matéria prima (I, II, III, IV, V). O experimento foi realizado conforme um arranjo do tipo Quadrado Greco-Latino* 5×5 *e os resultados são mostrados na Tabela 12:*

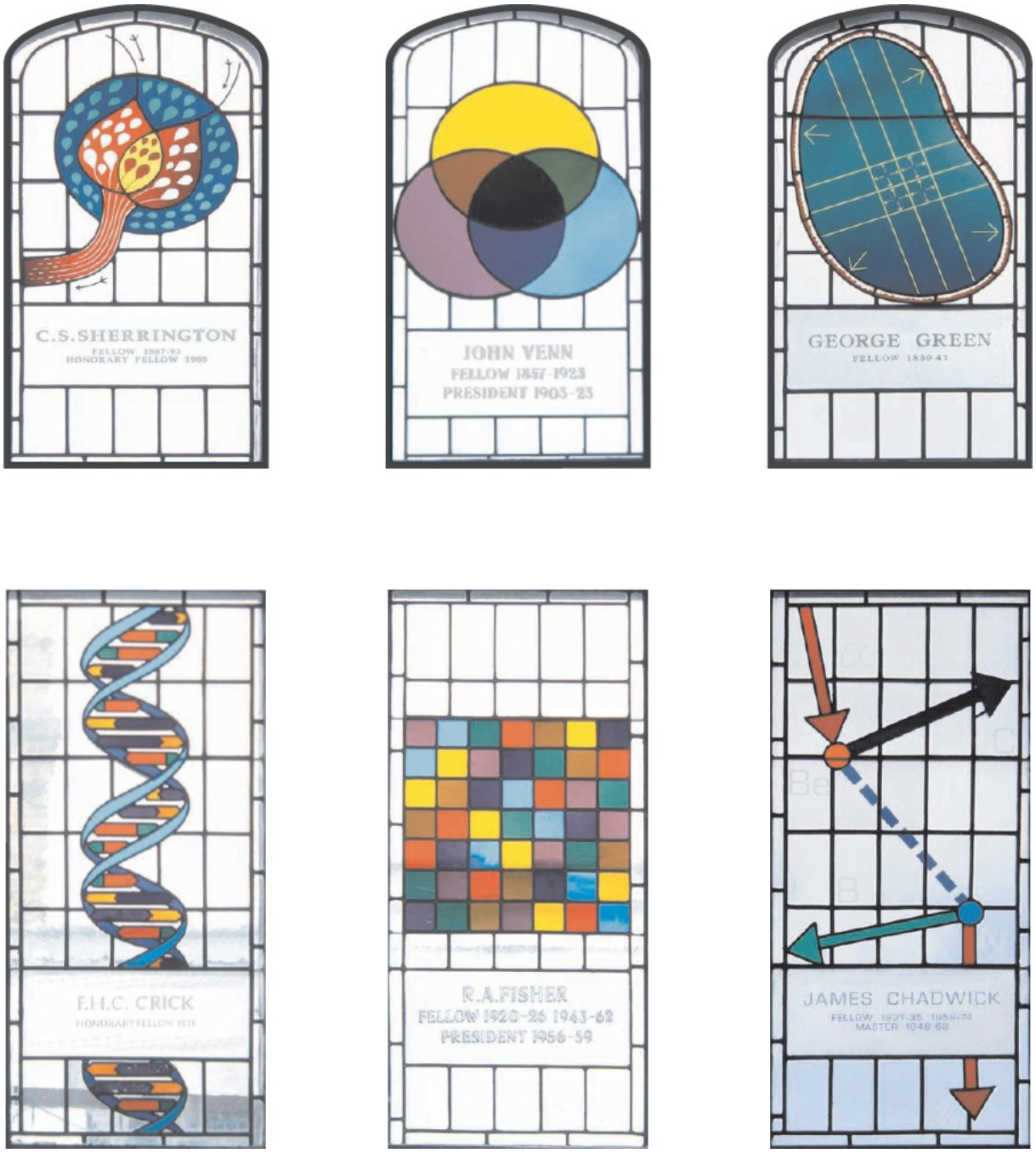
Tabela de concentração de ácidos					
	1	2	3	4	5
Lote I	A ϵ	B δ	C γ	D β	E α
Lote II	B α	C ϵ	D δ	E γ	A β
Lote III	C β	D α	E ϵ	A δ	B γ
Lote IV	D γ	E β	A α	B ϵ	C δ
Lote V	E δ	A γ	B β	C α	D ϵ

Fonte: Baseado em (RIBEIRO; CATEN, 2001, p. 63).

Tabela 12: Tabela de concentração de ácido em um arranjo de 5×5.

Em homenagem a R. A. Fisher, em 1989, o Gonville and Caius College, em Cambridge, Inglaterra, instalou em uma janela um vitral representando um quadrado latino de ordem 7 (Figura 5), apresentado no livro "The Design of Experiments"(FISHER, 1936), no qual foi escrito um capítulo dedicado aos quadrados latinos.

[4]Para obter um quadrado greco-latino ou quadrado de Euler é preciso a sobreposição de dois MOLS.



Fonte: https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2006.00203.x, acesso em 22 dez. 2021

Figura 5: Vitral no Gonville and Caius College (University of Cambridge) que representa o trabalho de Charles Sherrington, John Venn e George Green (linha superior); e a dupla hélice de DNA de Watson-Crick, o colorido **quadrado latino** 7×7 de Ronald Aylmer Fisher e as partículas subatômicas de James Chadwick (linha inferior).

2.2.1.2 **Códigos de correção de erros.**

Quando falamos em Teoria de Códigos, um dos problemas principais que vem à tona é a existência de erros ao transmitir informações e esse fato pode interferir na confiabilidade dos dados. Atualmente, quando digitamos algo em algum processador de texto, nos deparamos com um recurso chamado corretor ortográfico. Sua funcionalidade consiste em fornecer ao usuário do programa uma lista de sugestões de palavras, de um dicionário interno, que busca as correspondências de vocábulos mais próximos às letras correspondentes da palavra incorreta. Analogamente isso ocorre com a revisão de códigos. Há uma lista predefinida de "palavras de código" permitidas. Se o escritor de código digitar incorretamente uma sequência de caracteres, o programa encontrará a correspondência mais próxima da lista de palavras de código e corrigirá o erro automaticamente. Abaixo, focaremos mais na existência de tais códigos do que em como eles funcionam.

Definição 2.2.4. *Um código q-ário* $(n; M; d)$ **C** *é um conjunto de* M *palavras-código retiradas de um conjunto de* q *elementos, onde cada palavra-código tem comprimento* n *e distância mínima* d*.*

Observação 1. *A distância mínima* ***d*** *de um código q-ário é dada, grosso modo, pela quantidade mínima de caracteres ou símbolos entre as suas palavras-código.*

Observação 2. *O comprimento* ***n*** *em um código q-ário é definido pela quantidade fixa de caracteres ou símbolos de suas palavras-código.*

Exemplo 2.2.4. *Um* ***código ternário*** *(3-ário) (4; 9; 3) é um código com 9 palavras-código, cada uma com 4 letras, retiradas do alfabeto* $\{0, 1, 2\}$ *e com cada palavra diferindo entre si em pelo menos 3 lugares (ver Exemplo 2.2.5 idêntico apresentado para o Teorema 2.2).*

Teorema 2.2. *Existe um código q-ário* $(4; q^2; 3)$ *se e somente se existe um par de MOLS de ordem* q*.*

Demonstração. Seja C um código, com palavras-código $\{I; J; A_{ij}; B_{ij}\}$, onde os valores vêm de dois MOLS[5] A e B de ordem q, onde I é o número da linha, J é o número da coluna, A_{ij} é a entrada na linha i e coluna j do quadrado A, e da mesma forma para B_{ij} no quadrado B. Para quaisquer duas palavras de código, apenas uma coordenada pode ser a mesma. Primeiro provamos que a existência de MOLS implica a existência de um código: Suponha que exista um par de MOLS de ordem q. Então, se dois valores de I são

[5]Mutually Orthogonal Latin Squares ou quadrados latinos mutuamente ortogonais.

iguais, então J é diferente (caso contrário, eles formariam a mesma palavra de código). Quaisquer dois valores de A_{ij} são diferentes, porque é um quadrado latino e não pode haver duas entradas na mesma linha com o mesmo valor. O mesmo raciocínio se aplica a B_{ij}.

Um argumento simétrico se aplica ao valor J, referente às colunas. A única coisa que resta a considerar é se os valores de A_{ij} e B_{ij} são os mesmos em duas palavras de código. Se os valores de A_{ij} são os mesmos, então esses dois valores são duas entradas de uma transversal de B_{ij} e, portanto, os valores de B_{ij} são diferentes. Por outro lado, agora assumimos que existe um código e mostramos que os MOLS existem: Construa dois quadrados usando o código. Haverá entradas q^2. O fato de que todas as coordenadas $(I; A_{ij})$ e $(J; A_{ij})$ são diferentes prova que A é um quadrado latino, e similarmente com $(I; B_{ij})$ e $(J; B_{ij})$ com B. Como cada par de coordenadas $(A_{ij}; B_{ij})$ são diferentes, A e B são MOLS. □

Exemplo 2.2.5. *Este exemplo serve para ilustrar a ideia da demonstração do Teorema 2.2. Então, primeiramente, vamos considerar A e B, dois* ***MOLS de ordem 3****, e a seguinte construção:*

$$A = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 1 & 2 & 0 \\ \hline 2 & 0 & 1 \\ \hline \end{array} \quad e \quad B = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 2 & 0 & 1 \\ \hline 1 & 2 & 0 \\ \hline \end{array}$$

Localização (i, j)	A	B		Palavras-código
$(0, 0)$	0	0		0000
$(0, 1)$	1	1		0111
$(0, 2)$	2	2		0222
$(1, 0)$	1	2		1012
$(1, 1)$	2	0	$\longrightarrow$	1120
$(1, 2)$	0	1		1201
$(2, 0)$	2	1		2021
$(2, 1)$	0	2		2102
$(2, 2)$	1	0		2210

Fonte: (TANG, 2009, p. 7).

Tabela 13: Exemplo de aplicação de quadrados latinos em códigos.

Conforme (TANG, 2009, p. 7), devemos criar uma lista de todas as localizações de células 3^2 possíveis em uma matriz 3×3, essas localizações são representadas nas i linhas e nas j colunas da matriz. Para cada localização, anote-se o símbolo correspondente no quadrado A e o símbolo correspondente no quadrado B: isso cria a primeira tabela. Se

compactarmos os números dessas colunas juntos, obtemos a sequência de palavras-código na tabela à direita (Tabela 13).

Observe que esta tabela de palavras-código tem a seguinte propriedade: se você receber dois dos quatro dígitos de uma palavra-código, poderá determinar exclusivamente com qual palavra-código você começou. Para ver isso, basta observar que conhecer a linha junto com a coluna, A ou B determina exclusivamente de qual célula estamos falando (por causa da propriedade latina de A e B) e, portanto, determina exclusivamente o restante dos valores. Da mesma forma, conhecer a coluna e qualquer outra posição também determina exclusivamente a célula que estamos estudando e, portanto, a palavra-chave.

Finalmente, se você conhece A e B, você conhece todos os outros valores, porque este é um par de quadrados latinos mutuamente ortogonais e, desse modo (porque cada par de símbolos aparece exatamente uma vez) há uma única célula correspondente a esse par de símbolos. Por conseguinte, como o conhecimento de quaisquer dois símbolos determina uma palavra de forma única, duas palavras não têm dois locais em comum; portanto, a distância entre quaisquer duas palavras é de pelo menos 3. Logo, a distância $d(C)$ para este código é 3. É feito de palavras de base 3, de comprimento 4 e contém 9 palavras; e isto é exatamente o que estamos procurando no caso de $q = 3$.

Segundo (DéNES; KEEDWELL, 1991, p. 267), os códigos de correção de erros são aqueles usados para comunicações de mensagens, nos quais as mensagens serão codificadas em formato digital para transmissão e também poderão ser cifradas para torná-las ininteligíveis para interceptadores não autorizados. Em todo caso, a mensagem deve ser decodificada na extremidade receptora e quaisquer erros de transmissão detectados, se possível, corrigidos. Em decorrência desse fato, geralmente será utilizado um código de detecção e correção de erros.

Por exemplo, em um sistema de telefonia móvel, a área a ser coberta será dividida em regiões menores, cada uma atendida por um transmissor local. Se dois transmissores desses irradiarem a mesma frequência, pode ocorrer interferência e isso acarreta uma forma adicional de ruído que deve ser evitado, sempre que possível.

Em (DéNES; KEEDWELL, 1991, 268) vemos que na resolução de problemas de codificação, decodificação e interferência de transmissão, na década de 1940, quando a teoria da informação era uma ideia inteiramente nova, os pioneiros viam os **quadrados latinos** como uma importante ferramenta na construção de códigos com boas características. Posteriormente, quando os computadores digitais eletrônicos se difundiram e quando, na maioria das vezes, apenas códigos binários foram usados, o importante papel que os quadrados latinos poderiam desempenhar tende a ser esquecido, porque os pioneiros os usaram principalmente para a construção de códigos não binários.

A teoria dos quadrados latinos também é aplicada na criptografia como veremos no próximo capítulo, no qual inicialmente, esclarecemos que a criptografia era conhecida como uma arte e só recentemente passou a ser considerada uma ciência. Veremos quais são os seus conceitos básicos, os tipos de cifras, com destaque para a cifra de Vigenère. Depois apresentamos algumas evidências históricas do uso da criptografia, inclusive na literatura, em livros de Alan Poe e Conan Doyle e na escultura Kryptos.

3 CRIPTOGRAFIA

> Uma cifra deve ser fácil de usar; difícil de decifrar; e, se possível, livre de suspeitas.
>
> Francis Bacon

3.1 CRIPTOGRAFIA

Quando se desejava remeter alguma mensagem confidencial, inicialmente, a preocupação era tentar ocultar a existência da mensagem e não se indagava como o seu conteúdo ficava exposto, caso esse artifício fosse descoberto. Esse processo de ocultar um texto é conhecido por esteganografia[1]. Com o tempo, as primeiras cifras simples de substituição foram inventadas, cuja intenção era substituir algumas letras por outras, ou por símbolos, de forma que fosse de conhecimento restrito apenas dos confidentes.

A palavra criptografia é derivada de duas palavras gregas: kryptós (secreto, escondido) e gráphein (escrita). É uma área da criptologia, a arte e a ciência de transformar (criptografar) informações (texto simples) em uma forma intermediária (texto cifrado) que protege as informações em armazenamento ou em trânsito.

> Até recentemente, tanto a criptografia quanto a criptoanálise eram consideradas uma arte. Somente há cerca de vinte anos é que a criptologia, que engloba o estudo de ambas, passou a ser considerada uma ciência. A International Association for Cryptologic Research (IACR ou Associação Internacional para a Pesquisa Criptológica) é a organização científica internacional que atualmente coordena a pesquisa nesta área e marca sua presença na Internet no endereço www.iacr.org. Geralmente se pensa que a criptologia é algo recente. Na verdade, como ciência, está apenas saindo da adolescência; como arte, sua história tem milhares de anos. (TKOTZ, 2005, p. 16).

Nos últimos anos, com a difusão e disponibilidade das informações e pela multiplicidade de dados eletrônicos manipulados, a sociedade moderna passou a depender de meios de comunicação eficientes e seguros, para garantia de informações íntegras e legítimas. "Tornando a criptografia, assim, uma ciência com interesse em estudos muito mais abrangentes, que faz uso de uma grande variedade de disciplinas e tecnologias, da matemática à linguística, da teoria da informação à teoria quântica", segundo (ANDRADE;

[1]Esteganografia é uma palavra que deriva do grego, na qual estegano significa esconder, mascarar e grafia significa escrita.

LUNARDI; RAMOS, , p. 2).

Há aspectos de segurança da informação relacionados a criptografia, conforme (MENEZES; OORSCHOT; VANSTONE, 2018, p. 5), como confidencialidade, integridade de dados, autenticação e não repúdio, que veremos a seguir:

i A confidencialidade é um serviço usado para manter o conteúdo das informações não disponível ou divulgada a indivíduos, entidades ou processos sem autorização.

ii A integridade de dados é um serviço que trata da alteração não autorizada de dados. A garantia da integridade dos dados é dada pela capacidade de detectar a manipulação de dados por pessoas não autorizadas.

iii A autenticação é um serviço relacionado à identificação. Esse aspecto da criptografia geralmente é subdividido em duas classes principais:

  iii.i Autenticação de entidade (um usuário afirma ter uma identidade legítima em um sistema).

  iii.ii Autenticação de origem de dados (um destinatário pode verificar se as mensagens não foram violadas em trânsito (integridade dos dados) e se originam do remetente esperado (autenticidade)).

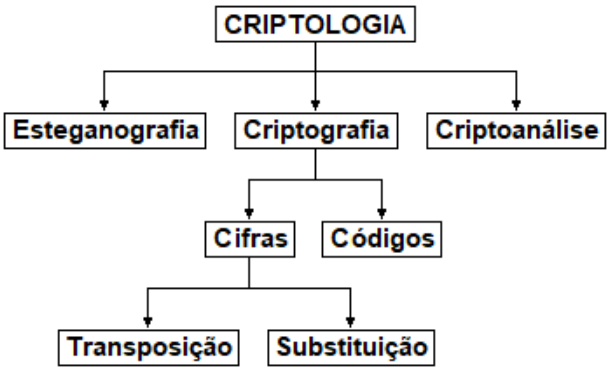
iv O não repúdio é um serviço que impede uma entidade de negar compromissos anteriores ou ações. Quando surgem disputas devido a uma entidade negar que certas ações foram tomadas, é necessário um meio para resolver a situação. Por exemplo, uma entidade pode autorizar a compra de imóvel por outra entidade e posteriormente negar tal autorização foi concedida. É necessário um procedimento envolvendo um terceiro confiável para resolver a disputa.

A criptografia é uma das áreas da criptologia e não é o único meio de prover segurança da informação, mas é um conjunto de técnicas que tem como propósito fundamental abordar adequadamente essas quatro áreas na teoria e na prática, através de medidas de prevenção e detecção de atividades maliciosas.

Na Figura 6, as áreas fundamentais da criptologia são a esteganografia, a criptografia e a criptoanálise. Da criptografia efluem-se os códigos e as cifras, destas destacam-se a transposição e a substituição, de acordo com (TKOTZ, 2005).

3.1.1 Conceitos básicos da criptologia

Os dois ramos principais da criptologia são: a criptografia, que é o estudo das técnicas para garantir o sigilo e/ou a autenticidade da informação; e a criptoanálise, que



Fonte: (TKOTZ, 2005)

Figura 6: Áreas da criptografia.

trata de frustrar essas técnicas, recuperar informações ou forjar informações que serão aceitas como autênticas.

Nessa subseção, identificamos e listamos alguns conceitos básicos da criptologia, baseados em (ANDRADE; LUNARDI; RAMOS,) e (CARMO; LEMES; FREITAS,):

- Criptologia é o estudo das técnicas de criptografia e criptoanálise.
- Criptografia é o conjunto de fundamentos e técnicas utilizadas para tornar a mensagem ininteligível àqueles que não possuem acesso aos algoritmo e chave empregados e abarcar a cifragem e a codificação.
- Criptoanálise é o emprego de técnicas para decifrar uma mensagem sem qualquer conhecimento dos detalhes de encriptação.
- Algoritmo de encriptação (algoritmo de cifragem ou cifra) realiza diversas substituições e transformações no texto claro. Parte central do esquema de encriptação.
- Algoritmo de decriptação ou decifragem é basicamente o algoritmo de encriptação executado de modo inverso. Ele recebe como entrada o texto cifrado e a chave e produz o texto claro original.
- Chave é uma entrada para o algoritmo de encriptação. A chave é um valor independente do texto claro e do algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave.
- Cifras simétricas oferece um estudo da encriptação simétrica, incluindo algoritmos clássicos e modernos. A ênfase está no algoritmo mais importante, o Advanced En-

cryption Standard (AES[2]). O Data Encryption Standard (DES[3]) também é abordado. Essa parte também enfatiza o algoritmo de encriptação de fluxo, RC4[4], e o tópico de geração de números pseudoaleatórios e aleatórios.

- Código é a substituição de uma unidade de texto original (ou seja, uma palavra ou frase significativa) por uma palavra-código (por exemplo, "ir para o objetivo primário" pode ser substituído por "fardo" e "ir para o objetivo secundário" pode ser substituído por "forte"). Outros exemplos são, o CPF[5] e os códigos de barras, formados por uma sequência com alternância de linhas brancas e pretas, estas barras contém informações sobre o fabricante, preço e origem do produto.

- Texto claro é a mensagem ou dados originais, inteligíveis, que servem como entrada do algoritmo de encriptação. Usa-se o termo texto ou mensagem, porém, algoritmos de cifragem aceitam qualquer tipo de dados.

- Texto cifrado é a mensagem embaralhada, produzida como saída do algoritmo de encriptação. Ela depende do texto claro e da chave secreta. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados distintos. O texto cifrado é um conjunto de dados aparentemente aleatório e, nesse formato, ininteligível.

Segundo (TRINTA; MACÊDO, 1998), os principais tipos de cifras são:

- Cifras de Transposição é o método pelo qual o conteúdo da mensagem é o mesmo, porém com as letras postas em ordem diferente. Por exemplo, pode-se cifrar a palavra "BARCO" e escrevê-la "OCRAB".

- Cifras de Substituição: neste tipo de cifra, troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição. As cifras de substituições podem ser subdivididas em:

  - Cifra de substituição simples, monoalfabética ou Cifra de César, é o tipo de cifra na qual cada letra da mensagem é substituída por outra, de acordo com uma tabela baseada geralmente num deslocamento da letra original dentro do alfabeto. Ela é também chamada Cifra de César devido ao seu uso pelo

[2]AES é um padrão de criptografia estabelecido em 2001, pelo National Institute of Standards and Technology (NIST) dos EUA.

[3]Baseado em um algoritmo, desenvolvido pela empresa IBM, chamado Lucifer. É o padrão utilizado pelo governo americano para a criptografia de seus dados desde 1978.

[4]RC2 e RC4 são algoritmos criados pelo Professor Ronald Rivest, são proprietários da RSA Data Security.

[5]Sigla de Cadastro de Pessoas Físicas.

imperador romano quando do envio de mensagens secretas. César quando queria enviar mensagens secretas a determinadas pessoas, substituía cada letra "A" de sua mensagem original pela letra "D", o "B" pelo "E", etc., ou seja, cada letra pela que estava três posições a frente no alfabeto.

- Cifra de substituição polialfabética utiliza várias cifras de substituição simples, nas quais as letras da mensagem são rodadas seguidamente, porém com valores diferentes. A mais conhecida deste tipo é a Cifra de Vigenère, primeiramente publicada em 1585 e foi considerada inquebrável até 1863.
- Cifra de substituição de polígramos: utiliza um grupo de caracteres ao invés de um único caractere individual para a substituição da mensagem. Por exemplo, "ABA" pode corresponder a "MÃE" e "ABB" corresponder a "JKI".
- Cifra de substituição por deslocamento, ao contrário da cifra de César, não usa um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério. Por exemplo, cifrar a palavra "CARRO" utilizando o critério de rotação "023", seria substituir "C" pela letra que está 0 (zero) posições a frente no alfabeto, o "A" pela letra que está 2 (duas) posições a frente, e assim por diante, repetindo-se o critério se necessário.

Agora que conhecemos alguns conceitos basilares da criptografia, faremos um breve relato de sua história.

3.2 CRIPTOGRAFIA: EVIDÊNCIAS HISTÓRICAS.

Nessa seção, trazemos um epítome sobre evidências históricas da criptografia.

De acordo com (KAHN, 1996), em uma cidade chamada Menet Khufu, situada na margem do rio Nilo, no Alto Egito, por volta de 1900 a.C., um mestre escriba ao esboçar os hieróglifos na tumba do nobre Khnumhotep II, substituiu alguns hieróglifos por outros, que decidiu, serem mais adequados para homenagear o sepultado, esse fato tornou partes da inscrição ininteligíveis, exceto para aqueles que sabiam qual substituição o escriba havia feito. Acredita-se que esse é o registro mais antigo de uma escrita com aspectos criptográficos.

Segundo (TKOTZ, 2005), a primeira mensagem criptografada na mesopotâmica, data de 1500 a.C., sendo escrita com caracteres cuneiformes em uma tabuleta de argila, na qual há a fórmula mais antiga conhecida de fabricação de esmaltes para louças de barro.

Ainda na antiguidade, apareceu a cifra Atbash, nela a primeira letra do alfabeto hebreu (Aleph) é trocada pela última (Taw), a segunda letra (Beth) é trocada pela penúltima (Shin) e assim progressivamente. A palavra Atbash deriva destas quatro letras: **A**leph **T**aw **B**eth **SH**in. Essa é uma das cifras hebraicas mais conhecidas, que datam de $600 - 500$ a.C., sendo encontrada no Antigo Testamento.

Por exemplo, na Bíblia, nos versículos no livro de Jeremias, conforme (SILVA; MARTINS, , p. 21):

- 25:26, lemos "a todos os reis do norte, próximos ou longínquos, uns após outros; a todos os reinos do mundo que habitam na superfície da terra. E depois deles beberá o rei de Sesac", a palavra "Sesac" significa Babilônia na língua hebraica.

- 51:1, "Eis o que declara o Senhor: vou levantar contra Babilônia e sua população de Lebcamai um vento de destruição", a palavra "Lebcamai" representa caldeus[6].

- 51:41, "Como foi tomada Sesac, e vencida a glória de toda a terra? Como se tornou Babilônia objeto de horror, no meio das nações?".

Texto original:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Texto cifrado:	ZYXWVUTSRQPONMLKJIHGFEDCBA

Fonte: Elaborado pelo autor.

Tabela 14: Cifra Atbash.

Nessa cifra, troca-se a letra n[7] pela letra $m - n + 1$, no qual m é o número de letras no alfabeto utilizado, como exemplo em português na Tabela 14:

Ainda segundo (TKOTZ, 2005), por volta de 300 a.C. na Índia, surgiu uma obra de Kautilya (a Artha-sastra) sobre a ciência de governar, na qual aconselhava aos embaixadores empregar criptografia e criptoanálise. Outro exemplo indiano, que se serviu de mensagens secretas no seu conteúdo é o conhecido livro erótico Kama-sutra, escrito por Vatsyayana.

Na Roma Antiga, foi utilizada a Cifra de César (ou cifra de troca), uma técnica de criptografia simples, um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto porém deslocada um certo número de posições, nesse caso, cada letra é substituída pela letra que está três casas a frente, isto é, a letra A é trocada pela letra D, a letra B é trocada pela letra E,

[6] Os caldeus eram um dos povos da antiguidade, que habitavam a região sul da Mesopotâmia, conhecida como Caldeia, região que atualmente é o território onde estão situados Iraque, Síria e Turquia.

[7] n é a posição da letra no alfabeto.

e assim sucessivamente até a letra Z que é trocada pela letra C. Esta Cifra é identificada como ROT3 (rotação em 3 posições), conforme mostrado na Tabela 15.

Alfabeto Normal:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabeto Cifrado:	DEFGHIJKLMNOPQRSTUVWXYZABC

Fonte: Elaborado pelo autor.

Tabela 15: Cifra de César.

No caso da Cifra de César, por exemplo, nós ciframos a palavra "criptografia" observando a Tabela 15 e resultado obtido foi a palavra cifrada "fulswrjudild".

Essa cifra recebeu essa designação em homenagem ao ditador[8] romano Caio Júlio César (100–44 a.C.), pois segundo Caio Suetônio Tranquilo, historiador romano (69-130 d.C.), ele a utilizava para proteger as mensagens militares, que enviava aos seus generais. Outras variantes são: a Cifra de César reversa, a Cifra de Vigenère, a Cifra Beaufort (uma combinação das duas últimas) e a ROT13 (o alfabeto gira em 13 posições), que ainda é amplamente utilizada.

Vale ressaltar que os alfabetos criados na Europa (latim e grego, por exemplo) facilitam muito o trabalho de criptografia, pois contêm relativamente poucas letras, que são simples de manipular. Empregar cifras de substituição para textos em chinês não é tão óbvio, igualmente no alfabeto japonês Kanji que possui mais de 40 mil caracteres.

Após o descobrimento de métodos de quebra de cifras simples de substituição, a permutação ordinária de letras deixou de ser segura o suficiente para manter o sigilo das mensagens. E o surgimento de novas cifras permitiu uma melhor mistura de letras, ocultando mensagens e modificando aspectos típicos da linguagem (frequência de letras, pares populares de caracteres e etc).

Vimos, anteriormente, que a criptoanálise estuda meios que possibilitem quebrar uma cifra, para isso é importante, sempre que possível, identificar o sistema de cifra empregado, que o criptoanalista pode não conhecer; o passo seguinte é a quebra do sistema de encriptação da mensagem.

A criptoanálise nasceu, por volta do ano 750 d.C., com a descoberta da **análise de frequências**[9]. Durante o nosso estudo, não foi descoberto quem propôs esse método pela primeira vez. O primeiro registro conhecido surge no livro "Escritos sobre a decifração de mensagens criptográficas", do filósofo e matemático árabe muçulmano, reconhecido como

[8] A ditadura romana era uma instituição acionada em circunstâncias excepcionais, para resolver situações emergenciais, como uma crise interna ou uma guerra, seus limites de atuação e duração eram prévia e explicitamente fixados e não excediam mais do que seis meses.

[9] Na qual as frequências das letras do idioma na mensagem são comparadas às frequências médias em textos desse idioma.

"pai da filosofia árabe", Al-Kindi. A análise de frequência vale-se de uma característica fundamental nas mensagens codificadas por meio de cifras monoalfabéticas: as frequências com que aparecem os símbolos (ou letras) no idioma da mensagem original.

Letra	Frequência %	Letra	Frequência %
A	$14,63$	N	$5,05$
B	$1,04$	O	$10,73$
C	$3,88$	P	$2,52$
D	$4,99$	Q	$1,2$
E	$12,57$	R	$6,53$
F	$1,02$	S	$7,81$
G	$1,3$	T	$4,34$
H	$1,28$	U	$4,63$
I	$6,18$	V	$1,67$
J	$0,4$	W	$0,01$
K	$0,02$	X	$0,21$
L	$2,78$	Y	$0,01$
M	$4,74$	Z	$0,47$

Fonte: (GTA/UFRJ, 2022)

Tabela 16: Análise de frequência de letras na língua portuguesa.

Nós falaremos sobre o emprego de decifragem utilizando frequência de letras na língua inglesa nos livros de Alan Poe e Conan Doyle, que será exibido na Seção 3.3. No entanto, nos perguntamos quanto à língua portuguesa, como se apresenta a frequência de letras na nossa língua? Para responder essa questão verificamos o que diz um estudo apresentado em (GTA/UFRJ, 2022), que concluiu que as vogais A, E, O, I, U e as consoantes D, M, N, R, S são as mais recorrentes, constituindo mais de 75% dos textos em Português (do Brasil). Para que fique mais simples a comparação das ocorrências das letras na língua portuguesa, criamos a Tabela 16, que mostra, percentualmente, as frequências de letras, como indicadas no site do Grupo de Teleinformática e Automação - GTA/UFRJ.

Na sua época, o algoritmo ROT3 era razoavelmente seguro, pois os inimigos de César (majoritariamente) eram analfabetos e caso soubessem ler, teriam muita dificuldade em decifrá-lo, apesar do tipo mais simples de cifra ser a cifra de substituição monoalfabética. Atualmente, a cifra de César não oferece segurança e mesmo a Cifra de Vigenère mais complexa pode ser quebrada através de testes matemáticos de comprimento de chave e da análise de frequência.

Percebemos que ao longo dos séculos, um elaborado conjunto de protocolos e mecanismos foi criado para lidar com questões de segurança da informação, quando esta é transmitida por documentos físicos.

Segundo (MENEZES; OORSCHOT; VANSTONE, 2018, 21), muitas vezes, os objetivos da segurança da informação não podem ser alcançados apenas por meio de algoritmos e protocolos matemáticos, mas requerem técnicas processuais e cumprimento de leis para alcançar o resultado desejado.

Por exemplo, a privacidade das cartas é fornecida por envelopes lacrados entregues por um serviço de correio. A segurança física do envelope é limitada, por isso são promulgadas leis que tornam crime abrir correspondência, para a qual não se está autorizado.

Às vezes, a segurança é alcançada não pela informação em si, mas pelo documento físico que a registra. Por exemplo, o papel-moeda requer tintas e materiais especiais para evitar a falsificação.

Na história recente, foi criada uma escultura chamada Kryptos[10] (Figura 7) do artista americano James Sanborn, instalada em 3 de novembro de 1990 na entrada da sede da CIA[11] em Langley, Virginia.

Fonte: https://www.cia.gov/legacy/headquarters/kryptos-sculpture/, acesso em 20 jan. 2022

Figura 7: A escultura Kryptos de James Sanborn em frente à sede da CIA.

Tem como tema a "coleta de inteligência", a obra é feita de um pedaço de madeira petrificada que sustenta uma grande tela de cobre em forma de S, na qual estão inscritas mensagens enigmáticas[12], cada uma com um código diferente. Ela contém quatro mensa-

[10]https://www.cia.gov/legacy/headquarters/kryptos-sculpture/, acesso em 20 jan. 2022

[11]CIA é a sigla para "Central Intelligence Agency" (Agência Central de Inteligência), é uma agência de inteligência do governo dos Estados Unidos, responsável por investigar e fornecer informações de segurança nacional para o presidente e o seu gabinete.

[12]https://www.elonka.com/kryptos/transcript.html

gens criptografadas (Figura 8), com seus 1800 caracteres, das quais três foram resolvidas[13]. Ainda há uma quarta seção na parte inferior,que permanece intacta e é conhecida como $K4$.

EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ	ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD	AKRYPTOSABCDEFGHIJLMNQUVWXZKRYP
VFPJUDEEHZWETZYVGWHKKQETGFQJNCE	BRYPTOSABCDEFGHIJLMNQUVWXZKRYPT
GGWHKK?DQMCPFQZDQMMIAGPFXHQRLG	CYPTOSABCDEFGHIJLMNQUVWXZKRYPTO
TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA	DPTOSABCDEFGHIJLMNQUVWXZKRYPTOS
QZGZLECGYUXUEENJTBJLBQCRTBJDFHRR	ETOSABCDEFGHIJLMNQUVWXZKRYPTOSA
YIZETKZEMVDUFKSJHKFWHKUWQLSZFTI	FOSABCDEFGHIJLMNQUVWXZKRYPTOSAB
HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE	GSABCDEFGHIJLMNQUVWXZKRYPTOSABC
EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX	HABCDEFGHIJLMNQUVWXZKRYPTOSABCD
FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF	IBCDEFGHIJLMNQUVWXZKRYPTOSABCDE
FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ	JCDEFGHIJLMNQUVWXZKRYPTOSABCDEF
ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE	KDEFGHIJLMNQUVWXZKRYPTOSABCDEFG
DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP	LEFGHIJLMNQUVWXZKRYPTOSABCDEFGH
DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG	MFGHIJLMNQUVWXZKRYPTOSABCDEFGHI
ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA	NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
CHTNREYULDSLLSLLNOHSNOSMRWXMNE	OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
TPRNGATIHNRARPESLNNELEBLPIIACAE	PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM
WMTWNDITEENRAHCTENEUDRETNHAEOE	QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR	RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ
EIFTBRSPAMHHEWENATAMATEGYEERLB	SMNQUVWXZKRYPTOSABCDEFGHIJLMNQU
TEEFOASFIOTUETUAEOTOARMAEERTNRTI	TNQUVWXZKRYPTOSABCDEFGHIJLMNQUV
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB	UQUVWXZKRYPTOSABCDEFGHIJLMNQUVW
AECTDDHILCEIHSITEGOEAOSDDRYDLORIT	VUVWXZKRYPTOSABCDEFGHIJLMNQUVWX
RKLMLEHAGTDHARDPNEOHMGFMFEUHE	WVWXZKRYPTOSABCDEFGHIJLMNQUVWXZ
ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR	XWXZKRYPTOSABCDEFGHIJLMNQUVWXZK
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO	YXZKRYPTOSABCDEFGHIJLMNQUVWXZKR
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP	ZZKRYPTOSABCDEFGHIJLMNQUVWXZKRY
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR	ABCDEFGHIJKLMNOPQRSTUVWXYZABCD

Fonte: https://www.cia.gov/legacy/headquarters/kryptos-sculpture/, acesso em 20 jan. 2022

Figura 8: A transcrição da escultura Kryptos.

A placa de metal da Kryptos parece um pergaminho desenrolado, foi somente em 1998 que David Stein, um analista da própria CIA, mas que não é um criptoanalista profissional, verificou que a placa é composta por duas "páginas". A metade direita, mais distante da árvore petrificada, contém uma tabela semelhante à de Vigenère.

[13]https://math.ucsd.edu/ crypto/Projects/KarlWang/index2.html#1

3.2.1 Cifra de Vigenère

A criação dessa cifra é erroneamente atribuída a Blaise de Vigenère (1523 - 1596); ela encontra-se originalmente descrita no livro, datado de 1553, com o título La Cifra del Sig. Giovan Battista Bellaso. Além disso, o disco de codificação que recebeu o nome de Vigenère foi inventado em 1467 (56 anos antes do seu nascimento) por Leon Battista Alberti (1404-1472), considerado o pai da criptologia ocidental.

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

Fonte: Elaborado pelo autor.

Figura 9: A grade de Blaise de Vigenère, também conhecida por tabula recta, é um quadrado latino de ordem 26.

De acordo com (TKOTZ, 2005, p. 22), em 1585, Vigenère escreveu Traicte des Chiffres (Tratado dos Números), com mais de 600 páginas, contendo a primeira representação européia de ideogramas japoneses. As informações sobre a criptologia são bastante confiáveis. Ele mostrou-se corretíssimo, atribuindo os devidos créditos a todos os autores citados na obra.

A Cifra de Vigenére é um método de criptografia manual (algoritmo criptográfico de texto alfabético) baseado em uma variação da Cifra de César. Ele funciona aplicando uma série de diferentes Cifras de César no texto simples, com base nas letras de uma palavra-chave selecionada. Na verdade, é uma forma simples de substituição polialfabética. Esse

método é uma matriz ou tabela (tabula recta, quadrado de Vigenère ou a tabela de Vigenère, Figura 9) que consiste nos alfabetos escritos 26 vezes em linhas diferentes, cada alfabeto deslocado ciclicamente para a esquerda em relação ao alfabeto anterior, correspondendo as 26 possíveis cifras de César.

A primeira descrição de uma cifra polialfabética, bem documentada, foi feita por volta de 1467 por Leon Battista Alberti. A Cifra de Vigenère às vezes é confundida com o disco de Alberti ou Cifra de Alberti. Johannes Trithemius, em 1508, criou a tabula recta (uma matriz de alfabetos alterados), que depois seria um componente da Cifra de Vigenère, que ficou inquebrável por quase trezentos anos.

Fonte: https://www.cryptomuseum.com/crypto/usa/ccd/index.htm, acesso em 04 nov. 2021

Figura 10: Disco de Cifra Confederado projetado por Francis LeBarre.

A Cifra de Vigenère foi empregada no Disco de Cifra Confederado (Figura 10) que foi usado em campo durante a Guerra Civil Americana (1861-1865). Nesse disco a sigla CSA significa Estados Confederados da América e SS representa Serviço Secreto. Nele, os 2 discos concêntricos possuem o alfabeto completo na seqüência normal em torno de sua circunferência. As letras da palavra-chave determinam em quantos lugares o disco interno deve ser deslocado.

Desde de sua criação em 1553, a cifra de Vigenère tornou o exemplo mais conhecido de cifra polialfabética, e sua base contribuiu para que novas cifras polialfabéticas mais avançadas surgissem, tal como a máquina Enigma (uma máquina eletromecânica de

criptografia, empregada para criptografar e descriptografar códigos de guerra).

A vantagem da Cifra de Vigenère é que ela não é suscetível à análise de frequência, pois em diferentes pontos do processo de criptografia, a cifra usa um alfabeto diferente de uma das linhas da tabela de Vigenère, ou seja, a mesma letra de texto simples nem sempre será criptografada com a mesma letra de texto cifrado, pois o alfabeto usado em cada ponto depende de uma palavra-chave repetida. Apesar disso, há uma fraqueza fundamental na segurança dessa cifra, a chave é repetida ao longo do texto simples.

Die Geheimſchriften

und

die Dechiffrir-Kunſt.

Mit beſonderer Berückſichtigung

der deutſchen und der franzöſiſchen Sprache

von

F. W. Kaſiski,

Major z. D.

Berlin, 1863.

Druck und Verlag von E. S. Mittler und Sohn.

(Zimmerſtraße 84. 85.)

Fonte: https://pages.mtu.edu/ shene/NSF-4/Tutorial/VIG/Vig-Kasiski.html, acesso em 05 jun. 2022

Figura 11: Folha de rosto do livro Criptografia e a arte da descriptografia de Kasiski.

Friedrich Kasiski[14] publicou um relato completo de como quebrar a cifra de Vigenère, no seu livro "Die Geheimschriften und die Dechiffrirkunst" (Criptografia e a arte da descriptografia) em 1863 (Figura 11), que não dependia de nenhum conhecimento do texto simples ou da chave (apesar de Charles Babbage em 1846, ter empregado uma técnica semelhante, porém nunca a publicou).

[14]Friedrich Wilhelm Kasiski (1805-1881) foi um major de infantaria prussiana, criptógrafo e arqueólogo.

Kasiski foi bem sucedido ao examinar sequências repetidas de caracteres no texto cifrado, constituindo-se um possível indicativo do comprimento da chave secreta. Na análise o objetivo era encontrar mais sequências repetidas de caracteres, que auxiliava a diminuir o tamanho da provável chave secreta.

Uma vez descoberto o comprimento da chave secreta, o texto cifrado pode ser reescrito em um número correspondente de colunas, com uma coluna para cada letra da chave. Cada coluna é composta de um texto simples, que foi criptografado por uma cifra monoalfabética ou de César e a partir daí a quebra o texto cifrado é realizada de modo semelhante àquele aplicado a uma cifra de César.

Fonte: https://www.cryptomuseum.com/crypto/usa/ccd/index.htm, acesso em 04 nov. 2021

Figura 12: Disco de cifra reversa de César.

O disco de cifra reversa de Vigenère, também chamado de disco de cifra reversa de César (Figura 12), é constituído por um anel externo com o alfabeto na sequência normal e um anel interno giratório com o alfabeto na ordem inversa (ou reversa). Ao anel interno é presa uma régua, que pode ser fixada em qualquer uma das letras do anel interno.

3.2.2 Exemplo do uso de uma cifra polialfabética

Ainda que as palavras do texto claro tenham seus comprimentos ocultos e o alfabeto de substituição seja aleatório (no caso da Cifra de César, por exemplo), existe como decifrar um texto utilizando dados de frequência, padrões de repetição e informações sobre o modo como as letras são combinadas entre si. E o que que torna a solução possível? É o fato de que uma determinada letra em texto claro é sempre substituída pela mesma letra

cifrada, consequentemente, todas as propriedades da linguagem simples, como frequências e combinações, são transferidas à cifra e podem ser usadas para desvendá-la. Parece então que uma maneira de obter maior segurança seria usar mais de um alfabeto para cifrar uma mensagem ou vários alfabetos diferentes, correlacionado os correspondentes da ordem em que os alfabetos devem ser usados.

Para exemplificar como utilizar uma cifra polialfabética, vamos adotar o seguinte algoritmo, empregaremos dois alfabetos e alternaremos as letras entre eles durante a criptografia. Esse é um processo de cifra polialfabética na qual há mais de um alfabeto de texto cifrado e uma regra que explica sua utilização. Nesse exemplo, os alfabetos de texto cifrado podem ser uma cifra de César com chave aditiva[15] 3 e uma cifra de César com chave aditiva 7. Para isso, escolhemos um texto claro e vamos cifrá-lo, substituindo as letras de ordem ímpar no alfabeto de cifra de César com chave aditiva 3 e trocando as letras de ordem par no alfabeto da cifra de César com a chave aditiva 7. Vejamos como podemos criptografar a mensagem "Universidade Federal de Santa Catarina", utilizando o exemplo dado:

Chaves aditivas:	Alfabetos:																									
Alfabeto normal:	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
3 (letras ímpares):	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
7 (letras pares):	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

Fonte: Elaborado pelo autor.

Figura 13: Cifras monoalfabéticas-aditivas.

Chaves aditivas:	Texto original:																															
0	U	N	I	V	E	R	S	I	D	A	D	E	F	E	D	E	R	A	L	D	E	S	A	N	T	A	C	A	T	A	R	I	N	A
1	v	o	j	w	f	s	t	j	e	b	e	f	g	f	e	f	s	b	m	e	f	t	b	o	u	b	d	b	u	b	s	j	o	b
2	w	p	k	x	g	t	u	k	f	c	f	g	h	g	f	g	t	c	n	f	g	u	c	p	v	c	e	c	v	c	t	k	p	c
3 (letras pares):	X	q	L	y	H	u	V	l	G	d	G	h	I	h	G	h	U	d	O	g	H	v	D	q	W	d	F	d	W	d	U	l	Q	d
4		r		z		v		m		e		i		i		i		e		h		w		r		e		e		e		m		e
5		s		a		w		n		f		j		j		j		f		i		x		s		f		f		f		n		f
6		t		b		x		o		g		k		k		k		g		j		y		t		g		g		g		o		g
7 (letras ímpares):		U		C		Y		P		H		L		L		L		H		K		Z		U		H		H		H		P		H
	Texto criptografado:																															
	X	U	L	C	H	Y	V	P	G	H	G	L	I	L	G	L	U	H	O	K	H	Z	D	U	W	H	F	H	W	H	U	P	Q	H

Fonte: Elaborado pelo autor.

Figura 14: Exemplo de criptografia com chaves aditivas.

Obtemos o texto cifrado abaixo:

[15]Cifra com chave aditiva basea-se em adicionar à posição ocupada por uma letra no alfabeto um valor que a desloca para a posição da letra-cifra. A Cifra de César original tem chave aditiva 3.

Texto claro	UNIVERSIDADE	FEDERAL	DE	SANTA	CATARINA
Texto cifrado	XULCHYVPGHGL	ILGLUHO	KH	ZDUWH	FHWHUPQH

Ou, se desejamos retirar o espaço entre as palavras, temos:

Texto claro	UNIVERSIDADEFEDERALDESANTACATARINA
Texto cifrado	XULCHYVPGHGLILGLUHOKHZDUWHFHWHUPQH

Ou podemos anotar o texto claro sem espaços, ainda escrever a palavra-chave abaixo da mensagem original, alinhando cuidadosamente cada letra da palavra-chave com cada letra do texto claro e repetindo cada letra da palavra-chave para se adaptar a frase original.

Texto claro	U	N	I	V	E	R	S	I	D	A	D	E	F	E	D	E	R	A	L	D	E	S	A	N	T	A	C	A	T	A	R	I	N	A
Palavra chave	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H
Texto cifrado	X	U	L	C	H	Y	V	P	G	H	G	L	I	L	G	L	U	H	O	K	H	Z	D	U	W	H	F	H	W	H	U	P	Q	H

Fonte: Elaborado pelo autor.

Figura 15: Escrita da palavra-chave abaixo da mensagem original.

Observando o texto claro, ou a mensagem original, "UNIVERSIDADE FEDERAL DE SANTA CATARINA"e analisando a frequência de letras percebemos que

Letra	U	N	I	V	E	R	S	D	A	F	L	T	C
Frequência	1	3	3	1	5	3	2	4	7	1	1	2	1

Fonte: Elaborado pelo autor.

E, nesse momento, verificando o texto cifrado, ou a mensagem criptografada, "XULCHYVPGHGL ILGLUHO KH ZDUWH FHWHUPQH", assim, examinando a frequência das letras notamos que

Letra	X	U	L	C	H	Y	V	P	G	I	O	K	Z	D	W	F	Q
Frequência	1	4	4	1	8	1	1	2	3	1	1	1	1	1	2	1	1

Fonte: Elaborado pelo autor.

Procedendo deste modo, a frequência das letras é alterada, pois na mensagem original, a letra A aparecia 7 vezes, enquanto na mensagem criptografada, a letra A foi substituída pelas letras D (uma vez) e H (seis vezes), esta última letra também substitui a letra E (duas vezes). Com isso, as informações sobre a maneira como as letras são combinadas e dispostas no texto claro, em um único alfabeto, são alteradas dificultando a decriptografia.

O remetente da mensagem crifada pode utilizar todas as combinações dos 26 alfabetos, obrigando tanto ao rementente quanto ao destinatário ter em mãos o mesmo quadrado de Vigenère (Figura 14), nesse caso é possível que outras pessoas também o possuam e até saibam o modo como funciona o processo de criptografia empregado, entretanto a palavra-chave, que somente o rementente e o destinatário conheçam, deve permanecer inacessível para qualquer outro agente.

		Chave																								
		h	m	k	x	a	r	i	e	p	u	o	t	y	b	z	c	w	d	v	f	s	g	q	j	n	l
T	y	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
e	l	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
x	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	B
t	n	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
o	x	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
	j	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
	c	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
	q	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
	w	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
	g	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
	d	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
	a	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
	r	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
	i	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
	e	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
	u	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
	o	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
	t	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
	z	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
	v	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
	h	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
	m	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
	k	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
	s	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
	f	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Elaborado pelo autor.

Figura 16: O quadrado de Vigenère com letras desordenadas.

No caso de uma substituição monoalfabética, fazemos uma relação entre cada letra do alfabeto original com um outro alfabeto permutado. Deste modo, considerando que cada letra do alfabeto deve ser substituída por uma letra diferente dela mesma, teremos $26!(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{1}{26!}) \cong 1,48 \times 10^{26}$ possibilidades de definir a chave deste código, que correspondem as permutacões caóticas das 26 letras do alfabeto (Figura 16), o que torna bem mais complicado o ataque por força bruta[16].

[16]Ataque de força bruta consiste em todo e qualquer método utilizado para descobrir uma senha, uma chave criptográfica ou qualquer tipo de informação sigilosa, por meio de tentativa e erro.

3.3 CRIPTOGRAFIA NA LITERATURA

Nos livros dos autores Arthur Conan Doyle e Edgar Allan Poe, os protagonistas empregaram a mesma técnica de criptoanálise, a análise de frequências da letras no idioma em que os livros foram escritos, nesses dois casos a língua inglesa. Na ánalise de frequência são verificadas a quantidade de letras, artigos definidos e indefinidos, preposições e palavras curtas que mais aparecem na escrita da língua vigente.

3.3.1 O escaravelho de ouro (The gold bug).

Edgar Allan Poe publicou, em 18 de dezembro de 1839, no jornal Alexander's Weekly Messenger da Filadélfia, EUA, um artigo chamado "Enigmatical and Conundrumical" sobre criptografia. Essa experiência concedeu a Poe a fama de criptoanalista excepcional e serviu de inspiração para que ele escrevesse "O escaravelho de ouro[17]", em 1843.

E foi nesse livro que o termo **criptógrafo** foi empregado pela primeira vez. Além desse fato, o autor (POE, 2012) utiliza criptografia e esteganografia em um dos seus melhores e mais famosos contos.

No livro, o protagonista é William Legrand, outrora rico, descendia de uma antiga família protestante francesa de Nova Orleans. Fora viver em uma cabana na ilha de Sullivan, perto de Charleston, na Carolina do Sul, EUA. Nessa cabana vivia também um negro velho, chamado Júpiter, que foi libertado da escravidão antes do infortúnio de Legrand, mas que se recusava, voluntariamente, a abandonar o seu jovem "sinhô Will".

O narrador visita o amigo Legrand e é informado que esse achara um enorme besouro ou escaravelho, que Júpiter teimava que o inseto era de ouro maciço. Após discordar de Júpiter, Legrand desenha o escaravelho em um pedaço de "tecido" e entrega ao narrador para analisar, esse comenta que o desenho do inseto parece uma caveira. Surpreso com a afirmativa do amigo, Legrand olha novamente para o desenho que fizera e guarda-o em lugar seguro, trancado a chave.

E no decorrer da história, o protagonista começa a agir de maneira estranha e não dá notícias sobre si ao narrador, até que um mês depois do ocorrido, recebe uma carta de Legrand entregue por Júpiter, convocando-o a visitá-lo, pois era um assunto importante. Tratava-se de acompanhar a ele e Júpiter em uma expedição sigilosa às colinas, no continente.

Eles seguem de barco até o continente e depois embrenham-se pelo mato até chegarem a um tabuleiro, perto do cume de uma colina quase inacessível, cercado de penhascos.

[17] https://perguntasaopo.files.wordpress.com/2012/02/edgar-allan-poe-o-escaravelho-de-ouro.pdf

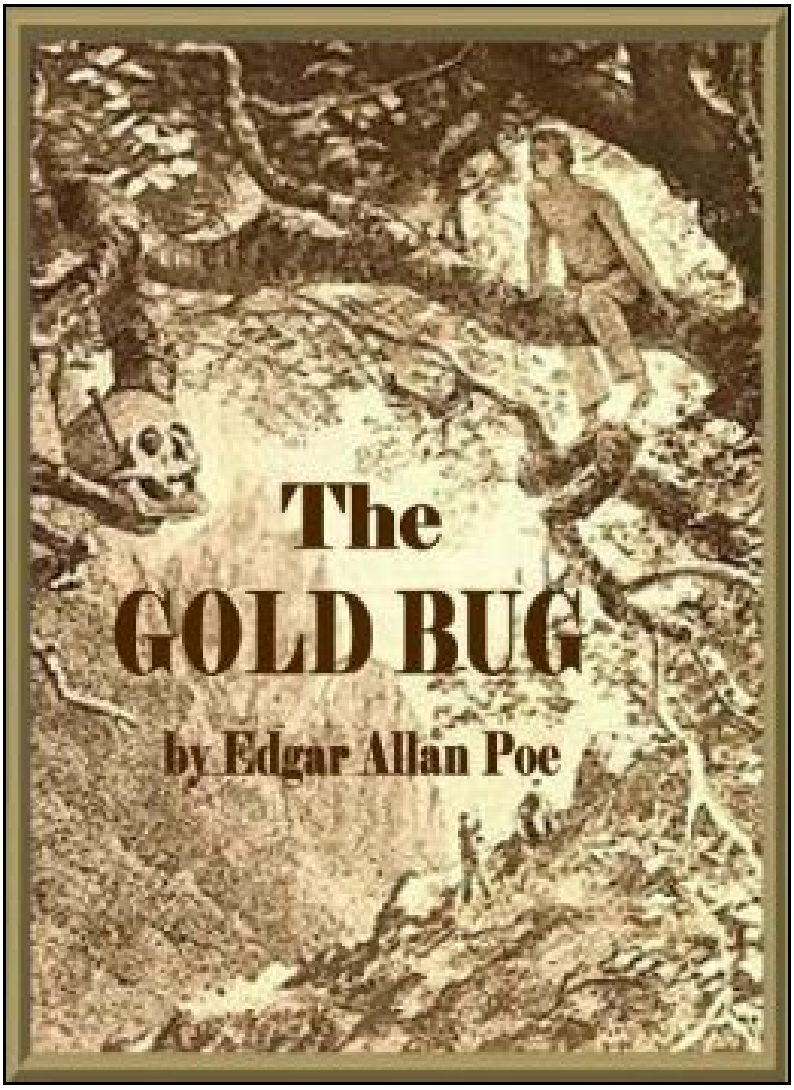


Figura 17: Capa do livro "The gold bug" de Edgar Allan Poe.

Legrand fica diante de um grande tulipeiro e pede que Júpiter suba nele, carregando o escaravelho (na Figura 17 ilustra Júpiter em um galho do tulipeiro).

A aventura dos três personagens segue e adiante no texto Legrand revela uma mensagem secreta que não aparecia no pedaço de "tecido" mostrado ao narrador, no início do livro.

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;1‡);:‡*8†83(88)5*†;46
(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1
(‡9;48081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

A mensagem criptografada apresenta esses algarismos e sinais (mas nenhuma letra) "5 3 ‡ † 0) 6 * ; 4 8 2 . ¶ 1 (: 9 ? - " (na ordem que aparecem na cifra). Ao analisá-la, contabilizamos as ocorrências (frequência), de cada símbolo, dispostas na Tabela 17 e

percebemos que:

Símbolo:	Ocorrência:	Símbolo:	Ocorrência:
Algarismo 8	33 vezes	Algarismo 1	8 vezes
Sinal ;	26 vezes	Algarismo 0	6 vezes
Algarismo 4	19 vezes	Algarismo 9	5 vezes
Sinal ‡	16 vezes	Algarismo 2	5 vezes
Sinal)	16 vezes	Sinal :	4 vezes
Sinal *	13 vezes	Algarismo 3	4 vezes
Algarismo 5	12 vezes	Sinal ?	3 vezes
Algarismo 6	11 vezes	Sinal ¶	2 vezes
Sinal (	10 vezes	Sinal −	1 vez
Sinal †	8 vezes	Sinal .	1 vez

Fonte: Elaborado pelo autor.

Tabela 17: Frequência de símbolos no livro "O escaravelho de ouro".

Para decifrar o enigma, Legrand diz que as letras mais frequentes na língua inglesa seguem a seguinte ordem: e, a, o, i, d, h, n, r, s, t, u, y, c, f, g, l, m, w, b, k, p, q, x, z (não aparecem nessa lista as letras j e v).

Na Tabela 17, o algarismo 8 é o símbolo mais presente. Como a letra "e" é que mais ocorre na língua inglesa. Podemos supor que algarismo "8" significa a letra "e", realizando essa troca, leremos:

53‡‡†305))6*;4e26)4‡.)4‡);e06*;4e†e¶60))e5;1‡);:‡*e†e3(ee)5*†;

46(;ee*96*?;e)*‡(;4e5);5*†2:*‡(;4956*2(5*-4)e¶e*;40692e5);)6†e)4‡‡;

1(‡9;4e0e1;e:e‡1;4e†e5;4)4e5†52ee06*e1(‡9;4e;(ee;4(‡?34;4e)4‡;161;:

1ee;‡?;

Podemos tentar obter o artigo "the" e verificamos que há seis ocorrências dos caracteres ";4e", vamos supor que ";4e" seja "the". Em seguida, inseriremos um espaço antes e após os artigos "the" obtidos e substituindo ";" por "t" e "4" por "h", temos:

53‡‡†305))6* the 26)h‡.)h‡) te06* the †e¶60))e5 t1‡) t:‡*e†e3(ee)5*†t

h6(tee*96*? te)*‡(the 5) t5*†2:*‡(th956*2(5*-h)e¶e* th0692e5) t)6†e)h‡‡t

1(‡9 the 0e1 te:e‡1 the †e5 th)he5†52ee06*e1(‡9 the t(ee th(‡?3h the)h‡t161 t:

1ee t‡? t

Após o penúltimo "the", lemos "t(eeth(+?3h", uma palavra que aparentemente não faz sentido, mas se a separarmos da seguinte maneira "t(ee th(+?3h", podemos propor que "t(ee" refere-se a palavra tree (árvore), desse modo, o sinal "(" significa a letra r e substituindo-a na cifra, leremos:

53‡‡†305))6* the 26)h‡.)h‡) te06* the †e¶60))e5 t1‡) t:‡*e†e3ree)5*†t

h6r tee*96*? te)*‡r the 5) t5*†2:*‡r th956*2r5*-h)e¶e* th0692e5) t)6†e)h‡‡t

1r‡9 the 0e1 te:e‡1 the †e5 th)he5†52ee06*e1r‡9 the tree thr‡?3h the)h‡t161 t:
1ee t‡? t

Há de se notar que após a palavra tree, aparece "thr‡?3h", que cremos tratar-se de "through", conseguindo assim mais três letras: ‡?3 ou oug, respectivamente.

5goo†g05))6* the 26)ho.)ho) te06* the †e¶60))e5 t1o) t:o*e†egree)5*†t
h6rtee*96*u te)*or the 5) t5*†2:*or th956*2r5*-h)e¶e* th0692e5) t)6†e)hoot
1ro9 the 0e1 te:eo1 the †e5 th)he5†52ee06*e1ro9 the tree through the)ho t161 t:
1ee tou t

Com essas letras substituídas, duas palavras parecem destacar-se ao final da primeira frase: "†egree" (ou degree) e "th6rtee*" (ou thirteen). Considerando "†" como d, "6" como i e "*" como n, além de destacar tais palavras, temos:

5good g05))in the 2i)ho.)ho) te0in the de¶i0))e5 t1o) t:one degree)5nd t
hir teen9inu te)nor the 5) t5nd 2:nor th95in2r5n-h)e¶en th0i92e5) t)id e)hoot
1ro9 the 0e1 te:eo1 the d e5 th)he5d 52ee0ine1ro9 the tree through the)ho t1i1 t:
1ee tou t

Antes da palavra thirteen lemos "degree)5nd" e depois dela "9inute)", o que sugere que ")" é a letra s, os algarismos 5 e 9 são as letras a e m. Ao substituí-las e adicionando espaços entre as palavras obtidas, o texto fica da seguinte forma:

agood g0assin the 2isho.shos te0in the de¶i0ssea t1os t:one degrees and t
hir teenminu tesnor the as tand 2:nor thmain2ran-hse¶en th0im2eas tsid eshoot
1rom the 0e1 te:eo1 the d ea thshead a2ee0ine1rom the tree through the shot 1i1t:
1eet out

Ressaltamos que nesse trecho do livro, o autor afirma que cifras desta natureza são facilmente solúveis e apresenta a tradução completa dos caracteres da mensagem. No entanto, continuamos com o processo de decodificação, mostrando todas as substituições dos símbolos pelas respectivas letras.

Retornando a cifra; vemos que no início, "agoodg 0assin the" pode ser lido como "a good g0ass in the", disso, encontramos a letra l (de 0). De "main2ran-hse¶enth0im2east" na segunda linha, podemos separar em "main 2ran-h se¶enth 0im2 east", e o símbolo ¶deve representar a letra v. Com essas substituições vemos que:

a good glass in the 2isho.s hostel in the devilssea t1os t:one degrees and t
hir teenminu tesnor the as tand 2:nor thmain2ran-hseven thlim2eas tsid eshoot
1rom the le1t e:eo1 the d ea thshead a2eeline1rom the tree through the sho t1i1 t:
1eet out

Do trecho que aparece "le1t e:eo1" e "1eet", o algarismo 1 pode ser trocado pela letra f. De "2isho.", "lim2" e "2ee", o 2 aponta para a letra b, vejamos com fica a cifra

após inserirmos essas duas letras:

a good glass in the bisho.s hostel in the devilssea tfos t:one degrees and t
hir teenminu tesnor the as tand b:nor thmainbran-hseven thlimbeas tsid eshoot
from the lef te:eof the d ea thshead abeelinefrom the tree through the sho tfif t:
feet out

Da cifra acima, verificando as palavras conhecidas e separando-as:

a good glass in the bisho.s hostel in the devils seat fost: one degrees and thirteen minutes north east and b: north main bran-h seventh limb east side shoot from the left e:e of the deaths head a bee line from the tree through the shot fift: feet out

De "bisho.s hostel" reescrevemos como "bishop's hostel", assim, o símbolo "." traduz-se na letra p. Olhando para "fost:", "b: north" e "e:e", cremos que ":" é a letra y. E o símbolo "−", em "bran-h", deve ser a letra c.

A good glass in the bishop's hostel in the devil's seat fosty one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the deaths head a bee line from the tree through the shot fifty feet out.

Na mensagem decrifada, a única palavra que não se encaixa é "fosty", que aqui será alterada para "forty". Revelando a mensagem decifrada no livro:

A good glass in the bishop's hostel in the devil's seat forty one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's head a bee line from the tree through the shot fifty feet out.

Que após ser traduzida para a língua portuguesa, podemos ler:

Um bom vidro no hotel do bispo na cadeira do diabo quarenta e um graus e treze minutos nordeste quadrante norte tronco principal sétimo galho lado leste atirai do olho esquerdo da caveira uma linha de abelha da árvore através do tiro cinquenta pés[18] distante.

[18] 50 pés equivale a 15,24 metros.

3.3.2 A Aventura dos Homens Dançantes (The adventure of the dancing men).

Arthur Conan Doyle escreveu o livro "A Aventura dos Homens Dançantes" em dezembro de 1903. Nele, o sr. Hilton Cubitt, de Ridling Thorpe Manor em Norfolk, Inglaterra, ao visitar Sherlock Holmes, conta que casou-se com uma americana chamada Elsie Patrick e entrega-lhe um pedaço de papel com uma sequência misteriosa de bonecos de palito ou dançantes (DOYLE, 1903).

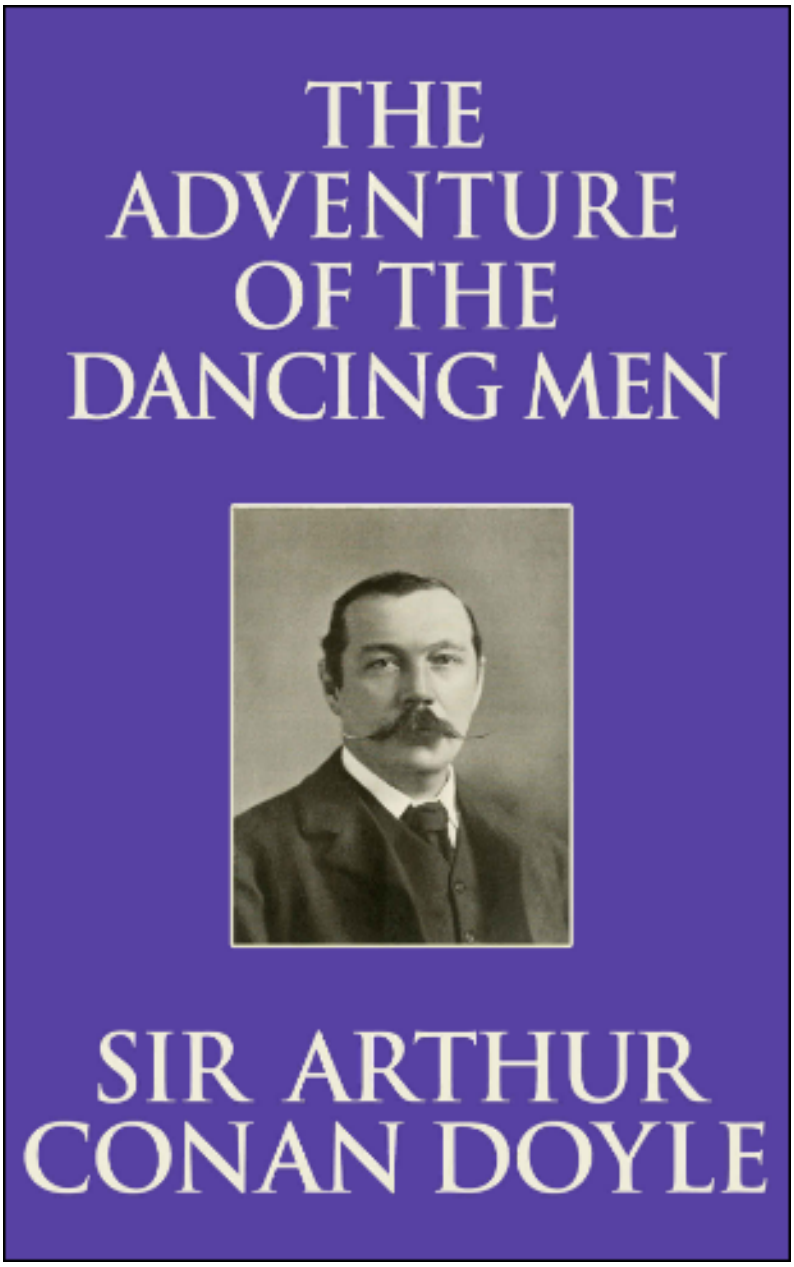


Figura 18: Capa do livro "The adventure of the dancing men" de Arthur Conan Doyle.

Hilton relata que estava feliz no casamento até que mensagens semelhantes foram recebidas pelo casal. Sua esposa Elsie ficou amendrontada com elas, porém não explicava

a razão do seu medo. Holmes começa a analisar as ocorrências das figuras de bonecos, percebe que deve tratar-se de uma cifra de substituição e desvenda o código utilizando análise de frequência.

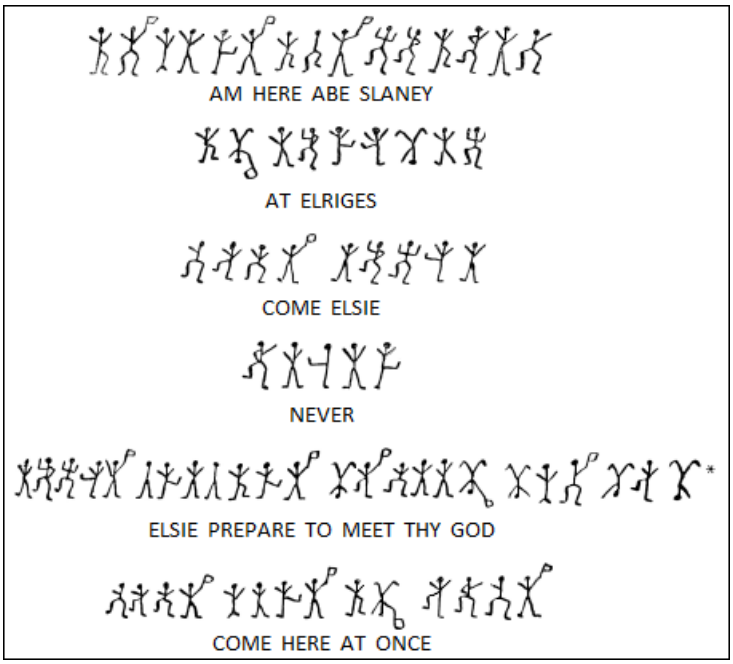
No livro, Doyle descreve o seguinte sobre as letras mais frequentes na língua inglesa.

> A ordem das letras mais comuns, depois do E, não é bem definida, e qualquer preponderância que se faça sentir numa folha impressa normal poderá desaparecer, quando se tratar de uma frase curta, tomada isoladamente. Falando por alto, as letras T, A, O, I, N, S, H, R, D e a letra L estão na ordem numérica em que mais aparecem; mas as letras T, A, O e I estão quase no mesmo plano, de modo que seria tarefa infindável tentar todas as combinações, até chegar a um resultado (CROWE, 2018, 56).

Fonte: (DOYLE, 1903)

Figura 19: Figura de homem dançante que representa a letra E.

Holmes analisa a primeira mensagem cifrada, com 15 figuras e sinaliza que a letra E seria a Figura 19, que se repete quatro vezes e considera que a bandeira na mão de um boneco indicaria a última letra de uma palavra.



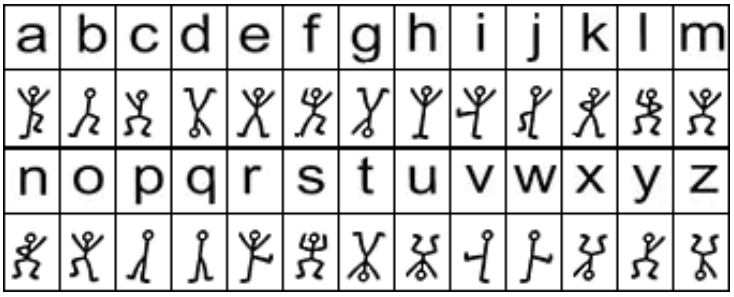
Fonte: (DOYLE, 1903)

Figura 20: Mensagens com as figuras de homens dançantes encontradas no livro.

Somente quando ele recebe, de Cubitt, a quarta mensagem com apenas cinco bonecos, ele consegue associá-los à palavra NEVER, obtendo três letras N, V e R, importantes para ajudá-lo a decifrar as mensagens anteriores.

Revendo a terceira mensagem, Holmes indaga que alguém que conhecera a sra. Cubitt, poderia citar o seu nome e a segunda palavra contendo duas letras E, com três letras intercaladas, poderia significar "Elsie". Dessa forma, conseguindo mais três letras úteis (L, S e I) para traduzir, quase totalmente, as outras mensagens.

E após alguns questionamentos, o detetive consegue, finalmente, deduzir a cifra (Figura 21) e a partir desse fato, ele escreve a última mensagem, mostrada na Figura 20 (com todas as mensagens cifradas que constam no livro), desvendando o mistério que envolvia o caso dos desenhos dos homens dançantes.



Fonte: (DOYLE, 1903)

Figura 21: Cifra do livro "A Aventura dos Homens Dançantes".

4 SUGESTÕES DE ATIVIDADES

Atualmente, os alunos têm acesso, facilmente, a computadores, celulares, jogos eletrônicos, aplicativos diversos e entre eles surgem jogos matemáticos que podem ser utilizados em sala de aula. Os jogos são interessantes para propor desafios, resolver problemas, estimula a cooperação entre os alunos, que exercitam a criatividade. Conforme (BRASIL, 2018, p. 265):

> Apesar de a Matemática ser, por excelência, uma ciência hipotético-dedutiva, porque suas demonstrações se apoiam sobre um sistema de axiomas e postulados, é de fundamental importância também considerar o papel heurístico das experimentações na aprendizagem da Matemática.

A BNCC também tutela a relevância da utilização de jogos nas aulas de matemática (BRASIL, 2018, p. 276)

> . [...] a aprendizagem em Matemática está intrinsecamente relacionada à compreensão, ou seja, à apreensão de significados dos objetos matemáticos, sem deixar de lado suas aplicações. Os significados desses objetos resultam das conexões que os alunos estabelecem entre eles e os demais componentes, entre eles e seu cotidiano e entre os diferentes temas matemáticos. Desse modo, recursos didáticos como malhas quadriculadas, ábacos, jogos, livros, vídeos, calculadoras, planilhas eletrônicas e softwares de geometria dinâmica têm um papel essencial para a compreensão e utilização das noções matemáticas.

Assim, utilizar jogos em sala de aula de matemática é uma atividade diferente para revisar os conteúdos já estudados ou ainda como uma abordagem prévia para novos assuntos, até como desafios, para que elaborem estratégias, desenvolvam habilidades, observem regras, trabalhem em grupo, respeitem adversários e o resultado do jogo. Como é dito por (ALBINO; SANTOS; MEDEIROS, 2019, p. 83):

> [...]. Por a Matemática ser uma disciplina abstrata, e ser adjetivada por muitos alunos como uma disciplina de difícil compreensão, os jogos podem quebrar, de certa forma, este pensamento e através destes os alunos passaram a vê-la como uma disciplina prazerosa e proporcionam a criação de vínculos positivos na relação professor-aluno e aluno-aluno. Com os jogos matemáticos, os alunos podem encontrar certo equilíbrio entre o real e o imaginário e expandirem seus conhecimentos e o raciocínio lógico-matemático.

Os jogos têm muitos atributos que são úteis em sala de aula como a existência de regras, controle do tempo, despertar o interesse pela matemática, incitar o raciocínio lógico, a saudável competitividade, entre outros aspectos, evidenciando que a sua utilização no ambiente estudantil, estimula o desenvolvimento cognitivo funcionando como uma ferramenta válida no processo de ensino e aprendizagem da matemática.

Nós selecionamos seis sugestões de atividades. Cinco vinculadas aos quadrados latinos, direta ou indiretamente e que julgamos interessantes para os alunos, tais como, o quebra-cabeça Kenken, o jogo das dezesseis cartas, o Sudoku, as mensagens cifradas (esta relacionada a criptografia), os quadrados mágicos e o jogo Erdös Latino.

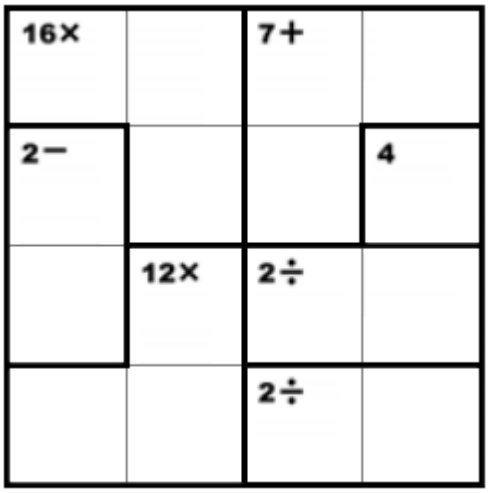
4.1 QUEBRA-CABEÇA KENKEN

O quebra-cabeça KenKen é uma matriz $n \times n$ preenchida com números inteiros de 1 a n, no qual cada elemento aparece exatamente uma vez em cada linha e em cada coluna. (DIACONU, 2015, p. 2) explica que, basicamente, o jogo é uma grade dividida em várias subgrades não sobrepostas, com bordas grossas, chamadas gaiolas, que têm diferentes formas e tamanhos. Cada uma dessas subgrades mostra um **resultado e uma operação matemática** (no canto superior esquerdo).

A operação matemática (adição, subtração, multiplicação ou divisão) é aplicada aos números dentro da gaiola para produzir o número correspondente ao **resultado**.

Por exemplo, na Figura 22 mostra um exemplo do quebra-cabeça KenKen 4×4. Nele aparece uma gaiola com o número 16, a operação de multiplicação e posições para três números, "**16*X***". Com isso, devemos multiplicar três números que resulte 16, ou seja, $2 \times 4 \times 2 = 16$.

Em outra gaiola, vemos "**2−**", nela devemos subtrair dois números e a diferença é igual a 2, podendo ser $3 - 1 = 2$. E assim devemos proceder do mesmo modo para cada gaiola, até completar a grade selecionada.



Fonte: http://www.kenkenpuzzle.com/, acesso em 25 jun. 2022

Figura 22: Exemplo do quebra-cabeça KenKen 4×4.

A versão do KenKen que apresentamos é jogada online no site que aparece na

Figura 22.

Esse jogo se basea em quadrados latinos. Se for jogado online, é possível escolher o idioma, selecionar o tamanho da grade, entre outras opções e ter acesso as regras do jogo que são:

i Escolher o tamanho da grade.

ii Inserir os números de 1 até o **tamanho da grade**.

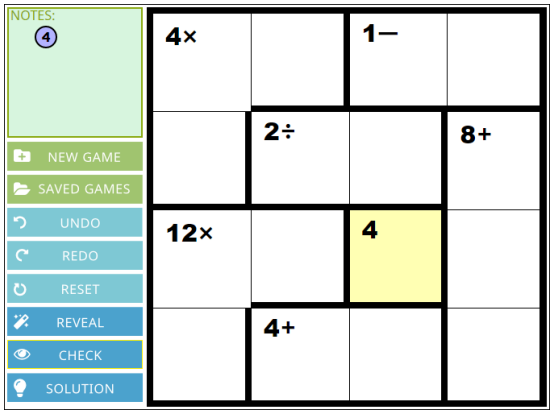
iii Não se pode repetir nenhum número na mesma fila ou na mesma coluna.

iv Os números dentro de cada conjunto de quadrados demarcados com linhas grossas, chamadas **gaiolas**, devem combinar (em qualquer ordem) de forma a produzir o **número pretendido**, indicado no canto superior, usando a **operação matemática** indicada.

v As gaiolas com apenas um quadrado devem ser preenchidas com o **número pretendido**, indicado no canto superior.

vi Pode repetir um número na mesma gaiola, desde que não se repita na mesma fila ou coluna.

vii Sempre que deseje ver se a sua solução é a correcta, clique em CHECK (ver Figura 23).



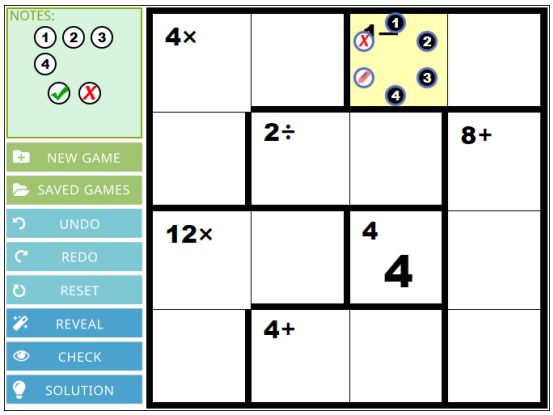
Fonte: http://www.kenkenpuzzle.com/, acesso em 25 jun. 2022

Figura 23: Opção de jogo KenKen 4×4.

Entrando no site do jogo e selecionando quadrados (ou grades) do tamanho 3×3 até 9×9. Para ilustrar um exemplo optamos por um quadrado 4×4 e pode surgir uma grade semelhante a Figura 23. Nessa Figura, vemos como diz a regra 5, há uma gaiola com

somente um quadrado com um número, nesse caso clicamos sobre a gaiola e digitamos o número 4 indicado no canto superior esquerdo para preencher essa gaiola.

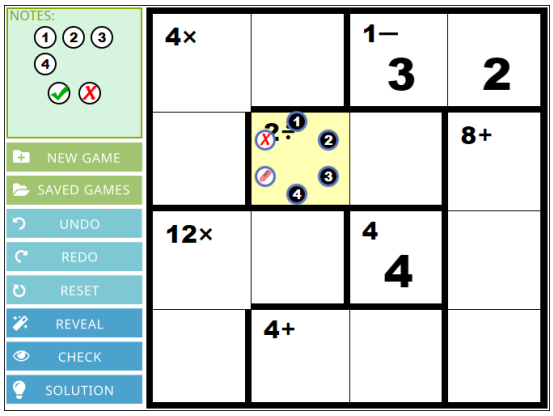
Na grade, sempre que clicamos sobre uma célula dentro de uma gaiola aparece as opções de números disponíveis, como é mostrado em **amarelo**, abaixo.



Fonte: http://www.kenkenpuzzle.com/, acesso em 25 jun. 2022

Figura 24: Números disponíveis por gaiola no jogo KenKen 4×4 selcionado.

Após completar uma gaiola, segue-se para outra, obedecendo a operação e o número pedido, procedendo assim até preencher toda a grade.



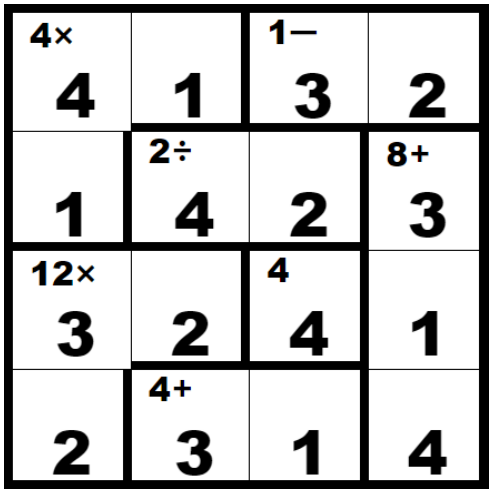
Fonte: http://www.kenkenpuzzle.com/, acesso em 26 jun. 2022

Figura 25: Preenchimento numérico das gaiolas do KenKen 4×4.

E finalmente, ao resolver o jogo escolhido, surge a expressão "KEN-GRATULATIONS!" acima da grade preenchida (um quadrado latino 4×4), mas que não aparece na Figura 26.

Ressaltamos que esse jogo também pode ser adaptado e impresso em papel, para ser jogado, por exemplo, individualmente ou em duplas.

Sugerimos que associado ao jogo sejam aplicadas as resoluções de exercícios com as quatro operações básicas, como mencionado na página 68.



Fonte: http://www.kenkenpuzzle.com/, acesso em 26 jun. 2022

Figura 26: Resolução do jogo KenKen 4×4 selecionado.

4.2 JOGO DAS DEZESSEIS CARTAS

Em (WILSON; WATKINS, 2013, p. 255) aparece o problema das dezesseis cartas figuradas (ou da corte) de um baralho que, anteriormente, abordamos quando falamos sobre a contribuição de Euler. E apresentamos uma possível resolução desse problema na Figura 4, que consistia em distribuir as dezesseis cartas figuradas (ás, rei, dama, valete) em um arranjo 4×4 de modo que cada linha, cada coluna e cada diagonal contenha um ás, um rei, uma rainha e um valete, todos de naipes diferentes. Assim, tanto os naipes quanto os valores formam, isoladamente, quadrados latinos mutuamente ortogonais (MOLS).

Utilizando qualquer baralho, as cartas descritas acima podem ser separaradas e utilizadas como um jogo em sala de aula.

Segundo (MORGADO et al., 1991, p. 2), "a solução de um problema combinatório exige quase sempre engenhosidade e a compreensão plena da situação descrita pelo problema". E juntamente com exemplos de problemas que abordam permutação, podemos complementar com esse jogo, para que os alunos busquem como executar a tarefa de construir quadrados latinos com essas cartas, conforme mostramos na Figura 27:

Abaixo na figura 28, apresentamos uma solução para o problema das cartas figuradas:

Fonte: Elaborado pelo autor.

Figura 27: Problema das dezesseis cartas da corte.

Fonte: Elaborado pelo autor.

Figura 28: Uma solução para o problema das dezesseis cartas da corte.

4.3 SUDOKU

De (POSSAMAI et al., 2020, p. 58) temos que o Sudoku é um quebra-cabeça, normalmente, composto de uma tabela 9×9 (81 células), dividida em 9 grades 3×3 (Tabela 18), que respectivamente têm 9 células e algumas células já contêm números. O objetivo do jogo consiste meramente em completar um quadrado latino, parcialmente preenchido

		7		**8**				**9**
	5		**6**		**1**		**2**	
			5		**3**			
	9	**6**	**1**		**4**	**8**	**3**	
3				**6**				**5**
	1	**5**	**9**		**8**	**4**	**6**	
			7		**5**			
	8		**3**		**9**		**7**	**6**
5				**1**				**3**

Fonte: Elaborado pelo autor.

Tabela 18: Exemplo da versão mais conhecida do Sudoku.

com números de 1 a 9, sem que haja quaisquer repetições de números na mesma linha, coluna ou grade.

A palavra Sudoku é uma espécie de sigla da expressão japonesa *Suuji wa dokushin ni kagiru*, que significa "os dígitos são limitados a uma ocorrência".

Este jogo, provavelmente segundo (GODINHO, 2008, p. 49), foi inspirado no quadrado latino, que teve origem com os estudos de Leonhard Euler no século XVIII, foi um dos quebra-cabeças numéricos que surgiram em jornais publicados na França em 1895.

Mas o esse jogo, verdadeiramente, foi criado por Howard Garns, um inventor de quebra-cabeças de Connersville, Indiana, EUA, em 1979, quando foi publicado na revista Dell Pencil Puzzles and Word Games. O quebra-cabeça era conhecido como "Number Place", pois envolvia colocar números individuais em espaços vazios em uma grade de 9×9.

O nome Sudoku foi proposto por Kaji Maki, o presidente da empresa editora Nikoli, responsável pela introdução deste passatempo no Japão e pela sua primeira publição no jornal Monthly Nikolist, da empresa, em abril de 1984. O termo Sudoku permanece uma marca registada da Nikoli.

Exite uma variedade de modelos de Sudokus, mas separamos alguns tipos que mais aparecem em almanaques, jornais, revistas e na internet: **Mini**, uma grade 6×6 com algarismos de 1 a 6; **Clássico ou Tradicional**, uma grade 9×9 com algarismos de 1 a 9; **Diagonal**, idêntico ao clássico com mais uma regra que não permite repetir números também nas diagonais da grade; **Irregular**, grade 6×6 com algarismos de 1 a 6, que contém polígonos irregulares e a regra extra de não repetir números no interior dos polígonos; e o **Mega**, grade 12×12 com algarismos de 1 a 12 e com as mesmas regras do clássico.

E para verificarmos como é a solução do exemplo apresentado anteriormente (Ta-

bela 18), preenchemos todas as células restantes, a grade completa é um quadrado latino 9×9 e fica da seguinte maneira (Tabela 19):

1	3	**7**	4	**8**	2	6	5	**9**
8	**5**	9	**6**	7	**1**	3	**2**	4
6	2	4	**5**	9	**3**	7	8	1
2	**9**	**6**	**1**	5	**4**	**8**	**3**	7
3	4	8	2	**6**	7	1	9	**5**
7	**1**	**5**	**9**	3	**8**	**4**	**6**	2
9	6	3	**7**	4	**5**	2	1	8
4	**8**	1	**3**	2	**9**	5	**7**	**6**
5	7	2	8	**1**	6	9	4	**3**

Fonte: Elaborado pelo autor.

Tabela 19: Exemplo anterior de Sudoku preenchido.

Observamos que o jogo pode ser utilizado como ferramenta para o desenvolvimento de regras de lógica em uma aula ou oficina de Matemática. E pode ser empregado para estimular a observância de instruções, concentração e raciocínio para resolvê-lo.

4.4 MENSAGENS CIFRADAS

Na seção 3.1 vimos que a cifra de substituição polialfabética utiliza usa uma série de diferentes cifras de César (cifras monoalfabéticas) baseadas em letras de uma senha e a mais conhecida e mais simples deste tipo é a Cifra de Vigenère. Que conforme o tamanho da chave e da mensagem pode tornar o processo demorado na codificação e decodificação de um texto. Como vimos na Seção 3.3, quando criptografamos a mensagem "UNIVERSIDADE FEDERAL DE SANTA CATARINA" e o texto cifrado era "XULCHYVPGHGLILGLUHOKHZDUWHFHWHUPQH".

Texto \ Chave	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Elaborado pelo autor.

Figura 29: Tábua de Vigenère destacando a Cifra de César.

Realizar uma atividade em sala de aula envolvendo criptografia empregando a Cifra de Vigenère poderia ser uma tarefa complexa e demorada para alunos. Então utilizar cifras monoalfabéticas como a Cifra de César (destacada na Figura 29 e na Tabela 20) seria mais simples e mais breve de ser confeccionada e experimentada.

Da tabela de Vigenère podemos extrair 26 cifras de César (Tabela 20) em tiras de papel e depois distribuir entre os alunos para que criem suas mensagens cifradas.

Outra opção para a tira da Tabela 20 é um disco de cifra de Vigenère (Figura 30), que nesta figura está indicando exatamente a cifra de César, mas contempla todas as possíveis cifras da Tábua de Vigenère, inclusive a ROT13 (rotação de 13 posições, Figura 21), que mencionamos na página 47.

A	B	C	D	E	F	G	H	I	J	K	L	M
d	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
q	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**

Fonte: Elaborado pelo autor.

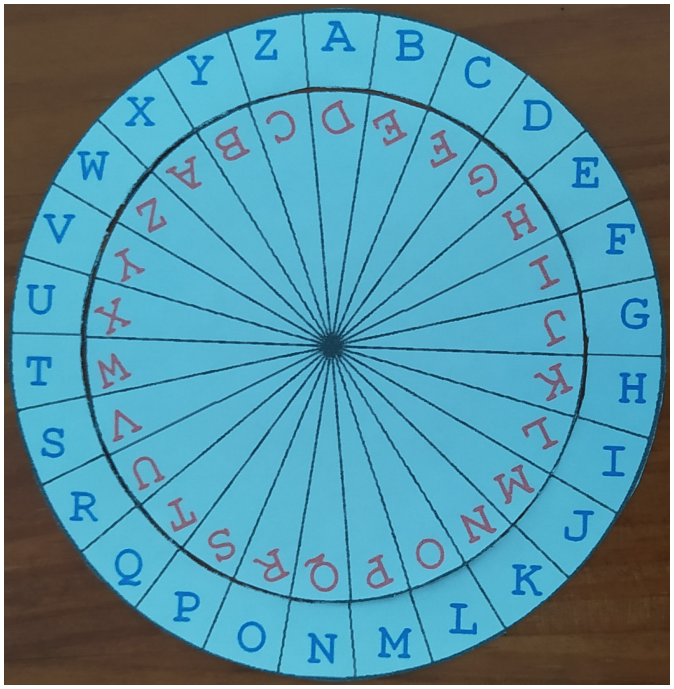
Tabela 20: Cifra de César representada em tira (ou faixa).

Ou se pode escolher uma letra do disco interno, que será a letra-chave, alinhando ela com a letra A, que indicará qual letra no disco interno (letras minúsculas) está associada a cada letra do disco externo (letras maiúsculas). Feito isso, para iniciar a codificação, basta escrever a mensagem desejada e depois substituir as suas letras no disco externo pelas letras correspondentes no disco interno.

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**
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**

Fonte: Elaborado pelo autor.

Tabela 21: Cifra ROT13 em tira (ou faixa).



Fonte: Elaborado pelo autor.

Figura 30: Disco de cifra de César de papel.

Codificação utilizando matrizes

Outra opção de atividade (relativa a criptografia) que sugerimos é associar o processo de criptografia ao estudo de matrizes quadradas invertíveis de ordem 2.

Por exemplo, utilizando a matriz $C = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$ como chave para cifrar e decifrar a mensagem "QUADRADO". Para isso devemos substituir cada letra da mensagem por um número, conforme mostramos na Tabela 22.

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

Fonte: Elaborado pelo autor.

Tabela 22: Substituição de letras por números no processo de cifragem.

Após a substituição de cada letra da mensagem por números, criamos uma matriz M com duas linhas, $M = \begin{pmatrix} 17 & 21 & 1 & 4 \\ 18 & 1 & 4 & 15 \end{pmatrix}$.

No passo seguinte, multiplicamos a matriz C pela matriz M para obter a matriz R.

$$R = C \cdot M = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 17 & 21 & 1 & 4 \\ 18 & 1 & 4 & 15 \end{pmatrix} = \begin{pmatrix} 53 & 23 & 9 & 34 \\ 141 & 68 & 23 & 87 \end{pmatrix}.$$

Deste modo, a matriz R é a nossa mensagem cifrada. E para o processo de decodificação, multiplicamos a matriz R pela matriz inversa de C, ou seja $C^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$.

$$M = C^{-1} \cdot R = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 53 & 23 & 9 & 34 \\ 141 & 68 & 23 & 87 \end{pmatrix} = \begin{pmatrix} 17 & 21 & 1 & 4 \\ 18 & 1 & 4 & 15 \end{pmatrix}.$$

E substituindo cada número da matriz M, de acordo com a Tabela 22, resgatamos a mensagem "QUADRADO".

4.5 QUADRADOS MÁGICOS.

O relato mais antigo de quadrado mágico é proveniente de uma lenda chinesa, que nos remete ao século 22 a.C., quando um imperador viu o desenho de um quadrado mágico 3×3 (Tabela 23) na carapaça de uma tartaruga que emergiu do rio Amarelo.

Durante a Idade Média, mencionamos que antigos autores árabes e indianos conheciam e utilizavam quadrados latinos para construir quadrados mágicos, inclusive Euler também empregou a mesma técnica, para construir quadrados mágicos e quadrados greco-latinos.

Antes de continuarmos vejamos o que são quadrados mágicos, segundo (POSSAMAI et al., 2020, p. 25).

> Um quadrado mágico é uma matriz quadrada $n \times n$, sendo $n > 2$, desenhada como um tabuleiro de damas com n linhas e n colunas, as quais são preenchidas com números distintos em arranjos particulares, de forma que a soma dos elementos de cada linha, de cada coluna, da diagonal principal e da diagonal secundária sejam iguais a uma constante, chamada constante mágica.

6	**1**	**8**
7	**5**	**3**
2	**9**	**4**

Fonte: Elaborado pelo autor.

Tabela 23: Quadrado mágico tradicional de ordem 3.

O modelo mais simples e tradicional de um quadrado mágico é o de ordem "3", também conhecido como Lo-Shu (Tabela 23). Observe que para o quadrado mágico da Tabela 23 a soma dos elementos de cada linha, de cada coluna, da diagonal principal e da diagonal secundária é igual a 15 (sua constante mágica, Equação 4.5). Mas como calculamos uma constante mágica de um quadrado $n \times n$?

Considere em quadrado mágico $n \times n$, preenchido com os números $1, 2, \ldots, n^2$ e denote por K a sua constante mágica. A soma, S_n, de todas as entradas do quadrado é dada por:

$$S_n = 1 + 2 + 3 + \cdots + (n^2 - 3) + (n^2 - 2) + (n^2 - 1) + n^2. \tag{4.1}$$

Notemos que é uma progressão aritmética de razão 1 a qual pode ser reescrita como,

$$S_n = n^2 + (n^2 - 1) + (n^2 - 2) + (n^2 - 3) + \cdots + 3 + 2 + 1. \tag{4.2}$$

Somando-se as equações (4.1) e (4.2), teremos,

$$\begin{aligned} 2S_n &= [n^2+1] + [(n^2-1)+2] + [(n^2-2)+3] + \cdots + [(n^2-1)+2] + [n^2+1] \\ &= \underbrace{(n^2+1) + (n^2+1) + (n^2+1) + \cdots + (n^2+1) + (n^2+1) + (n^2+1)}_{n^2\ vezes.} \end{aligned} \tag{4.3}$$

Isto é, $2S_n = n^2 \cdot (n^2+1)$, logo, $S_n = \dfrac{n^2 \cdot (n^2+1)}{2}$. Lembremos que a constante mágica é a soma dos elementos de cada linha, de cada coluna e de cada diagonal, e por termos n linhas e n colunas, então, $K = \dfrac{S_n}{n}$. Desse modo temos,

$$K = \frac{n \cdot (n^2+1)}{2}. \tag{4.4}$$

Utilizando a fórmula obtida para determinar a constante mágica de um quadrado mágico de ordem 3 tradicional (Tabela 23), com $n = 3$, confirmamos que $k = 15$.

$$K = \frac{3 \cdot (3^2+1)}{2} = \frac{3 \cdot 10}{2} = \frac{30}{2} = 15. \tag{4.5}$$

E como podemos construir quadrados latinos? Em (PICKOVER, 2011), no primeiro capítulo (Construção mágica), observamos alguns métodos para construções de quadrados mágicos, tais como aqueles atribuídos a Simon de la Loubère ou siamês (também em (POSSAMAI et al., 2020, p. 36), Claude Gaspar Bachet de Méziriac, Stairstep, John Lee Fults, Ralph Strachey, Diagonal e Albrecth Dürer, entre outros.

Todos os métodos de construção de quadrados mágicos variam em complexidade e como o nosso objetivo é propor atividades em sala de aula, vamos nos concentrar, sobretudo, em quadrados mágicos de ordem ímpar, em especial de ordem 3, e de ordem 4. Pois segundo (PICKOVER, 2011, 38), os "métodos gerais correspondentes para a construção de quadrados mágicos de ordem par são difíceis de implementar com lápis e papel, e quadrados mágicos de ordem par simples são geralmente os mais difíceis de construir".

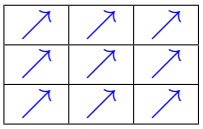
Em busca de um meio simples de construção de quadrados mágicos, escolhemos o método de la Loubère ou método siamês, que constrói **qualquer quadrado mágico de ordem ímpar** e que foi trazido para a França pelo matemático e diplomata francês Simon de la Loubère (1642–1729) após regressar do Reino do Sião[1]. Esse método segue a lógica do "método ascendente direito" por motivos que apresentaremos adiante, conforme (PICKOVER, 2011, 38):

E ainda podemos associar técnicas de manipulação algébrica e resolução de equações, por exemplo, ao calcular a equação 4.5.

[1] Atual Reino da Tailândia.

4.5.1 Método de la Loubère ou Siamês

Começaremos com a construção de um quadrado mágico de ordem 3 e explicando a lógica do "método ascendente direito" que significa fazer movimentos para cima e para a direita para preencher o quadrado com os números $1, 2, \ldots, 8, 9$, ou grosso modo, mover-se na diagonal com mostra a Tabela 24.



Fonte: Elaborado pelo autor.

Tabela 24: "Método ascendente direito" do Método Siamês.

Agora, podemos construir o quadrado 3×3 seguindo os seguintes passos mostrados na Tabela 25 e detalhados abaixo:

(1) Colocar no centro da primeira linha o número 1, ou seja, primeira linha, segunda coluna.

(2) Para colocar o número 2, sobe uma célula e depois uma à direita, ficando em uma linha fora do quadrado e na terceira coluna, então o 2 é posto na terceira linha (que corresponde a primeira linha acima do quadrado) e terceira coluna.

(3) Para colocar o 3, sobe uma célula e depois outra à direita, que fica em uma coluna fora do quadrado e na segunda linha, daí o 3 é colocado na segunda linha e primeira coluna (que corresponde a primeira coluna à direita do quadrado).

(4) Ao subir uma célula e ir uma à direita, coincide com a célula já ocupada pelo 1, quando isso ocorre desce uma célula a partir do 3 e o 4 fica na terceira linha e primeira coluna.

(5) Seguindo a lógica do "método ascendente direito", o 5 fica embaixo do 1.

(6) O 6 é posto à direita do 1.

(7) Ao subir uma célula e ir uma à direita, coincide com a célula já ocupada pelo 4, então o 7 fica embaixo do 6.

(8) Escrevemos o 8 em cima do 3.

(9) E o 9 embaixo do 5.

(1)
	1	

(2)
	1	
		2

(3)
	1	
3		
		2

(4)
	1	
3		
4		2

(5)
	1	
3	5	
4		2

(6)
	1	6
3	5	
4		2

(7)
	1	6
3	5	7
4		2

(8)
8	1	6
3	5	7
4		2

(9)
8	1	6
3	5	7
4	9	2

Fonte: Elaborado pelo autor.

Tabela 25: Construção de quadrado mágico 3×3 pelo método siamês.

No nosso trabalho não analisamos todas as características do quadrado mágico de ordem ímpar como em (POSSAMAI et al., 2020, 38). Bem como as contruções de diversos quadrados mágicos de ordens duplamente par, ou seja, múltiplos de 4, que adotam o método do matemático Abu Muzaffar Asfizari, de acordo com (POSSAMAI et al., 2020, 47).

Nós mostraremos, na próxima subseção, o motivo pelo qual elegemos esse método para a construção de quadrados mágicos de ordem 4.

4.5.2 Método de construção de quadrados mágicos de ordem duplamente par

Esse método, conforme Abu Muzaffar Asfizari, é utilizado para os chamados quadrados mágicos de ordem duplamente par ou múltiplos de 4 e também o selecionamos pela sua praticidade, pois o nosso intento é a sua utilização em sala de aula. Neste trabalho escolhemos construir apenas o quadrado de ordem 4.

Para construção do quadrado desejado, vamos utilizar dois quadrados 4×4.

Inicialmente, o primeiro com os números $1, 2, 3, \ldots, 14, 15, 16$, escrevendo $1, 2, 3, 4$ na primeira linha, $5, 6, 7, 8$ na segunda linha, $9, 10, 11, 12$ na terceira e $13, 14, 15, 16$ na última; e o segundo quadrado com os mesmos números, mas em ordem decrescente, na primeira linha $16, 15, 14, 13$, na segunda $12, 11, 10, 9$, na terceira $8, 7, 6, 5$ e na última $4, 3, 2, 1$; como na Tabela 26:

No primeiro quadrado, vamos realçar, colorindo, cinco quadrados menores, quatro de ordem 1, em verde, posicionados nos cantos e um quadrado de ordem 2 no centro, em amarelo. No quadrado da direita, realçaremos em azul, as células onde estão os números $15, 14, 12, 9, 8, 5, 3, 2$. Estes na Tabela 27:

E, na etapa final da construção, destacamos as células coloridas dos dois quadrados

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

16	15	14	13
12	11	10	9
8	7	6	5
4	3	2	1

Fonte: Elaborado pelo autor.

Tabela 26: Construção de quadrado mágico de ordem 4 - parte 1.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

16	15	14	13
12	11	10	9
8	7	6	5
4	3	2	1

Fonte: Elaborado pelo autor.

Tabela 27: Construção de quadrado mágico de ordem 4 - parte 2.

e as sobrepomos, formando um quadrado mágico 4×4 com as células totalmente coloridas. E sobrepondo as partes não pintadas que foram separadas, também formamos outro quadrado mágico 4×4, completamente branco, como podemos conferir na Figura 28.

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

Fonte: Elaborado pelo autor.

Tabela 28: Construção de quadrado mágico de ordem 4 - parte 3.

E para confirmarmos que o quadrado mágico de ordem 4 obtido pelo método acima está correto, vamos calcular a sua constante mágica pela Equação 4.4 e verificar que para $n = 4$, $k = 34$. O que pode ser rapidamente verificado, somando-se os números nas linhas, colunas, diagonal principal e diagonal sevcundária.

$$K = \frac{4 \cdot (4^2 + 1)}{2} = \frac{4 \cdot 17}{2} = \frac{68}{2} = 34. \tag{4.6}$$

4.6 ERDÖS LATINO.

O professor doutor da Faculdade de Ciências da Universidade de Lisboa, Jorge Nuno Silva, em 2011, idealizou um jogo chamado Erdös Latino, em (SILVA, 2012) , que consite em um tabuleiro quadrado com 25 casas quadradas, 25 peças circulares numeradas (ou discos numerados), sendo 5 peças com o número 1, 5 com o número 2, 5 com o número 3, 5 com o número 4 e 5 com o número 5, e 5 peças semicirculares para marcar as colunas conquistadas.

Fonte: https://www.luduscience.com/erdos.html, acesso em 7 jul. 2022

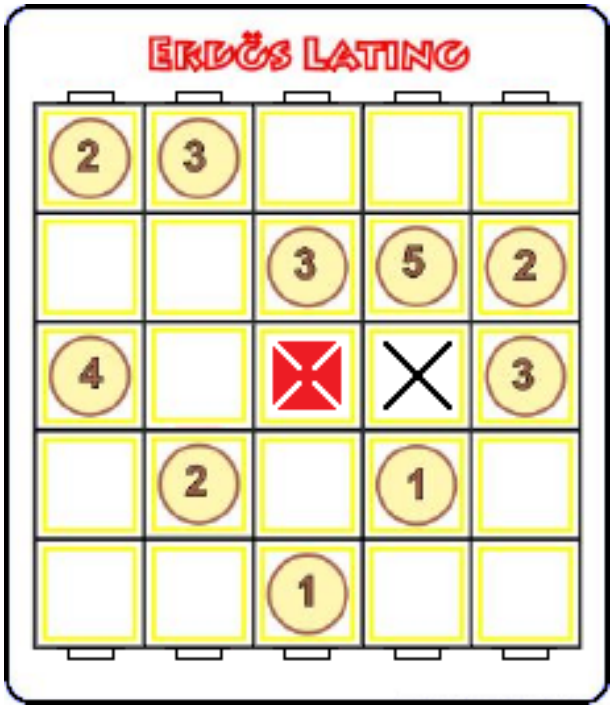
Figura 31: Tabuleiro de Erdös Latino.

A regra dita que cada jogada consiste em colocar um disco com um número em um quadrado livre, desde que tal movimento não origine repetição de número em alguma linha ou coluna (conceito de quadrado latino).

É jogado em dupla, que revezam as jogadas, o primeiro que, na sua vez, não conseguir jogar por não ter nenhum lance disponível, perde. Inclusive pode acontecer que o tabuleiro fique totalmente preenchido com peças, sendo assim, o jogador que tiver conquistado mais colunas é o vencedor.

Uma coluna é conquistada pelo jogador que, na sua vez, primeiro conseguir uma sequência crescente de comprimento 3 nessa coluna. Crescente, neste contexto, significa

que os números crescem em direção ao adversário. Logo, para vencer, é importante saber quem conquistou primeiro a coluna.



Fonte: https://www.luduscience.com/erdos.html, acesso em 7 jul. 2022

Figura 32: Exemplo de partida do Erdös Latino.

Por exemplo, na Figura 32 vemos que no tabuleiro estão marcados uma cruz de malta e um "X" preto.

O jogador A que está posicionado "abaixo" no tabuleiro, precisa inserir a peça, com o número 2, no lugar da cruz de malta para conquistar essa coluna. Enquanto o jogador B posicionado "acima", pode apenas colocar as peças "2" ou "5" no local da cruz de malta, praticamente, sem chance de conquistar essa coluna.

No caso da coluna onde está o "X" preto, o jogador A só pode colocar a peça "2" naquela posição e marcar a conquista da coluna, se não tiver a peça "2" no lugar da cruz de malta.

Outro detalhe, o jogo possui três níveis, descritos abaixo:

Principiante — As peças são misturadas com as faces numéricas ocultas e cada jogador deve tirar uma, aleatoriamente, em cada rodada.

Iniciado — As peças misturadas ficam sempre com as suas faces expostas e cada jogador, na sua vez, escolhe livremente qual jogar.

Misto — Após misturadas, as peças são distribuídas 12 para um e 13 para o outro jogador, aquele que recebeu 13 peças começa a partida.

5 CONCLUSÃO

Quando iniciei esse trabalho, não imaginava que as pesquisas sobre quadrados latinos tivessem a abrangência que vislumbrei e como a conjectura de Euler incentivou o ímpeto de matemáticos por buscar e descobrir novas aplicações para os quadrados latinos.

No nível pessoal, a proposta da pesquisa proporcionou uma rica experiência de aprendizagem e descobertas. Detalhes por vezes impulsionam mudanças pessoais e também em várias áreas do conhecimento, por exemplo, a impossibilidade de Euler encontrar dois quadrados latinos mutuamente ortogonais que resolvessem o problema dos trinta e seis oficiais ou o grito "eureka" de Arquimedes de Siracusa.

Dos quadrados latinos, o interessante foi me indagar, no início da pesquisa, que não é difícil construir quadrados mágicos utilizando quadrados latinos mutuamente ortogonais e se seria viável realizar o inverso, pois existem quadrados mágicos de ordem 6, mas isso se deu até ler sobre os trabalhos de Tarry Gaston, R. Fisher e F. Yates.

Quanto à criptografia, que está se desenvolvendo como ciência, há enormes desafios pela frente, já que com o surgimento de novos sistemas computacionais com capacidades que prometem tornar obsoletos os sistemas criptográficos atuais, logo as portas para novas pesquisas matemáticas estão abertas.

O objetivo da dissertação foi descobrir aplicações dos quadrados latinos, particularmente, como surgiram na criptografia e como foram utilizados; durante o processo de pesquisa, descobrimos bons exemplos na Cifra de Vigenère e suas variações, com destaque para o código de correção de erros. Além disso, a pesquisa foi limitada à aplicação básica de atividades em sala de aula com esses dois temas.

Nesse contexto, tanto os quadrados latinos quanto a criptografia são assuntos interessantes para serem sugeridos e desenvolvidos para atividades em sala de aula e foi gratificante perceber que os jogos Erdös Latino e KenKen têm potencial para isso.

E finalizando, sugerimos para futuras pesquisas:

- Utilização de quadrados latinos para fornecer mais segurança contra criptoanálise.
- Combinatória - cifras de substituição por polígramos (utiliza grupos de caracteres em vez de caracteres individuais).
- Função - cifras de transposição (cada caracter permanece inalterado, mas sua posição é alterada na mensagem segundo alguma regra ou função).
- Construção de quadrados mágicos utilizando o método de Euler.

- Atividades em sala de aula baseadas em quadrados latinos ou criptologia.

REFERÊNCIAS

ALBINO, H. E. V.; SANTOS, Y. A.; MEDEIROS, K. M. de. Os jogos matemÁticos para minimizar a matematofobia dos alunos: Um encontro no laboratÓrio de matemÁtica. *Ensino Aprendizagem de Matemática*, p. 81, 2019.

ANDRADE, E. R.; LUNARDI, R. C.; RAMOS, N. U. Conceitos basicos de criptografia.

ARANDA, M. H.; JUNG, C. F.; CATEN, C. S. T. Aplicação do projeto de experimentos para otimização de uma inovação tecnológica. *Revista Gestão Industrial. Ponta Grossa, PR. Vol. 4, n. 2 (2008), p. 116-132*, 2008.

BOSE, R. C.; SHRIKHANDE, S. S. On the falsity of euler's conjecture about the non-existence of two orthogonal latin squares of order 4t+ 2. *Proceedings of the National Academy of Sciences*, National Acad Sciences, v. 45, n. 5, p. 734–737, 1959.

BRASIL. *Base Nacional Comum Curricular: educação é a base. Ministério da Educação*. 2018. Disponível em: `http://basenacionalcomum.mec.gov.br/`. Acesso em: 24 jun. 2022.

CARMO, F. J.; LEMES, P. A.; FREITAS, T. H. Criptografia e pgp.

CROWE, M. J. The return of sherlock holmes (1905). In: *The Gestalt Shift in Conan Doyle's Sherlock Holmes Stories*. [S.l.]: Springer, 2018. p. 109–141.

DIACONU, A.-V. Kenken puzzle-based image encryption algorithm. In: *Proc Rom Acad Ser A*. [S.l.: s.n.], 2015. v. 16, p. 313–320.

DOYLE, A. C. *Os dançarinos*. 1903. Disponível em: `https://mundosherlock.wordpress.com/canon\_e/arthur-conan-doyle-a-volta-de-sherlock-holmes-1905/os-dancarinos/`. Acesso em: 04 nov. 2021.

DUARTE, J. B. Princípios sobre delineamentos em experimentação agrícola. 1996.

DéNES, J.; KEEDWELL, A. D. *Latin squares: New developments in the theory and applications*. [S.l.]: Elsevier, 1991.

EULER, L. Recherches sur un nouvelle espéce de quarrés magiques. *Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen*, p. 85–239, 1782.

FARIAS, F. G. et al. Quadrados latinos e quadrados mágicos - uma proposta didática. Universidade Federal da Paraíba, 2017.

FISHER, R. Statistical methods for research workers,(1925) oliver and boyd. *Edinburgh and London*, 1958.

FISHER, R. A. Design of experiments. *British Medical Journal*, BMJ Publishing Group, v. 1, n. 3923, p. 554, 1936.

FISHER, R. A.; YATES, F. et al. 110: The 6 x 6 latin squares. 1934.

FRISINGER, H. H. The solution of a famous two-centuries-old problem the leonhard euler-latin square conjecture. *Historia Mathematica*, Academic Press, v. 8, n. 1, p. 56–60, 1981.

GODINHO, G. *Cecilia Solange*. Tese (Doutorado) — Universidade de Aveiro, 2008.

GTA/UFRJ, G. de Teleinformática e automação. *Decifrando Textos em Português*. 2022. Disponível em: `https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html`. Acesso em: 05 jun. 2022.

KAHN, D. *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. [S.l.]: Simon and Schuster, 1996.

KEEDWELL, A. D.; DÉNES, J. *Latin squares and their applications*. [S.l.]: Elsevier, 2015.

LAMBERT, J. Cifrador simétrico de blocos: projeto e avaliação. *Rio de Janeiro: Instituto Militar de Engenharia*, 2004.

MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S. A. *Handbook of applied cryptography*. [S.l.]: CRC press, 2018.

MORGADO, A. C. de O. et al. Análise combinatória e probabilidade. *Sociedade Brasileira de Matemática, Rio de Janeiro*, 1991.

MORGADO, D. A. C. Quadrados latinos e grafos. 2012.

PICKOVER, C. A. The zen of magic squares, circles, and stars. In: *The Zen of Magic Squares, Circles, and Stars*. [S.l.]: Princeton University Press, 2011.

POE, E. A. *O escaravelho de ouro*. 2012. Disponível em: `https://perguntasaopo.files.wordpress.com/2012/02/edgar-allan-poe-o-escaravelho-de-ouro.pdf`. Acesso em: 04 nov. 2021.

POSSAMAI, A. et al. Quadrados mágicos. 2020.

REIS, M. M. et al. Um modelo para o ensino de controle estatístico da qualidade. Florianópolis, SC, 2001.

RESENDE, M. D. V. de R. *Matemática e estatística na análise de experimentos e no melhoramento genético*. [S.l.]: Embrapa Florestas, 2007.

RIBEIRO, J. L. D.; CATEN, C. t. Projeto de experimentos. *Porto Alegre: FEEng/UFRGS*, 2001.

SANTOS, C. A. d. et al. Quadrados latinos: um estudo histórico-filosófico da matemática. Blumenau, SC, 2018.

SILVA, A. F. da; MARTINS, R. M. Criptografia: aspectos históricos e matemáticos.

SILVA, J. N. Notas sobre o problema anterior e erdös latino. *Boletim da Sociedade Portuguesa de Matemática*, 2012.

SáNCHEZ, I. F. H. *Quadrados Latinos com aplicações em engenharia de software*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2011.

TANG, J. Latin squares and their applications. *Np: np*, 2009.

TARRY, G. *Le problème des 36 officiers*. [S.l.]: Secrétariat de l'Association française pour l'avancement des sciences, 1900.

TKOTZ, V. Criptografia: segredos embalados para viagem. *São Paulo: Novatec*, p. 16, 2005.

TRINTA, F. A. M.; MACÊDO, R. C. d. Um estudo sobre criptografia e assinatura digital. *Pernambuco: DI/UFPE*, 1998.

WALLIS, W. D.; GEORGE, J. C. *Introduction to combinatorics*. [S.l.]: Chapman and Hall/CRC, 2016.

WILSON, R.; WATKINS, J. J. *Combinatorics: ancient & modern*. [S.l.]: OUP Oxford, 2013.

APÊNDICE A – Diferença entre cifras monoalfabéticas e polialfabética.

No transcorrer do trabalho, por diversas vezes surgiram os termos "cifra monoalfabética" e "cifra polialfabética". Com o intuito de sintetizar as diferenças entre os dois tipos de cifras, que a primeira tem como exemplo a Cifra de César e a segunda a Cifra de Vigenère, elaboramos a Tabela 29.

Cifra Monoalfabética	**Cifra Polialfabética**
Cada símbolo em texto simples é substituído por um símbolo fixo em texto cifrado.	É uma cifra baseada em substituição, utilizando vários alfabetos de substituição.
A relação entre os caracteres do texto simples e os caracteres no texto cifrado é biunívoca.	Um caracter no texto simples é associado a diferentes caracteres no texto cifrado.
É uma cifra de substituição simples.	É uma cifra de múltiplas substituição.
Pode ser uma cifra de substituição aditiva, multiplicativa, afim e monoalfabética.	Pode ser Vigenère, Autokey, Playfair, Hill, one-time, pad, rotor e cifra Enigma.
É uma cifra de substituição na qual utiliza-se os mesmos mapeamentos fixos do texto simples para letras cifradas em todo texto.	É uma cifra de substituição na qual letras do texto simples em diferentes posições são codificadas usando diferentes criptoalfabetos.
São suscetíveis à análise de frequência.	Não são suscetíveis à análise de frequência, mas são vulneráveis quanto à repetição da palvra-chave.

Fonte: Elaborado pelo autor.

Tabela 29: Comparação entre cifras monoalfabéticas e polialfabéticas.