REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA: UM MAPEAMENTO DE DISSERTAÇÕES DE MESTRADO DE 2016 A 2025

CRYPTOGRAPHY IN MATHEMATICS EDUCATION: A MAPPING OF MASTER'S THESES FROM 2016 TO 2025

LA CRIPTOGRAFÍA EN LA ENSEÑANZA DE LAS MATEMÁTICAS: UN MAPEO DE TESIS DE MAESTRÍA DE 2016 A 2025

Lucas Purificação Mendes de Souza
Mestrando, Instituto Federal do Piauí – IFPI, Brasil
E-mail: lucksmendes@gmail.com

Benjamim Cardoso da Silva Neto
Doutor, Instituto Federal do Maranhão – IFMA, B
E-mail: benjamim.neto@ifma.edu.br

Kalisson Miranda dos Santos
Mestrando, Instituto Federal do Piauí – IFPI, Brasil
E-mail: Kalissonmiranda2@gmail.com

Antônio Ribeiro Silva Neto
Mestrando, Instituto Federal do Piauí – IFPI, Brasil
E-mail: ribe007@gmail.com

José Carlos Cecopierre Roldan Junior
Mestre, Instituto Federal do Piauí – IFPI, Brasil
E-mail: Joseroldan695@gmail.com

Guilherme Gonçalves Holanda
Mestre, Instituto Federal do Piauí – IFPI, Brasil
E-mail: guylhermeholanda96@gmail.com

Resumo

O presente artigo apresenta um mapeamento qualitativo de caráter descritivo acerca das intersecções entre a Criptografia e o ensino da Matemática apresentadas em dissertações de mestrado presentes no Catálogo de Teses e Dissertações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior e a Biblioteca Digital Brasileira de Teses e Dissertações no intervalo de tempo entre os anos de 2016 e 2025 e que apresentavam atividades ou propostas didáticas para o ensino de Matemática na Educação Básica. O foco deste artigo é determinar como a História da Criptografia pode ser utilizada como ferramenta didática para o ensino da Matemática, para tal foi primeiro abordado acerca do uso da arte de codificar por diversas civilizações históricas e após isso foi realizada uma análise das dissertações que se associavam simultaneamente a Educação e Criptografia, dando enfoque e descrevendo de maneira mais detalhada, em sequência como foi abordado o uso de métodos

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

históricos para ensinar Matemática, bem como também quais conteúdos foram associados a tais métodos.

Palavras-chave: Matemática; Criptografia; Métodos Históricos.

Abstract

This article presents a descriptive, qualitative mapping of the intersections between cryptography and mathematics education found in master's theses—specifically those featuring activities or pedagogical proposals for K-12 mathematics—listed in the CAPES (Coordination for the Improvement of Higher Education Personnel) Catalog of Theses and Dissertations and the Brazilian Digital Library of Theses and Dissertations between 2016 and 2025. The study focuses on determining how the history of cryptography can serve as a pedagogical tool for teaching mathematics; to this end, it first addresses the use of the art of encoding by various historical civilizations, followed by an analysis of theses linking education and cryptography. It subsequently provides a detailed description of how historical methods were employed to teach mathematics and identifies the specific mathematical content associated with these methods.

Keywords: Mathematics; Cryptography; Historical Methods.

Resumen

Este artículo presenta un mapeo cualitativo de carácter descriptivo sobre las intersecciones entre la criptografía y la enseñanza de las matemáticas, a partir de tesis de maestría incluidas en el Catálogo de Tesis y Disertaciones de la Coordinación de Perfeccionamiento de Personal de Nivel Superior (CAPES) y en la Biblioteca Digital Brasileña de Tesis y Disertaciones, en el periodo comprendido entre 2016 y 2025, y que incluían actividades o propuestas didácticas para la enseñanza de las matemáticas en la educación básica. El objetivo de este artículo es determinar cómo la historia de la criptografía puede utilizarse como herramienta didáctica para la enseñanza de las matemáticas; para ello, primero se abordó el uso del arte de codificar por parte de diversas civilizaciones históricas y, posteriormente, se realizó un análisis de las tesis que vinculaban la educación con la criptografía, describiendo con mayor detalle cómo se abordó el uso de métodos históricos para enseñar matemáticas, así como qué contenidos se asociaron a dichos métodos.

Palabras clave: Matemáticas; Criptografía; Métodos Históricos.

1. Introdução

O desenvolvimento de pesquisas em Educação Matemática tem se configurado como ampliado nos últimos anos, contudo, algumas áreas, linhas de pesquisa e temas de estudos ainda se comportam com um quantitativo reduzido de trabalhos e produções acadêmicas, e esses temas costumam ser de interesse de professores e pesquisadores. O movimento de pesquisas em determinadas temáticas pode fazer emergir novos pontos de interesses em discussões, novos

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

problemas e novos questionamentos que por sua sinalizam diferentes maneiras de pesquisar e até mesmo de se perguntar.

As pesquisas na área da Educação Matemática revelam diferentes temáticas e até mesmo informa sobre as direções que temas de estudos estão tomando. Nesse texto, no entanto, indagamos sobre as pesquisas que se utilizam da criptografia em sala de aula para o ensino de Matemática. Para tal, desenvolvemos um mapeamento de pesquisas de dissertações e teses sobre criptografia em sala de aula, pois intuímos que esses estudos podem informar caminhos didáticos que podem ser tomados por outros professores e pesquisadores no estudo dessa temática e na elaboração de novas estratégias didáticas. Esse estudo se trata de um recorte de uma dissertação de mestrado que promove a inserção da criptografia e de seus métodos históricos em uma proposta didática para sala de aula.

Pontuamos que criptografia não é um conteúdo trabalhado em sala de aula nas aulas de matemática, porém os conteúdos matemáticos podem se entrelaçar de alguma forma com informações da criptografia, porém, esse é um trabalho didático que necessita que o professor estude, pesquise e engaje seus alunos de alguma forma em sala, sob alguma perspectiva didática ou pressuposto metodológico para o ensino de Matemática.

De acordo com Silva, Perovano e Silva (2022) a criptografia faz parte da história da humanidade, do cotidiano humano e faz uso de ferramentas matemáticas e pode ser um recurso importante para o aguçamento da curiosidade, da criatividade e do empenho de estudantes no processo de aprendizagem de Matemática. Para Hefez (2022), a expressão criptografia é de origem grega que significa escrita oculta tendo por intuito tornar privada uma mensagem ao remetente e ao destinatário da mensagem enviada, de forma que mesmo que terceiros tenham acesso ao que está escrito eles não terão o entendimento do que a mensagem codificada significa, dificultando a descrição e compreensão da leitura, o que também proporcionou o desenvolvimento de novas técnicas que permitiam decodificar mensagens criptografadas, com isso permitindo e acompanhando ainda mais o advento da tecnologia.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Desse modo, neste artigo, nos perguntamos de que maneira pesquisas de dissertações e teses tem trabalhado criptografia no ensino de Matemática? Estabelecemos como principal recorte trabalhos de 2016 a 2025, últimos dez anos, e que necessariamente tenham desenvolvido propostas para sala de aula no âmbito da Educação Básica. Nossa metodologia se baseou no mapeamento de pesquisas da forma como é descrito por Fiorentini, Passos e Lima (2016) como sendo a busca por evidências em meio a um levantamento organizado e buscas por material acadêmico produzido em um determinado período de tempo.

Elegemos o Catálogo de Teses e Dissertações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior e a Biblioteca Digital Brasileira de Teses e Dissertações e foram constatados 26 trabalhos que utilizavam do método histórico acerca da criptografia como uma perspectiva metodológica, sendo que ampla maioria destes (22) são dissertações feitas por alunos do Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

As formas de codificar e também decodificar mensagens tem suas bases em noções matemáticas, em virtude disso, o presente artigo vem, dentre outros objetivos, com o intuito de dialogar acerca das possibilidades quanto ao uso da criptografia no ensino da Matemática em sala de aula.

Simultânea a ideia de utilizar da Criptografia, o presente artigo visa questionar o uso da História da Matemática como ferramenta pedagógica no ensino da disciplina em questão, daí surge a fusão pensada em englobar ambos os tópicos apresentando a possibilidade de trabalhos com a utilização da História da Criptografia.

Para tal foi utilizado do estudo bibliográfico que conforme Prodanov e Freitas (2013, p. 54) se baseia no estudo “a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet [...]”, sendo este dividido em 2 partes: a primeira relacionada a História da Criptografia e a segunda associada a utilização da Criptografia em sala de aula.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Assim, por meio deste estudo, espera-se como objetivo avaliar o uso da História da Criptografia como ferramenta de ensino da Matemática, abordando sobre a utilização da criptografia ao longo da história, analisando as dissertações relacionadas a temática “Criptografia e Ensino” disponíveis no catálogo de teses e dissertações da CAPES e por fim dialogando sobre as dissertações que utilizam de artefatos históricos da Criptografia como ferramenta de ensino da Matemática.

2. Revisão da Literatura

2.1 Criptografia ao longo da História

Do contrário do que se imagina a senso comum, ao se atrelar criptografia a modernidade devido ao frequente uso de tecnologia para aplicação da mesma, existem registros que comprovam a utilização da arte de esconder mensagens em diversas civilizações, por diversos intervalos de tempo em grande parte visando garantir a proteção de mensagens como afirma Quaresma (2008, p. 01):

> A necessidade de proteger os canais de comunicação entre pessoas de uma mesma comunidade vem desde os primórdios da civilização, a ideia de não só proteger os meios de comunicação mas também de proteger o próprio conteúdo da mensagem, através da cifração da mensagem é também muito antiga.

A criptografia tem seu primeiro registro nas terras faraônicas, segundo Tkotz (2024) por volta de 1900 a.C. em uma vila egípcia nas proximidades do rio Nilo, nomeada de Menet Khufu, a tumba de Khnumhotep II recebeu algumas substituições nos hieróglifos por outros que o escriba responsável acreditava ser mais adequados. Ainda que essa troca não tenha sido utilizada para ocultar segredos a mesma segue sendo considerada a primeira criptografia da história.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Figura 1: Tumba de Khnumhotep II



Fonte: Museu Egípcio Rosacruz

A antiga China foi uma das civilizações responsáveis pelo desenvolvimento de outra maneira de tornar uma mensagem segura: a esteganografia, nesta o conceito é um tanto diferente da criptografia, já que para esteganografar não há necessidade de codificar mensagem, basta apenas escondê-la, num geral com os mensageiros.

Al Cimino (2018, p. 12) corrobora com as informações ditas a cima ao citar que “na antiga China, as mensagens secretas eram escritas em papel ou seda finíssimos, enrolados numa bolinha e cobertas por cera. A bolinha era escondida no portador, talvez até inserida no ânus ou engolida”.

A civilização indiana foi de grande importância para a criptografia tanto no uso de diversos meios de ocultar mensagens, quanto no desenvolvimento da criptoanálise, termo utilizado para designar o estudo das formas de codificação com o intuito de desvendar tais táticas e “quebrar” os segredos por trás das mensagens.

Tkotz (2024) cita duas obras indianas da idade antiga que abordam sobre o uso de mensagens secretas, a primeira obra é a Artha-sastra, que aborda sobre a ciência de governar atribuída a Kautilya, onde há a recomendação que embaixadores utilizem de mensagens secretas e também da criptoanálise como forma de obter inteligência, a outra obra é o Kama-sutra, livro erótico desenvolvido por Vatsyayana,

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

que relaciona a uma das 64 artes que as mulheres deveriam conhecer e praticar as comunicações secretas tanto escritas, quanto faladas.

Outra civilização amplamente citada ao se falar de Idade Antiga e que também fez grande uso da criptografia foi a mesopotâmica, Al Cimino (2018) afirma que às margens do rio Tigre na região da antiga Selêucia, no Iraque, foi encontrada uma placa que apresentava a fórmula para fazer esmalte em cerâmica com código simples, por meio do uso da escrita cuneiforme.

Ainda em conformidade com Al Cimino (2018) os escribas assírios e babilônios tinham o costume de utilizar de formas raras de letras cuneiformes como um código para assinar ou mesmo datar suas placas. Por meio de comparação entre essas placas e outras placas com texto em formatos originais tornou possível a descoberta de tal código.

Figura 2: Escrita cuneiforme mesopotâmica



Fonte: Shutterstock

A Bíblia, o livro sagrado do Cristianismo, desenvolvido ao longo de cerca de 1600 anos e dividido entre Antigo e Novo Testamento, apresenta também trechos em que utiliza-se da codificação de mensagens, conforme Tkotz (2024, p. 17) “Em Jeremias 25:26 e 51:41, a forma Sheshach aparece no lugar de Babel (“Babilônia”) e, em 51:1, leb kmai (“coração do meu inimigo”) substitui kashdim (“caldeus”). Esta cifra é conhecida como atbash”.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

A cifra citada anteriormente utiliza da substituição de letras, de maneira que a primeira letra do alfabeto passa a ser representada pela última, a segunda pela penúltima e assim por diante, Conforme Al Cimino (2018, p. 14) “A palavra “atabash” reflete o padrão de substituição. É formado por “aleph”, “taw” e “shin” – a primeira, a última, a segunda e a penúltima letras do alfabeto hebraico”.

Durante a Antiguidade a criptografia foi amplamente utilizada no caráter militar, um exemplo que comprova isso é citado por Singh (2007) ao destacar o Bastão de Licurgo utilizado pelos Espartanos durante o século V a.C.

Figura 3: Bastão de Licurgo



Fonte: Al Cimino

Esse método consistia em enrolar em um bastão o material em que a mensagem seria repassada e após isso escrever tal mensagem na horizontal em relação ao comprimento do bastão, por fim o material utilizado para escrever a mensagem era desenrolado e como consequência a mensagem acabava por ficar completamente embaralhada, de maneira que para conseguir ler a mensagem seria necessário um outro bastão com as mesmas medidas do bastão original.

Além dos Espartanos diversos outros povos utilizaram a criptografia também para fins militares, dentre essas destaca-se a civilização romana com o código de Julio César, também chamada de cifra de substituição, que curiosamente “é o único da antiguidade usado até hoje” (Ordonez; Pereira; Chiaramonte, 2005, p 12), tal método consistia em codificar a mensagem por meio da mudança cíclica do alfabeto, ou seja, trocando as letras do alfabeto original por letras que estão em uma determinada quantidade de posições a frente dessa pela ordem alfabética, de forma

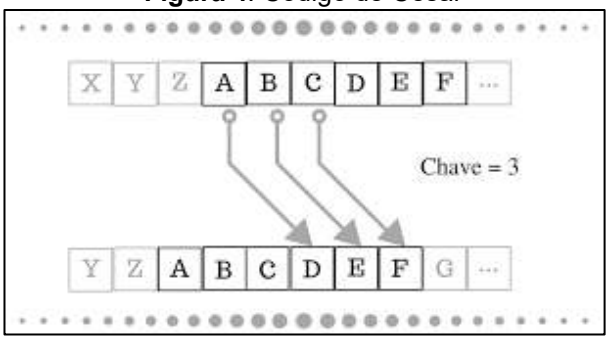
CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

que para decodificar tal mensagem era necessário saber quantas posições cada letra do alfabeto teria sido alterada.

Figura 4: Código de César



Fonte: Cifra de Cesar - Princípios de criptografia como trote educacional e em comemoração ao dia da mulher (2018)

Outra civilização antiga que merece ressalva por método criptográfico utilizado em guerra é a civilização grega, que resistiu a tentativa de dominação romana com Políbio e seu quadro.

> Onde as letras do alfabeto eram arranjadas da esquerda para a direita, de cima para baixo, em um quadrado 5x5. Cinco números eram então alinhados no topo do lado de fora do quadrado e cinco números no lado esquerdo do quadrado verticalmente. As letras poderiam ser deduzidas por referência cruzada desses números. Mensagens seriam enviadas por longas distâncias usando dez tochas. O remetente tinha cinco tochas à esquerda e outras cinco à direita, dispostas de modo que o receptor seria capaz de contá-las facilmente (Rank, 2015, n.p.).

Figura 5: Quadro de Políbio

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fonte: História da criptografia – cifras e códigos (2015)

Durante a Idade Média a criptografia ficou estagnada no que se refere ao desenvolvimento de novas técnicas no continente europeu, porém em paralelo a isto, no mundo muçulmano a criptografia, em particular a criptoanálise, evoluía a todo vapor, conforme afirma Al Cimino (2018, p. 22) “documentos de Estado sigilosos,

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

como o registro tributário, eram normalmente cifrados, e os manuais oficiais tinham capítulos sobre criptologia."

O grande responsável por tal desenvolvimento foi o islâmico Abu al-Kindî "o filósofo dos árabes" Conforme Al Cimino (2018) em um de seus manuscritos, intitulado *Da elucidação de correspondência codificada*, al-Kindî explica como decodificar uma mensagem utilizando da análise de frequência de acordo com a quantidade de vezes que uma letra ou mesmo um grupo de letras aparece no texto codificado.

Figura 6: Al-Kindî



Fonte: University of St Andrews

Bem como os árabes durante a Idade Média, a Idade Moderna teve grande avanço na criptoanálise no continente europeu, Al Cimino (2018) cita que durante o século XVI surgiu Giovanni Soro denominado como o primeiro grande decodificador da Europa, o autor afirma ainda que sua fama na época foi tão grande que o papa do período o contratou para desvendar códigos que os demais analistas não conseguiam decifrar. Após isso com a eclosão de novos conflitos no continente o surgimento de novos métodos de codificar tornou-se necessário por diversas partes da Europa.

Por volta de 1467 com base em seus estudos quanto aos meios de codificação Leon Battista Alberti, arquiteto italiano, notou que os meios de codificação por substituição simples estavam defasados para a época, visto que os criptoanalistas haviam se desenvolvido bastante em técnicas de decodificação.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

A partir daí então, o mesmo tratou de desenvolver um novo aparelho de codificação onde as substituições não seguiriam um simples padrão, tal método ficou conhecido como o disco de Alberti. Conforme Al Cimino (2018, p.38) “o aparelho consistia de dois discos de cobre com um eixo em comum que giravam um em relação ao outro”, sendo que o disco maior (externo) continha as letras maiúsculas do alfabeto em ordem e números de 1 a 4, enquanto que o disco menor (interno) tinha letras minúsculas em ordem aleatória.

O autor explica ainda como o disco era utilizado:

> A posição inicial é fixada no disco interno. A letra corresponde no disco extermo é escrita como maiúscula. Então, a mensagem é codificada trocando-se as letras maiúsculas do disco externo pelas minúsculas logo abaixo. De vez em quando, insere-se uma nova maiúscula na mensagem. Então, o ponto de partida do círculo interno é movido até essa letra, e a codificação recomeça, usando, em essência, outro alfabeto cifrado. (Al Cimino, 2018, p. 38)

Figura 7: Disco de Alberti



Fonte*:* Shutterstock

Compartilhando do mesmo pensamento de Alberti de que uma substituição simples estava atrasada para a época, o francês Blaise de Vigenère desenvolveu um método de codificação tomando por base o código de Cesar criado na antiguidade, resolvendo a fragilidade do método em questão para o período, já que conforme Takata (2017, p.86) “o maior problema das cifras de troca e substituição era a de que

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

cada letra do texto original era sempre criptografada com uma mesma letra no texto cifrado. Isso possibilita a quebra da cifra por meio da análise das estatísticas da língua na qual ela foi escrita".

Nesse método o alfabeto é disposto em uma tabela 26x26, de modo que cada linha está organizada de maneira que: a primeira linha inicia com a letra A, segue o alfabeto e finaliza com Z, a segunda linha inicia com B, segue o alfabeto e finaliza com A, a terceira inicia com C, segue o alfabeto e finaliza com B e segue-se o mesmo padrão até a última linha que inicia com Z e finaliza com Y.

Figura 8: Cifra de Vigenère



	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: Al Cimino

Francis Bacon, filósofo, político e escritor inglês foi outro a desenvolver um método de codificação, conhecido como a cifra de Bacon, tratava-se de uma cifra de substituição na qual as letras do alfabeto eram substituídas por um grupo de 5 letras, de maneira que essas 5 alternavam apenas entre a e b. Tkotz (2024, p. 230-231) explica o método e sua funcionalidade:

> Bacon usou um alfabeto de 24 letras em que o I e o J se equivalem, assim como o U e o V. Para cada uma das letras do alfabeto, ele atribuiu um grupo de cinco caracteres composto apenas por letras a e b. Como foram apenas usados dois tipos de caracteres, a cifra é considerada binária, e como os grupos são de cinco elementos, é considerada de cinco bits. A formação

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

> dos grupos segue uma sequência lógica igual à da composição dos números binários [...]. Nos grupos de Bacon, o elemento a pode ser substituído por 0 e o elemento b, por 1, para se obter seus equivalentes binários.

Figura 9: Código de Bacon

Letra	Grupo	Binário		Letra	Grupo	Binário
A	aaaaa	00000		N	abbaa	01100
B	aaaab	00001		O	abbab	01101
C	aaaba	00010		P	abbba	01110
D	aaabb	00011		Q	abbbb	01111
E	aabaa	00100		R	baaaa	10000
F	aabab	00101		S	baaab	10001
G	aabba	00110		T	baaba	10010
H	aabbb	00111		U/V	baabb	10011
I/J	abaaa	01000		W	babaa	10100
K	abaab	01001		X	babab	10101
L	ababa	01010		Y	babba	10110
M	ababb	01011		Z	babbb	10111

Fonte: Caballero (2012)

A criptografia se fez bastante presente também na Idade Contemporânea, tendo em vista que o sigilo é de grande valia em conflitos, durante esta época as mensagens eram transmitidas via rádio, tendo em vista que as mensagens poderiam ser facilmente ouvida por inimigos os alemães desenvolveram a cifra ADFGVX que se tratava de uma evolução do quadro de Políbio já explicado anteriormente.

Conforme afirma Al Cimino (2018, p. 67) “A cifra ADFGVX usa uma codificação em duas etapas. O quadro de Políbio tem seis linhas e seis colunas, designadas pelas seis letras. Então, o quadro é preenchido com as 26 letras do alfabeto e os dez algarismos de 0 a 9”, após isso, para codificar a mensagem analisava-se a linha e coluna em que cada letra estava, assim, cada letra era substituída por um par de letras. A segunda etapa consistia em organizar a mensagem codificada em uma nova tabela que em sua primeira linha terá uma palavra chave, por fim bastaria realizar a transposição de colunas em ordem alfabética, a considerar-se a palavra chave.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Figura 10: Cifra ADFGVX

	A	D	F	G	V	X
A	1	4	7	R	E	G
D	I	M	N	T	A	B
F	C	D	F	H	J	K
G	L	O	P	Q	S	U
V	V	W	X	Y	Z	0
X	2	3	5	6	8	9

Fonte: Crypto Corner (2023)

Já a segunda guerra mundial ocorreu entre 1939 e 1945 e marcou o embate entre aliados e o eixo, os aliados tendo por principais membros Reino Unido, União Soviética, França, Esados Unidos e China, enquanto que o eixo contava com Alemanha, Itália e Japão, neste período a codificação de mensagens teve um grande salto em evolução visto que o uso de máquinas foi aderido para dificultar ainda mais os códigos.

Conforme Tkotz (2024) a máquina Enigma, criada com o intuito de codificar mensagens alemãs foi desenvolvida ainda durante o período da primeira guerra mundial, porém foi apenas em 1933 que o exército e a marinha alemã aderiram a tal e a mesma foi de grande serventia para os países do eixo durante a segunda guerra mundial.

Figura 11: Máquina Enigma



Fonte: Revista Galileu – Globo (2019)

Devido ao alto nível de complexidade da máquina Enigma a tropa dos aliados uniu diversos matemáticos com o intuito de decodificar as mensagens elaboradas

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

por tal máquina, Al Cimino (2018) aborda ainda que visando a segurança dos decodificadores o governo britânico os alocou em Bletchley, território cercado por hectares de campo e de fácil acesso ferroviário a cidades como Londres, em virtude disso ficaram conhecidos como criptoanalistas de Bletchley Park. Este grupo de foi de grande valia para que os aliados vencessem a guerra, Al Cimino (2018, p. 120) cita que “durante a batalha da Grã-Bretanha, Bletchley Park se concentrou em decifrar códigos da força aérea alemã”.

Dentre os muitos gênios presentes em Blethley Park, Al Cimino (2018) aborda que Alan Turing, um matemático de Cambrige, que adentrou ao grupo de criptoanalistas com apenas 27 anos de idade, recebeu os créditos do primeiro-ministro do Reino Unido Winston Churchill como tendo sido responsável pela maior contribuição à vitória aliada contra a Alemanha nazista.

A criptografia na atualidade ainda se faz bastante necessária, por mais que não mais em guerras, como em grande parte dos casos citados até então, com o mesmo objetivo de todos os outros métodos: garantir a segurança daqueles que estão se comunicando, seja para proteger conversas de redes sociais ou mesmo dados de contas bancárias.

O método que se destaca atualmente é conhecido por sistema RSA e recebe este nome em alusão ao nome de seus desenvolvedores, este método utiliza de noções matemáticas tais como: números primos, fatoração, multiplicação e congruência modular, conforme afirma Hefez (2022, p. 272)

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

3. Procedimentos metodológicos: o mapeamento e a organização

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

A base para o processo metodológico de pesquisa se deu pelo uso do mapeamento de pesquisa descrito por Fiorentini, Passos e Lima (2016) como um método que se preocupa com os aspectos descritivos das pesquisas, o que se pode ir apontando sobre o comportamento de estudos e uma organização sobre principais temáticas, é nesse ponto que evidenciamos nosso questionamento sobre a forma pela qual a criptografia está sendo trabalhada em pesquisas de teses e dissertações de 2016 a 2025 no Brasil.

Ainda segundo os autores citados no parágrafo anterior o mapeamento dá conta de informar de onde são quem são os autores, quais pressupostos metodológicos e quais aspectos teóricos foram estudados e pesquisados a partir do montante de levantamento que é realizado.

Nesse caso, para sustentar nossa pergunta inicial de pesquisa, nos indagamos, com a finalidade de apontar no estudo, quem são os autores, de qual Instituição de Ensino Superior (IES), ano de defesa, qual a vinculação da criptografia com o ensino de matemática, qual o viés metodológico, qual a proposta didática produzida e para quais níveis de ensino da Educação Básica foi direcionada. Em seguida estabelecemos uma descrição sobre os métodos mais destacados nos trabalhos identificados.

Para a análise de dados, foi realizada a pesquisa de dissertações no catálogo de teses e dissertações da CAPES, sendo este desenvolvido em 2002 pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) com o intuito de facilitar o acesso a teses e dissertações defendidas em programas de pós-graduação stricto sensu e publicadas no país (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, 2025).

Para filtrar as dissertações de interesse para tal pesquisa foi utilizado como termo chave a frase “criptografia e educação” no item buscar do catálogo, foram localizadas 97 publicações relacionadas a tais temáticas, das quais após breve análise 51 se enquadravam nos quesitos desejados: ser desenvolvida na última década (2016-2025) e apresentar atividades ou propostas didáticas para o ensino

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

de Matemática na Educação Básica.

4. Resultados acerca do estudo das dissertações

Quadro 1: Identificação e caracterização das dissertações

Título da dissertação	Autor (Ano) IES	Conteúdos matemáticos	Nível de ensino	Dissertação de aluno do PROFMAT	Utilizou de métodos históricos como metodologia
APLICAÇÕES DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA A PARTIR DA RESOLUÇÃO DE PROBLEMAS	Abizai Campos Lima (2019) UESB	Congruência modular	Ensino médio	Sim	Não
CRIPTOGRAFIA E SEGURANÇA RSA: contextualização e aplicação	Adeilson Carlos de Lima Alves (2019) UFMA	Sequências e Tabelas	Ensino fundamental maior e ensino médio	Sim	Sim
A criptografia como estímulo à aprendizagem matemática	Ana Lourdes Moreno Rodrigues Silva (2021) UESB	Equação de 1º grau	Ensino fundamental maior	Sim	Sim
A CRIPTOGRAFIA NO ENSINO FUNDAMENTAL II: CONTEXTO HISTÓRICO, CIFRAS SIMÉTRICAS, APLICAÇÕES DE CONTEÚDOS MATEMÁTICOS E	Ana Paula Ferreira dos Santos (2016) UENF	Tabelas, Sequências, círculo e circunferência	Ensino fundamental maior	Sim	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

MUITAS OUTRAS CURIOSIDADES.					
TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA: UMA PROPOSTA DE ENSINO PARA ALUNOS DE MATEMÁTICA OLÍMPICA	Anderson Pinheiro Machado (2018) UFSM	Números primos, MDC, MMC e divisibilidade	Ensino fundamental maior	Sim	Sim
Criptografia e algumas aplicações em sala de aula	Andresa Laurett da Silva (2021) UFSC	Funções e permutação	Ensino médio	Sim	Sim
As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim.	Beatriz Fernanda Litoldo (2016) UNESP	Funções	Ensino médio	Não	Não
UM ESTUDO EXPLORATÓRIO ENVOLVENDO CRIPTOGRAFIA E NOÇÕES DE COMPUTAÇÃO QUÂNTICA	Bruna Schwarz Nunes Luiz (2021) UFSCAR	Fatoração de números	Ensino fundamental maior	Sim	Não
Aplicações de Criptografia no Ensino Básico	Bruno Laranjeira Nunes (2017) UERJ	Funções e matrizes	Ensino médio	Sim	Não
Introdução à criptografia e	Dafne de Moraes Deparis	Estatística, números	Ensino fundamental maior	Sim	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

atividades para a Educação Básica	(2021) UNIOESTE	decimais e porcentagem			
ENIGMÁTICA: uma proposta metodológica para o ensino de alguns objetos matemáticos usando a criptografia	Dayziane do Socorro Epifanio da Silva (2023) UFPA	Critérios de divisibilidade, funções e matrizes	Ensino médio	Sim	Não
RSA-CrypTa: UMA APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO MÉDIO	Edmarcos Martins Jordão (2023) UNIVASF	Números primos, fatoração, MMC, MDC e equações de primeiro grau	Ensino médio	Sim	Não
CRIPTOGRAFIA: UMA ENGENHARIA DIDÁTICA, COM FUNÇÕES, MATRIZES E CIFRA DE HILL, PARA O ENSINO MÉDIO	Eliseu da Rocha Marinho Filho (2016) UFOPA	Funções e matrizes	Ensino médio	Sim	Não
Criptografia RSA para o Ensino Médio	Eliton Mendes Pedrosa Simes (2023) UFRPE	Congruência modular	Ensino médio	Sim	Não
CodeClass: o uso da tecnologia como recurso metodológico no ensino da criptografia	Erlon Assunção Wandenkolk Alves (2019) UESB	Congruência modular	Ensino médio	Sim	Não

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Criptografia RSA: da teoria à aplicação em sala de aula	Evelyn Gomes da Silva (2019) USP	Matrizes	Ensino médio	Sim	Não
CRIPTOGRAFIA: COMO PRESERVAR SUAS INFORMAÇÕES UTILIZANDO OS CONCEITOS BÁSICOS DE MATRIZES	Fábio Santos Celestino (2017) UFRRJ	Equações e matrizes	Ensino médio	Sim	Não
Criptografia RSA: uma abordagem para o ensino médio	Fabricia Auxiliadora Queiroz (2018) UFMT	Divisibilidade e números primos	Ensino médio	Sim	Não
Explorando Elementos da Criptogra a RSA no Processo Educacional.	Fabricio Antonio Barzan (2025) UFMT	MDC, uso de planilhas	Ensino fundamental e ensino médio	Sim	Sim
UM ESTUDO EXPLORATÓRIO ENVOLVENDO CRIPTOGRAFIA E FATORAÇÃO NUMÉRICA	Fernanda Rodrigues Gomes (2022) UFSCAR	Fatoração numérica	Ensino médio	Não	Não
O ENSINO DE MATEMÁTICA ATRAVÉS DO ESTUDO DE TÉCNICAS CRIPTOGRÁFICAS UTILIZANDO O FORMATO WEBQUEST	Gabriel Teixeira Soares das Neves (2016) UFRJ	Contagem, matriz, funções, MMC e MDC	Ensino médio	Sim	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Explorando Códigos Corretores de Erros e Criptografia como Ferramentas Didáticas no Ensino Básico	Gilvania Carla Busatta (2024) UNIFESP	Números racionais, gráficos e tabelas, números primos, múltiplos e princípio multiplicativo	Ensino fundamental maior	Sim	Sim
ENSINO DE MATEMÁTICA BÁSICA USANDO CRIPTOGRAFIA	Guilherme Henrique Lima Silva (2023) UFCA	Funções, múltiplos e divisores	Ensino fundamental maior e ensino médio	Sim	Sim
A CRIPTOGRAFIA COMO RECURSO DIDÁTICO NO ENSINO MÉDIO	Guilherme Inácio Lemos Braga (2020) UFV	Porcentagem, funções e congruência modular	Ensino médio	Sim	Sim
USO DE FERRAMENTAS DE CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA PARA OS ENSINOS FUNDAMENTAL II E MÉDIO: PROPOSTAS DE ATIVIDADES	Isac Rosa Rodrigues (2024) UNEMAT	Geometria, progressão aritmética e matriz	Ensino fundamental maior e ensino médio	Sim	Sim
CRIPTOGRAFIA: Uma Abordagem Para o Ensino Médio	Jean Mendes Jansen (2016) UFMA	Funções e matrizes	Ensino médio	Sim	Não
SALA DE AULA INVERTIDA: PROPOSTA DE	Josias Dioni Bravim	Funções	Ensino médio	Não	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

INTERVENÇÃO NAS AULAS DE MATEMÁTICA DO ENSINO MÉDIO	(2017) IFES				
A APLICABILIDADE DA CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO CONTEXTO DA EDUCAÇÃO PROFISSIONAL	Josirene Zalenski de Siqueira Carvalho (2020) UNIR	Funções e matrizes	Ensino médio	Sim	Sim
A Criptografia no Ensino da Matemática: aplicações para a Educação Básica	Katarine Araújo Baldez de Carvalho (2018) UEMA	Sistema de numeração e conjuntos	Ensino fundamental maior e ensino médio	Sim	Sim
O Estudo da Criptografia RSA no Ensino Básico com Auxílio de Softwares Computacionais	Marcel Cavalcante Cerqueira (2016) UFAL	Divisão euclidiana e abordagem acerca de congruência modular	Ensino Médio	Sim	Sim
CRIPTOGRAFIA: UM ESTUDO HISTÓRICO E APLICADO A MATEMÁTICA DO ENSINO BÁSICO	Mauricio Soares dos Reis (2020) UEMS	Números reais e funções	Ensino médio	Sim	Sim
A CRIPTOGRAFIA MOTIVANDO O ESTUDO DAS FUNÇÕES NO 9º ANO DO ENSINO FUNDAMENTAL	Moisés de Oliveira Moura (2019) UFT	Funções	Ensino fundamental maior	Sim	Sim
APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO DE ANÁLISE	Nathan Lopes dos Santos	Análise combinatória e funções	Ensino médio	Sim	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

COMBINATÓRIA E SEGURANÇA DIGITAL NO ENSINO MÉDIO	(2024) UESB				
APLICAÇÕES DE CRIPTOGRAFIA NO ENSINO MÉDIO	Paulo Francisco de Araújo (2017) UFV	Congruência modular	Ensino médio	Sim	Não
CRIPTOGRAFIA EM UMA ABORDAGEM ELEMENTAR	PEDRO VALIM SAMPAIO (2021) UFSCAR	Funções	Ensino médio	Não	Sim
INTRODUZINDO NOÇÕES SOBRE CRIPTOGRAFIA NO ENSINO DE JOVENS E ADULTOS: RELACIONANDO BASE BINÁRIA E FUNÇÕES À CRIPTOGRAFIA	Rafael Mendonça dos Anjos (2020) Colégio Pedro II	Base 10, base binária, funções e porcentagem	EJA	Sim	Sim
CRIPTOGRAFIA: PROPOSTA DE ATIVIDADES PARA O ENSINO BÁSICO	Raissa Santos Rossetti Pereira (2020) UEMS	Números primos, funções e divisibilidade	Ensino médio	Sim	Não
CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA E CHAVE PÚBLICA RSA	REJEANE DE LIMA (2019) UDESC	Congruência modular	Ensino médio	Sim	Não

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Criptografia Kid-RSA adaptada: uma abordagem didática no estudo das operações de multiplicação e divisão	Renata Santos Lopes Cereja (2018) UFRJ	Divisibilidade e números primos	Ensino fundamental maior	Sim	Não
O ENSINO DE FUNÇÕES CONTEXTUALIZADO À CRIPTOGRAFIA	Roberta Maíra Verderi Braila (2021) UFSCAR	Funções	Ensino médio	Não	Sim
Congruência Modular no desenvolvimento da aprendizagem de Matemática nos anos finais do Ensino Fundamental	Roberto Amorim Silva (2022) UEMA	Congruência modular	Ensino fundamental maior	Sim	Não
Aritmética Modular: uma Aplicação no Ensino Fundamental	Rodolfo Cavalcante Pinheiro (2018) UFG	Divisibilidade e números primos	Ensino fundamental maior	Sim	Não
A CRIPTOGRAFIA COMO UMA FERRAMENTA PARA O ENSINO DA MATEMÁTICA NO ENSINO MÉDIO	Rubens Brás de Lucena (2020) UFRRJ	Círculos e matrizes	Ensino médio	Sim	Sim
Criptografia como ferramenta educacional no ensino da Análise Combinatória	Sávia Cristina Vidal (2019) USP	Análise combinatória	Ensino médio	Não	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

CRIPTOGRAFIA RSA NO ENSINO MÉDIO UM RECURSO DE MOTIVAÇÃO E APRENDIZAGEM	Tércio Rodrigues Freire (2020) UFT	Congruência modular	Ensino médio	Sim	Não
Criptografia RSA: da aritmética modular à sala de aula	Thiago de Mattos Serafim (2022) CEFET-MG	Congruência modular	Ensino fundamental maior e ensino médio	Sim	Não
Estudo sobre os Principais Aspectos da Criptografia Simétrica e Assimétrica ao longo da História	Thiago Marques Esteves Póvoa (2019) UnB	Funções e aritmética modular	Ensino fundamental maior	Sim	Sim
UMA METODOLOGIA COM USO DE CRIPTOGRAFIA PARA ENSINO DE FUNÇÕES	Valdemar Danilo de Carvalho (2020) UFSCAR	Funções	Ensino médio	Não	Não
EXPLORANDO OS NÚMEROS PRIMOS E UMA DAS SUAS APLICAÇÕES ATUAIS: A CRIPTOGRAFIA	Vivian da Silveira Miranda (2020) UFLA	Números primos	Ensino fundamental maior e ensino médio	Sim	Não
UMA PROPOSTA DE ATIVIDADES PARA EDUCAÇÃO BÁSICA ENVOLVENDO CRIPTOGRAFIA E FUNÇÕES	Walmir Pereira Salmazzo (2021) UEL	Funções	Ensino fundamental maior e ensino médio	Sim	Não
Teoria dos números e Criptografia RSA	Wélisson Martins Mota	Funções	Ensino médio	Sim	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

	(2023) UFPB				

Fonte: Elaborado pelos autores

Dentre as 51 dissertações, 31 propunham aulas com a inclusão de criptografia direcionadas ao Ensino Médio, 11 direcionadas ao Ensino Fundamental – Anos finais (6° ao 9°), 8 propunham simultaneamente atividades para os dois níveis e 1 apresentava a utilização da criptografia na Educação de Jovens e Adultos (EJA).

Nestas a criptografia foi utilizada como recurso de ensino da Matemática em diversos conteúdos, dentre os quais, os que mais foram associados foram: Matrizes, Funções, Divisibilidade e os Números Primos, porém em menores quantidades, também foi possível observar o uso da mesma em auxilio a tópicos como circunferências, sistemas de numerações, equações e até mesmo, congruência modular (tópico comum a ser estudado no Ensino Superior, em cursos que englobem cálculo).

Para a aplicação foram utilizados principalmente como maneira de estudo a codificação e a decodificação de mensagens associando métodos tradicionais de codificar a tópicos da Matemática, além desta forma, notou-se também o uso de tecnologias, como por exemplo os aplicativos Geogebra e CodeClass além também do uso da linguagem de programação Python.

Notou-se que 26 das 51 dissertações analisadas utilizaram em algum momento como recurso didático métodos de codificação aplicados por grandes civilizações ao longo da história, enquanto que o restante optou pelo uso da criptografia atual como ferramenta de ensino para a Matemática.

Dos tópicos de história da Criptografia citados anteriormente destacam-se o uso do Bastão de Licurgo, Cifra de Cesar, Disco de Alberti e Cifra de Vigenère, que foram associados a diversos tópicos da Matemática, tais como: montagem de tabelas, noções de geometria espacial, sequências, funções afim, probabilidade, noções de circunferência.

CC BY

REMUNOM
ISSN 2178-6925

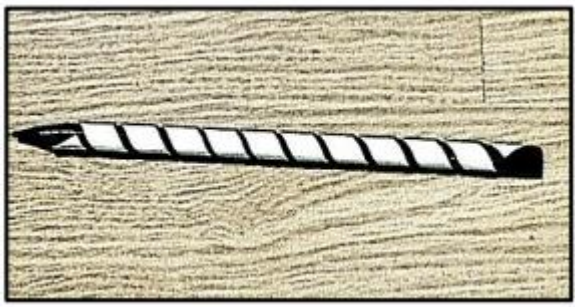
Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

Um dos muitos artefatos utilizados a caráter militar durante a antiguidade, o bastão de Licurgo, serve atualmente como instrumento de auxílio para o ensino acerca da criptografia bem como também como forma de aplicação de conceitos matemáticos, conforme afirma Rodrigues (2024, p. 47) ao detalhar o material com termos matemáticos como “um prisma cuja base é um polígono regular, de modo que, ao redor de suas faces retangulares enrolamos uma tira de papel ou outro material para escrita e escrevemos uma mensagem ao longo do eixo longitudinal”.

O autor anterior utiliza do bastão de Licurgo aplicando o exercício de codificação e decodificação de mensagens, porém sem o uso do bastão na parte da decodificação, tendo em vista que o intuito era fazer com que seus alunos percebessem o padrão em que a mensagem se encontrava, para assim determinar qual a base do prisma utilizado para codificar a mensagem.

Para a explicação da cifra por transposição Santos (2016) utiliza do bastão de Licurgo para ter a mensagem pré-codificada e a partir desta inserir o texto em uma tabela e aplicar a mudança de colunas nesta tabela. A autora cita ainda a utilização de um bastão de Licurgo feito em sala, utilizando de materiais de fácil acesso, tais quais, um lápis como bastão, tiras de papel e uma caneta para escrever a mensagem.

Figura 12: Bastão de Licurgo feito com lápis



Fonte: Santos (2016)

Outro método de codificação bastante citado e atrelado ao ensino da Matemática é a Cifra de Cesar que devido ao padrão de mudança cíclica do alfabeto pode ser bastante associada a ideia de função afim, Silva (2021) utiliza do método como uma forma de desafio a seus alunos apresentando um pequeno parágrafo

CC BY

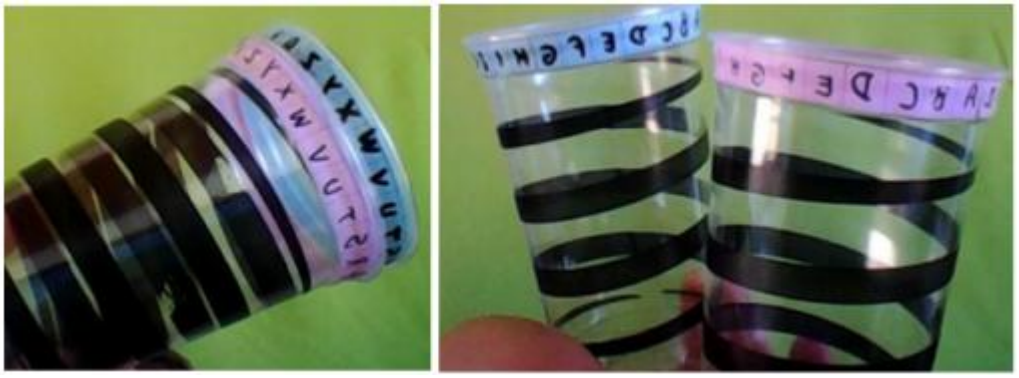
REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

codificado e dando-lhes a missão de decodifica-lo, em sequência a autora apresenta a função afim f(x) = x + 3 onde cada letra do alfabeto é associada a um número de 1 a 26, que coincidia com a codificação do parágrafo inicialmente proposto.

Silva (2021) apresenta a utilização de um material prático denominado kit de encriptação, feito com materiais de fácil acesso (copos descartáveis, fitas coloridas e caneta), por meio desse material os alunos podem representar a codificação de acordo com a Cifra de Cesar mantendo um copo com o alfabeto corrente e outro com a função a qual foi utilizada para codificar cada letra do alfabeto.

Figura 13: Kit de encriptação



Fonte: Silva, Ana (2021)

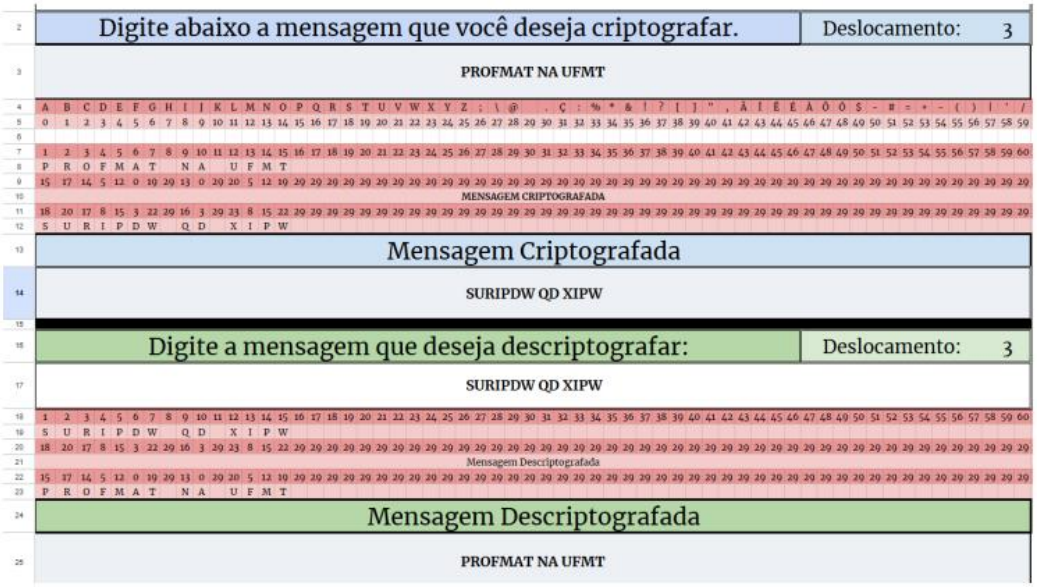
Barzan (2025) demonstra a utilização do código de Cesar como uma forma alternativa de trabalhar o uso da tecnologia em sala, para isto o autor desenvolveu com os alunos uma planilha eletrônica com os devidos códigos de maneira que uma coluna codificaria automaticamente a outra coluna seguindo uma determinada função.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

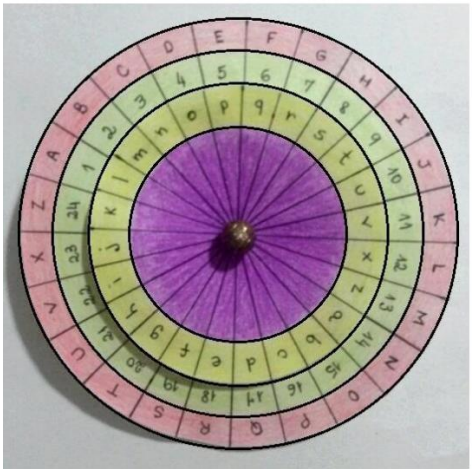
Figura 14: Código de Cesar em planilha eletrônica



Fonte: Barzan (2025)

Santos (2016) aborda, dentre outros meios, sobre a utilização do Disco de Alberti em sala de aula, a autora primeiramente cita sobre a construção do material e como este feito é útil para relembrar noções básicas da geométrica com os alunos, mais especificamente ao abordar sobre o círculo e seus elementos.

Figura 15: Disco de Alberti feito com papel



Fonte: Santos (2016)

A mesma lista ainda que após a confecção dos discos os alunos utilizaram destes para resolver problemas diretamente associados a Matemática com diversos conteúdos, tais como: “números naturais, números primos, múltiplos, divisores,

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

MMC, MDC, expressões numéricas envolvendo raiz quadrada e potência e o algoritmo da divisão" (SANTOS, 2016, p. 69).

Outro dos métodos utilizado foi a Cifra de Vigenère, sendo esta muito associada na Matemática a tópicos relacionados a localização, como encontrar dados em tabelas ou mesmo plano cartesiano, Póvoa (2019) apresentou como proposta de aula a divisão dos alunos em grupos e a aplicação do código entre eles com o objetivo de codificar e decodificar mensagens.

Apresentando outra forma de utilizar da Cifra de Vigenère e seguindo a forma como o mesmo abordou o código de Cesar, Barzan (2025) aborda acerca da construção e utilização de uma planilha eletrônica que visa codificar de maneira automatizada seguindo fórmulas matemáticas e palavras chave.

Figura 16: Cifra de Vigenère em planilha eletrônica



Fonte: Barzan (2025)

5. Considerações Finais

Por meio do estudo bibliográfica, foi possível compreender a utilização de pontos históricos da Criptografia como um recurso didático de extremo valor no

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

ensino da Matemática em diversos de seus conteúdos. As análises documentais feitas apresentam ideias de vários autores quanto ao uso da codificação e decodificação de mensagens, visando apresentar a aplicabilidade daqueles conteúdos na prática.

As dissertações com as quais este artigo dialoga abordam sobre a explicação não apenas teórica dos conteúdos, os mesmos incluem exemplos práticos realizados pelos próprios alunos fazendo uso da codificação e decodificação realizada por civilizações passadas. Tal fato corrobora com a participação dos alunos no aprendizado não só dos conteúdos matemáticos, mas também históricos e até mesmo tecnológicos.

É claro que a utilização da História da Criptografia, assim como a utilização de qualquer outro recurso, necessita de um certo tempo para o professor se preparar tanto no que se refere a associação com o conteúdo que se visa trabalhar quanto na preparação de matérias, porém por meio dos relatos abordados nas dissertações analisadas para a elaboração deste artigo ficou evidente que fazer uso da codificação e decodificação de mensagens é uma ótima maneira de englobar a Matemática com sua história, aplicabilidade e mesmo tecnologia.

Diante de tudo explanado, espera-se que este artigo seja uma forma de apresentar aos professores uma breve abordagem acerca da história da Criptografia e também da utilização da História da Matemática como recurso metodológico, bem como apresentar algumas das muitas formas de abordar a associação da codificação de mensagens com conteúdos matemáticos tanto de nível fundamental quanto médio, tais como: noções de geometria plana e espacial, funções, localização e operações com números naturais.

Referências

BARZAN, Fabricio Antonio. **Explorando Elementos da Criptografia RSA no Processo Educacional**. Dissertação (Mestrado Profissional em Matemática – PROFMAT) – Universidade Federal de Mato Grosso, Cuiabá - MT 2025.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

CAPES. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. **Portal de Periódicos da Capes**. Brasília, 2025. Disponível em: https://www.periodicos.capes.gov.br/. Acesso em: 8 set. 2025.

CIMINO, Al. **A História da Queda dos Códigos Secretos: dos antigos códigos secretos à criptografia quântica**. Traduzido por Maria Beatriz de Medina. São Paulo: M,Books Brasil Editora, 2018.

FIORENTINI, D.; PASSOS, C. L. B; LIMA, R. C. R. (Orgs.). **Mapeamento da pesquisa acadêmica brasileira sobre o professor que ensina matemática: período 2001 –2012**. Campinas, SP: FE/UNICAMP, 2016.

HEFEZ, Abramo. **Aritmética**. 3ª edição – Rio de Janeiro: SJM – Sociedade Brasileira de Matemática, 2022.

ORDONEZ, Edward David Moreno; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em software e hardware**. 1. ed. São Paulo: Novatec, 2005.

PÓVOA, Thiago Marques Esteves. **Estudo sobre os Principais Aspectos da Criptografia Simétrica e Assimétrica ao longo da História**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade de Brasília (Unb), Brasília, 2019.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

QUARESMA, Pedro; LOPES, Elsa. **Criptografia**. p. 1-8, 2007. Disponível: https://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/artigo-gazeta08.pdf. Acesso em: 9 nov. 2025

RANK, Michael. **Espiões, espionagem e operações secretas: da Grécia Antiga à Guerra Fria**. Traduzido por Shana Marcele Oliveira e Silva. Babelcube Inc., 2015.

RODRIGUES, Isac Rosa. **Uso de ferramentas de criptografia no ensino de Matemática para os ensinos fundamental II e médio: propostas de atividades**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade do Estado de Mato Grosso (UNEMAT), Sinop – MT, 2024.

SANTOS, Ana Paula Ferreira dos. **A criptografia no ensino fundamental II: contexto histórico, cifras simétricas, aplicações de conteúdos matemáticos e muitas outras curiosidades**. Dissertação (Mestrado em Matemática) – Universidade Estadual do Norte Fluminense Darcy Ribeiro. Centro de Ciência e Tecnologia. Laboratório de Ciências Matemáticas. Campos dos Goytacazes - RJ, 2016.

CC BY

REMUNOM
ISSN 2178-6925

Received: 13/08/2026 - **Accepted:** 08/09/2026
Vol: 13.19
DOI: 10.66104/pebwgw42
Pages: 1-33

SILVA, Ana Lourdes Moreno Rodrigues. **A criptografia como estímulo aprendizagem matemática**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Estadual do Sudoeste da Bahia, Vitoria da Conquista, 2021.

SILVA, Ana Lourdes Moreno Rodrigues; PEROVANO, Ana Paula; SILVA, Fernando dos Santos. A Criptografia como motivação para a aprendizagem matemática. **REMAT: Revista Eletrônica da Matemática**, Bento Gonçalves, RS, v. 9, n. 1, p. e2002, 23 de fevereiro de 2023.

SILVA, Andresa Laurett da. **Criptografia e algumas aplicações em sala de aula**. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Santa Catarina, Blumenau, 2021.

SINGH, Simon. **O livro dos códigos: a ciência do sigilo – do antigo Egito à criptografia quântica**. Tradução de Jorge Calif. 14ª ed. Rio de Janeiro: Record, 2022.

TAKATA, Guilherme Ohta. **A criptografia moderna**. Revista Resgates, v. 3, n. 1, p. 83–92, 2017. Disponível em: https://static1.squarespace.com/static/637bb31bc82d6a0e64a33d3d/t/6470f6db2d5c8b1814aba6c2/1722006373009/stockler-2017-revista-resgates.pdf. Acesso em: 27 maio. 2025

TKOTZ, Viktoria. **Criptografia: Segredos Embalados para Viagem**. São Paulo: Novatec Editora, 2024.

CC BY