

ENGENHARIA DIDÁTICA: UMA EXPERIÊNCIA COM O TEMA CRIPTOGRAFIA

Clarissa de Assis Olgin¹

ULBRA

Claudia Lisete de Oliveira Groenwald²

ULBRA

RESUMO

Este artigo apresenta uma Engenharia Didática com o tema Criptografia para o desenvolvimento de atividades didáticas que aliem os conteúdos matemáticos do Ensino Médio a esse tema e, que incentivem o manuseio de calculadoras científicas no Ensino de Matemática. Hoje, a Criptografia é utilizada em auditorias eletrônicas, na autenticação de ordens eletrônicas de pagamento, no código de verificação do ISBN, nos navegadores de Internet, entre outras situações do dia a dia. Este trabalho justifica-se porque é importante que o professor trabalhe com temas atuais, proporcionando, ao educando, o contato com as tecnologias, entre elas a calculadora. Os resultados apontam que o tema Criptografia possibilita o desenvolvimento de atividades didáticas para exercitar e revisar conteúdos desenvolvidos em sala de aula, através de atividades de codificação e decodificação, envolvendo os conteúdos matemáticos do Ensino Médio. Esse artigo está vinculado ao Grupo de Estudos Curriculares em Educação Matemática (GECEM) e ao convênio ULBRA – HP Calculadoras.

Palavras-Chave: Educação Matemática. Engenharia Didática. Criptografia.

ABSTRACT

This paper presents a Didactic Engineering with the theme Cryptography for the development of didactic activities that cover mathematics contents taught in High School considering the theme and that promote the use of scientific calculators in the

¹ clarissa_olgin@yahoo.com.br

² claudiag@ulbra.br

teaching of Mathematics. Today, cryptography is used in electronic audits, in the authentication of electronic payment orders, ISBN verification codes, Internet browsers and other daily applications. This study is justified in the light of the importance to provide the means for the teacher to work using current topics, affording the pupil the contact with technologies, among which the calculator. The results obtained indicate that the theme Cryptography allows developing didactic activities that put to practice and review contents developed in the classroom based on activities involving coding and decoding actions and mathematics contents taught in High School. This paper is part of the efforts conducted by the Group of Curricular Studies on Mathematics Education (GECEM) and a partnership Lutheran University of Brazil (ULBRA) established with HP Calculadoras.

Keywords: Mathematical Education, Didactic Engineering, Cryptogaphy.

INTRODUÇÃO

O ponto de referência do processo de ensino e aprendizagem, da Matemática, deve ser a abordagem de assuntos de interesse do aluno, que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos. A Matemática se torna interessante para a aprendizagem quando desenvolvida de forma integrada e relacionada a outros conhecimentos, e o tema Criptografia apresenta-se como motivador e gerador de situações didáticas que permitem o aprofundamento dos conteúdos desenvolvidos no Ensino Médio, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas.

Este artigo apresenta uma Engenharia Didática com o tema Criptografia para o desenvolvimento de atividades didáticas para o Currículo de Matemática do Ensino Médio. Segundo Tamarozzi (2001), este tema permite ao professor de Matemática desenvolver atividades didáticas de codificação e decodificação, para revisar, reforçar e aprofundar os conteúdos matemáticos do Ensino Médio.

O tema Criptografia tem um papel importante nos dias atuais, pois é utilizado nos recursos humanos (auditoria eletrônica e lacre de arquivos de pessoal e pagamentos), em compras e vendas (autenticação de ordens eletrônicas de pagamento), nos processos jurídicos (transmissão digital e custódia de contratos), na automação de escritórios (autenticação e privacidade de informações), no código de verificação do ISBN, nos navegadores de Internet, entre outras situações da vida cotidiana.

1. CURRÍCULO DE MATEMÁTICA NO ENSINO MÉDIO

Segundo a Lei de Diretrizes e Bases da Educação Nacional (BRASIL, 1996), o Ensino Médio apresenta as seguintes finalidades:

- *a consolidação e o aprofundamento dos conhecimentos adquiridos no ensino fundamental, possibilitando o prosseguimento de estudos;*

- *a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação ou aperfeiçoamento posteriores;*
- *aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico;*
- *a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina.*

Na etapa final da Educação Básica, espera-se que o estudante esteja preparado para atuar na sociedade, na qual está inserido, de forma efetiva, sabendo se comunicar claramente, resolver problemas do dia-a-dia e do trabalho, tomar decisões, trabalhar com eficiência e em cooperação.

Encontra-se, nas Orientações Curriculares para o Ensino Médio (BRASIL, 2006), que o aluno deve ser capaz de utilizar a Matemática: na resolução de problemas do cotidiano; para modelar fenômenos das distintas áreas do conhecimento; para compreender a Matemática como conhecimento social e construído ao longo da história; para entender a importância da Matemática no desenvolvimento científico e tecnológico.

Nesse sentido, para poder alcançar as finalidades do ensino, é necessário um currículo que atenda aos princípios referidos. Neste trabalho, o conceito de currículo está fundamentado em Coll (1999):

Currículo é o projeto que preside as atividades educativas escolares, define suas intenções e proporciona guias de ação adequadas e úteis para os professores, que são diretamente responsáveis pela sua execução. Para isso, o currículo proporciona informações concretas sobre o que ensinar, quando ensinar, como ensinar e que, como e quando avaliar (1999, p. 45).

Ainda, conforme o autor, o currículo é a realização do planejamento curricular, tomada de decisão dos objetivos que se deseja alcançar, organização dos conteúdos, elaboração das estratégias didáticas, definição da metodologia de ensino. Portanto, é “a estratégia para a ação educativa” (D’AMBROSIO, 1997, p. 68).

Outro ponto chave para a realização de uma aprendizagem significativa, para Coll (1999), é a funcionalidade:

A educação escolar deve sempre ocupar-se de que os conhecimentos adquiridos – conceitos, habilidades, valores, normas etc – sejam funcionais, isto é, possam ser efetivamente utilizados quando as circunstâncias nas quais o aluno se encontrar assim exigirem (1999, p. 55).

O currículo deve sempre levar em consideração os aspectos de funcionalidade dos conteúdos para os alunos, em que se proponham atividades didáticas que levem os alunos a visualizarem a aplicabilidade dos mesmos, seja em situações dentro ou fora do ambiente escolar, no cotidiano ou na história (COLL, 1999).

A escolha de temas para o Ensino Médio deve possibilitar o uso de conteúdos de Matemática, permitindo que o aluno aprofunde e exercite os conteúdos já trabalhados em séries anteriores, crie estratégias de resolução de problemas, tenha autonomia na resolução das atividades didáticas e trabalhe em grupo, buscando aprimorar a sua formação acadêmica e social. Buscando, nesse sentido, alcançar as indicações citadas anteriormente.

Trabalhar com o tema proposto pode permitir que o estudante desenvolva habilidades que podem ser utilizadas no ambiente de trabalho e no convívio em sociedade, pois é um tema atual, de grande utilização, aplicado a várias situações da vida moderna e adapta-se aos conteúdos do Currículo de Matemática do Ensino Médio (CANTORAL, 2003; GROENWALD e FRANKE, 2008; GROENWALD, FRANKE e OLGIN, 2009; TAMAROZZI, 2001).

Uma forma de estimular o desenvolvimento dessas habilidades é “propondo aulas de Matemática que estimulem a participação, valorizem a iniciativa, os avanços individuais, o crescimento coletivo, o respeito mútuo” (PIRES, 2000, p.156).

Raths apud Coll (1999) propõe doze princípios para ajudar o professor a justificar a necessidade de se incluir ou não uma atividade no Currículo, afirmando que uma atividade é preferível a outra se:

1. *permite ao aluno tomar decisões razoáveis quanto ao modo de desenvolvê-la e verificar as consequências da sua escolha;*
2. *atribuir ao aluno um papel ativo em sua realização;*
3. *exigir do aluno uma pesquisa de ideias, processos intelectuais, acontecimentos ou fenômenos de ordem pessoal ou social e estimulá-lo a comprometer-se com a mesma;*
4. *obrigar o aluno a interagir com sua realidade;*

5. *puder ser realizada por alunos de diversos níveis de capacidade e com interesses diferentes;*
6. *obrigar o aluno a examinar num novo contexto uma ideia, conceito, lei, que já conhece;*
7. *obrigar o aluno a examinar ideias ou acontecimentos que normalmente são aceitos sem discussão pela sociedade;*
8. *colocar o aluno e o educador numa posição de sucesso, fracasso ou crítica;*
9. *obrigar o aluno a reconsiderar e revisar seus esforços iniciais;*
10. *obrigar a aplicar e dominar regras significativas, normas ou disciplinas;*
11. *oferecer ao aluno a possibilidade de planejá-la com outros, participar do seu desenvolvimento e comparar os resultados obtidos;*
12. *for relevante para os propósitos e interesses explícitos dos alunos. (1999, p. 80-81)*

Observando o exposto acima, entende-se que o tema Criptografia está fortemente ligado aos princípios 1, 2, 3, 4, 6 e 11. Ao primeiro princípio, devido à possibilidade que oferece de elaborar atividades didáticas em que o aluno pode criar estratégias de resolução de problemas e verificar a sua validade. O segundo princípio refere-se ao fato das atividades didáticas aliarem o tema aos conteúdos matemáticos do Ensino Médio, possibilitando aos alunos autonomia para verificar o melhor caminho para encontrar a solução, permitindo que eles mobilizem seus conhecimentos e se tornem mais ativos no processo de ensino. O princípio três também pode ser percebido nas atividades didáticas com o tema Criptografica, pois exigem que os alunos se concentrem na resolução, criem estratégias e as verifiquem. A Criptografia oportuniza atividades didáticas que estão presentes na vida cotidiana e que envolvem conteúdos matemáticos como, por exemplo, atividade de criptogramas e Código ISBN, o que corresponde ao princípio quatro. O princípio seis pode ser percebido no fato da Criptografia proporcionar o desenvolvimento de atividades didáticas que possibilitam revisar e reforçar os conteúdos já trabalhados, tais como, princípios fundamentais da aritmética, funções e matrizes, além de explorar novos conteúdos, no Currículo de Matemática do Ensino Médio como, por exemplo, a atividade envolvendo o Código de verificação ISBN, que explora o conteúdo de aritmética modular. O trabalho em grupo é essencial, porque permite a discussão dos caminhos para a resolução.

Segundo Groenwald e Ruiz (2006, p. 21):

As pessoas que trabalham em grupo possuem mais idéias, mais energia e mais criatividade para enfrentar obstáculos do que uma pessoa só, além de reforçar as competências individuais. Logo, o resultado de um trabalho em grupo é mais produtivo que a soma das competências individuais.

As atividades envolvendo o tema Criptografia fazem com que o aluno tenha que compreender os processos de resolução do colega e vice-versa, para entender a lógica de resolução do outro, princípio onze, além de possibilitar o trabalho em grupo.

Trabalhar com esse tema, aliado aos conteúdos matemáticos do Ensino Médio, pode ser uma estratégia para o professor de Matemática revisar e reforçar alguns conteúdos, possibilitando ao estudante dessa etapa do Ensino Básico conhecer um pouco da história da Criptografia e ampliar seus conhecimentos referentes aos conteúdos desenvolvidos nas atividades didáticas propostas.

1.1 Criptografia: história e aplicações

O nome Criptografia vem das palavras gregas *kriptós* que significa escondido, oculto e *graphein* que significa escrita (SINGH, 2003). Consiste em codificar informações, usando uma chave, antes que essas sejam transmitidas, e em decodificá-las, após a recepção, através de um processo de codificação. A criptografia torna possível o envio de mensagens incompreensíveis para uma terceira pessoa que, eventualmente, venha a interceptá-las, mas que poderão ser lidas pelo seu destinatário, que conhece o critério para decifrar o texto encriptado (TERADA, 1988; TAMAROZZI, 2001; SCHEINERMAN, 2003; ZATTI e BELTRAME, 2009).

Para Tamarozzi (2001), o princípio básico da criptografia é encontrar uma transformação (função) injetiva f entre um conjunto de mensagens escritas em um determinado alfabeto (de letras, números ou outros símbolos) para um conjunto de mensagens codificadas. O desafio de um processo criptográfico é ocultar eficientemente os mecanismos (chaves) para a inversão de f , de modo que estranhos não possam fazê-lo.

Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são

textos cifrados ou criptogramas. O processo de converter um texto comum em cifrado é chamado cifrar ou criptografar e o processo inverso, de converter um texto cifrado em comum, é chamado decifrar (ZATTI E BELTRAME, 2009).

A criptografia é uma arte bastante antiga, presente desde o sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. E o mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século.

Depois da segunda guerra mundial, com a invenção do computador, a área realmente floresceu, incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços na decifração de códigos utilizados. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

O citale espartano foi o primeiro aparelho criptográfico militar, utilizado durante o século V a.C.. Era um bastão de madeira, onde se enrolava uma tira de couro e se escrevia a mensagem em todo o comprimento desse bastão. Para enviar a mensagem, de forma despercebida, a tira de couro era desenrolada do citale e utilizada como um cinto, com a mensagem voltada para dentro. Como na tira de couro a mensagem ficava sem sentido para decifrá-la, era necessário que o receptor tivesse um citale de mesmo diâmetro para enrolar a tira de couro e ler a mensagem.

Outro tipo de cifra foi utilizada por Júlio César, que consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto. César utilizava o alfabeto normal para escrever a mensagem e o alfabeto cifrado para codificar a mensagem que mais tarde seria enviada. Esse método de criptografia ficou conhecido como Cifra de César.

Como as cifras de substituição monoalfabéticas eram muito simples e facilmente decifradas por criptoanalistas, através da análise de frequência de cada letra, no texto cifrado, surgiu a necessidade de criar novas cifras, mais elaboradas e mais difíceis de serem descobertas. A solução encontrada, no século XVI, pelo diplomata francês Blaise Vigenère, foi uma cifra de substituição polialfabética. Um exemplo de cifra de substituição polialfabética foi a Cifra de Vigenère, que utilizava 26 alfabetos cifrados diferentes para codificar uma mensagem.

Alberti, citado por Singh (2003), foi o criador da primeira máquina criptográfica, o Disco de Cifras, é um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado. Porém seu inventor sugeriu que fosse mudada a disposição do disco durante uma mensagem, o que iria gerar uma cifra polialfabética, o que dificultaria a sua decodificação, pois desse modo ele estaria mudando o modo de mistura durante a cifragem e isso tornaria a cifra difícil de ser quebrada.

Em 1918, o inventor Artur Scherbius e seu amigo Richard Ritter fundaram uma empresa. Um dos projetos de Artur Scherbius era substituir os sistemas criptográficos, usados na primeira guerra mundial. Então, utilizando a tecnologia do século XX, ele desenvolveu uma máquina criptográfica, que era uma versão elétrica do disco de cifras. Essa máquina recebeu o nome de Enigma. Para decifrar uma mensagem da Enigma, o destinatário precisaria ter outra Enigma e uma cópia do livro de códigos, contendo o ajuste inicial dos misturadores para cada dia.

Em 1943, foi projetado o Colossus, computador utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela Enigma. O Colossus deu início a uma era moderna da criptografia, em que os computadores eram programados com chaves de codificação muito mais complexas do que as utilizadas pela Enigma. Essa nova técnica de criptografia era de uso exclusivo do governo e de militares para guardar informações.

Como as cifras de substituição sofriam constantes ataques dos criptoanalistas, começaram a utilizar os computadores, os quais utilizavam criptografias complexas, mas não apresentavam, ainda, a segurança necessária para não serem invadidos por pessoas que não deveriam ter acesso aos códigos de criptagem contidos neles. Para solucionar esse problema, foram criados dois algoritmos de codificação: o DES (sistema de chave secreta) e o RSA (sistema de chave pública).

Ao longo da história, foram criados mecanismos de codificação, denominados códigos, cifras e senhas usados para manter o segredo das mensagens a serem enviadas. Um exemplo de aplicação da Criptografia foi a Cifra de substituição monoalfabética, denominada Cifra do Chiqueiro que foi utilizada pelos maçons livres

para guardar seus segredos (SINGH, 2003). A cifra consiste em substituir uma letra por um símbolo, seguindo o padrão apresentado na figura 1.

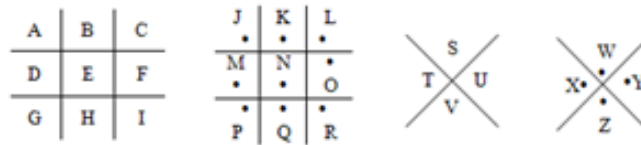


Figura 1: exemplo do padrão utilizado pela Cifra do Chiqueiro.

A codificação da Cifra do Chiqueiro é realizada encontrando a posição da letra em uma das quatro grades da figura 1 e desenhando a porção da grade que representa a letra a ser codificada, por exemplo, a letra **E** corresponde ao símbolo .

Outro exemplo de codificação foi utilizado pelos jovens apaixonados da Inglaterra vitoriana não podiam expressar seu amor publicamente, então começaram a trocar mensagens codificadas através dos jornais, em colunas dedicadas às mensagens dos leitores. Essas colunas ficaram conhecidas como “colunas de óbito” (SINGH, 2003). Charles Babbage e seus amigos Sir Wheatstone e o barão Lyon Playfair foram os criadores da Cifra de Playfair, que substitui cada par de letras da mensagem a ser codificada por outro par de letras. Para codificar, primeiramente escolhe-se uma palavra-chave, por exemplo, ULBRA. Antes da cifragem, as letras do alfabeto são escritas em um quadrado 5X5, começando com a palavra chave e combinando as letras I e J em um único elemento, conforme a figura 2.

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

Figura 2: quadro da Cifra de Playfair.

A mensagem original é escrita em pares de letras, ou dígrafos. As duas letras em qualquer dígrafo devem ser diferentes, o que se consegue inserindo, por exemplo, uma letra *x* caso apareçam letras iguais ou se o número de letras for ímpar. A cifragem começa da seguinte forma: se as duas letras estiverem na mesma linha, elas são substituídas pela letra imediatamente à direita de cada uma delas, se

uma delas estiver no final da linha, ela é substituída pela letra que está no começo da linha. Se ambas as letras estiverem na mesma coluna, elas serão substituídas pela letra que está imediatamente abaixo de cada uma e, neste caso, se uma das letras for a última letra da coluna, será substituída pela letra que está no topo da coluna.

Se as letras no dígrafo não estiverem nem na mesma linha, nem na mesma coluna, seguimos a seguinte regra: para cifrar a primeira letra olhe ao longo de sua linha até chegar à coluna em que está a segunda letra; a letra que estiver nesta intersecção irá substituir a primeira letra. Para cifrar a segunda letra, utilize o mesmo raciocínio.

A figura 3 apresenta um exemplo de codificação utilizando a cifra referida.

Texto original	A vida é bela
Texto original em pares	AV – ID – AE – BE – LA
Texto Codificado	UZ – PI – BG – EK – BU

Figura 3: exemplo de cifragem utilizado pela Cifra de Playfair.

Para codificar o par AV, tem-se que, como não estão na mesma linha e nem na mesma coluna, utilizar-se a regra de olhar primeiro ao longo da linha até chegar à coluna onde está a segunda letra, e a letra que estiver na intersecção irá substituir a primeira letra. Para cifrar a segunda letra, utiliza-se o mesmo raciocínio, conforme figura 4.

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

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

Figura 4: exemplo da cifragem do par AD utilizando a Cifra de Playfair.

Em 1918, foi introduzido o ADFGVX, uma cifra de guerra que se acreditava dar maior segurança às mensagens a serem enviadas. Foi utilizada pelos alemães, que acreditavam fosse imbatível, mas o criptoanalista Georges Painvin quebrou a

Cifra ADFGVX e descobriu onde os alemães atacariam (SINGH, 2003). As letras ADFGVX foram escolhidas porque quando traduzidas para os pontos e traços do código Morse diminui a possibilidade de erros durante a transmissão.

A Cifra ADFGVX para codificar utiliza uma grade 6x6, preenchida com 36 quadrados, onde se coloca as 26 letras do alfabeto e 10 algarismos. Na primeira linha e coluna colocam-se as letras A, D, F, G, V e X, conforme figura 5.

	A	D	F	G	V	X
A	8	p	3	d	l	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Figura 5: quadro da Cifra ADFGVX.

Inicia-se a codificação pegando cada letra da mensagem a ser enviada, localizando a sua posição na grade, e substitui-se pelas letras da linha e da coluna, por exemplo, **d** será substituído por **AG**. Uma mensagem codificada por esta cifra ficará conforme a figura 6.

Palavra original	Lógica
Palavra codificada	DADGGVVGFGDV

Figura 6: exemplo de codificação da Cifra ADFGVX.

Para cifrar a letra L, localiza-se sua posição na grade e se substitui pelas letras que estão na sua linha e coluna, como mostra a figura 7.

	A	D	F	G	V	X
A	8	p	3	d	l	N
D	l	t	4	o	A	H
F	7	k	b	c	5	Z
G	j	u	6	w	G	M
V	x	s	v	i	R	2
X	9	e	y	0	F	Q

➔ I = DA

Figura 7: exemplo de codificação da Cifra ADFGVX.

Percebe-se que a Criptografia, no decorrer da história, vem sendo utilizada para fins militares e pessoais. E nos dias atuais, esse tema vem sendo utilizado em

auditoria eletrônica, na autenticação de ordens eletrônicas de pagamento, nos navegadores de Internet, entre outras situações, o que demonstra ser um tema que apresenta diversas aplicabilidade (TERADA, 1988).

Segundo Tamarozzi (2001) a Criptografia é um tema atual que possibilita o desenvolvimento de atividades didáticas, que podem ser desenvolvidas no Ensino Básico, que levem os alunos a aprimorarem seus conhecimentos, e que permite que o professor de Matemática desenvolva atividades didáticas de matemática de codificação e decodificação. Reforça GROENWALD e FRANKE (2008) que esse tema permite que os alunos adquiram as habilidades e competências de resolver problemas, criar estratégias de resolução, autonomia durante o processo de aprendizagem, permitindo que eles se tornem mais autoconfiantes e concentrados na realização das atividades propostas.

As atividades propostas neste artigo possibilitam o uso de calculadoras na sala de aula. Segundo Krist (1995), as calculadoras podem servir de laboratório para os alunos, pois com esse instrumento eles podem realizar experiências e desenvolverem suas próprias idéias e estratégias. Ainda, segundo os Parâmetros Curriculares Nacionais (1998), o professor de matemática deve fazer uso da calculadora sempre que achar necessário ao aprendizado do aluno, porque ela contribui para um repensar do processo de aprendizagem da disciplina de Matemática.

2. PROBLEMA DA PESQUISA

O problema de pesquisa, dessa investigação foi: Como desenvolver uma Engenharia Didática que envolva os conteúdos matemáticos do Ensino Médio com o tema Criptografia?

3. HIPÓTESES DA PESQUISA

Por ser uma Engenharia Didática a pesquisa apresentou as seguintes hipóteses:

- existe relação entre o tema Criptografia e os conteúdos do Ensino Médio;
- através das atividades didáticas, com o tema Criptografia, o aluno é capaz de aprofundar e revisar os conteúdos matemáticos do Ensino Médio e conhecer o tema.

4. OBJETIVOS DA PESQUISA

Este trabalho teve como objetivo geral investigar a possibilidade de implementar uma Engenharia Didática para o desenvolvimento do tema Criptografia aliado aos conteúdos de Matemática do Ensino Médio.

Para alcançar o objetivo geral da pesquisa foram traçados os seguintes objetivos específicos: investigar a relação entre a Criptografia e os conteúdos matemáticos do Ensino Médio; pesquisar atividades didáticas com o tema Criptografia para o Ensino Médio; implementar (desenvolver, aplicar e avaliar) um experimento com alunos do Ensino Médio com a sequência didática desenvolvida; e investigar se o aluno estabelece relações com o tema Criptografia através das atividades didáticas aplicadas.

5. METODOLOGIA DA PESQUISA

A metodologia de pesquisa adotada foi a Engenharia Didática, a qual apresenta dois níveis de pesquisa, a microengenharia e a macroengenharia (MACHADO, 2008). A pesquisa, em microengenharia, estuda um determinado assunto, preocupando-se com os fenômenos que ocorrem em sala de aula. A macroengenharia compõe a complexidade da microengenharia com os fenômenos do processo de ensino e aprendizagem (ARTIGUE, 1995). Esta pesquisa se baseia em uma microengenharia, pois busca desenvolver uma Engenharia Didática que envolva os conteúdos matemáticos do Ensino Médio com o tema Criptografia.

Também é importante ressaltar que a metodologia de Engenharia Didática possui uma validação essencialmente interna, que possibilita a confrontação da análise *a priori* com a *posteriori* (ARTIGUE, 1995).

A Engenharia Didática, também, caracteriza-se por apresentar variáveis didáticas, que podem ser variáveis macro-didáticas ou globais, as quais se referem à organização geral da engenharia, ou variáveis micro-didáticas ou locais, que se referem à organização de uma fase da engenharia. As variáveis macro-didáticas, nesse trabalho, foram o tema Criptografia e o Currículo de Matemática do Ensino Médio, pois possibilitam o desenvolvimento de atividades didáticas que levem o estudante a revisar e reforçar conteúdos abordados anteriormente. As variáveis micro-didáticas foram os conteúdos de Matemática envolvidos nas atividades propostas (ARTGUE, 1995).

Essa engenharia exige que o educador realize um projeto que desafie a sua criatividade. Nesse sentido, apresenta-se o tema Criptografia como motivador e desencadeador de situações-problema, relacionando os conceitos matemáticos e as situações didáticas propostas pelo educador.

Segundo Artigue (1995, p.38), uma Engenharia Didática é composta por quatro fases consecutivas, que se dividem em: análises preliminares; concepção e análise *a priori*; aplicação de uma sequência didática e a análise *a posteriori* e validação.

Dentro da pesquisa em Engenharia Didática, na fase das análises preliminares, é realizada a análise do objeto em estudo, ou seja, é feito um referencial teórico que irá fundamentar o projeto. Nessa fase, o educador deve levar em consideração as constatações empíricas, concepções do aprendiz e compreender as condições nas quais será exposta a experiência. Nessa fase da pesquisa, também se deve levar em consideração:

A análise epistemológica dos conteúdos contemplados pelo ensino; a análise do ensino atual e de seus efeitos; a análise da concepção dos alunos, das dificuldades e dos obstáculos que determinam sua evolução; a análise do campo dos entraves no qual vai se situar a efetiva realização didática (MACHADO, 2008, p. 238).

O levantamento dessas questões deve considerar o objetivo da pesquisa, pois o pesquisador deve ter clareza sobre o que realmente deseja pesquisar

(MACHADO, 2008). Com relação à pesquisa, na fase das análises preliminares, foi realizada uma pesquisa bibliográfica, com o propósito de investigar o tema Criptografia, sua história e aplicações. Essa fase foi um estudo exploratório, buscando aliar a Criptografia e os conteúdos matemáticos do Ensino Médio, desenvolvendo atividades didáticas, para que o estudante consiga reforçar conteúdos e agir em atividades didáticas com aplicações do tema.

Segundo Artigue (1995), na fase da concepção e análise *a priori*, delimita-se as variáveis didáticas. Nessa fase, buscou-se delimitar e compreender as variáveis didáticas, as quais foram analisadas durante o desenvolvimento da sequência didática, procurando determinar quais são as variáveis relevantes para a pesquisa, buscando uma relação do conteúdo de Matemática do Ensino Médio com as atividades propostas que levem o aluno a adquirir conceitos relevantes sobre o tema.

De acordo com Artigue (1995), as análises *a priori* apresentam uma parte descritiva e uma parte de previsão, referente à situação didática que se pretende aplicar. Isso é reforçado por Machado (2008), o qual afirma que análise *a priori*:

Comporta uma parte de descrição e outra de previsão e está centrada nas características de uma situação didática que se quis criar e que se quer aplicar aos alunos visados pela experimentação (MACHADO, 2008, pg. 243).

O pesquisador deve se preocupar em descrever as características da situação didática, verificar as possibilidades de ação dos alunos e analisar qual seria o comportamento do aluno frente à situação aplicada. Para Machado (2008):

A análise a priori objetiva a consideração do aluno sob dois aspectos: o descritivo e o previsivo. Não há nela, tradicionalmente, lugar para o papel do professor, que, quando aparece, é simplesmente no aspecto descritivo. O aluno é considerado o ator principal (MACHADO, 2008, pg.244).

Nas análises *a priori*, foram descritas as características da situação didática que se pretendia aplicar e procurou-se prever as ações possíveis do estudante durante a situação proposta.

Na fase de experimentação, realizou-se a aplicação da sequência didática, na qual se conseguiu aproximar os resultados práticos da análise teórica. A Engenharia Didática se utiliza das sequências didáticas para construção de um conhecimento

significativo pelo aluno, onde o educador busca novas intervenções com a finalidade de articular diferentes atividades no decorrer de uma unidade didática (PAIS, 2005). Também aplicaram-se os instrumentos da pesquisa e foram realizados registros das observações.

Segundo Pannuti (2004):

A sequência didática é uma outra modalidade organizativa que se constitui numa série de ações planejadas e orientadas com o objetivo de promover uma aprendizagem específica e definida. Essas ações são seqüenciais, de forma a oferecer desafios com o grau de complexidade crescente, para que as crianças possam colocar em movimento suas habilidades, superando-as e atingindo novos níveis de aprendizagem (2004, p. 4).

Segundo Zabala (1998) uma sequência didática é formada por aulas planejadas e analisadas previamente, com o objetivo de verificar situações de aprendizagem envolvendo os conceitos previstos no projeto elaborado pelo educador. A Criptografia é um tema que proporciona ao professor a liberdade de realizar diversas atividades, com graus de complexidade distintos, que busquem desencadear, no aluno, habilidades e competências que o tornem mais autônomo durante o seu processo de ensino e aprendizagem (GROENWALD; FRANKE, 2007).

Na fase das análises *a posteriori*, foram analisados os dados da aplicação da sequência didática, obtidos através de diversos recursos: a observação direta do pesquisador, questionários aplicados nos alunos participantes do experimento, a análise dos registros desses alunos. Através da análise, conseguiu-se identificar e mostrar a realidade da produção dos alunos no desenvolvimento da sequência didática.

A validação foi o processo de verificação dos objetivos pré-estabelecidos no projeto, comparados com a confrontação dos resultados obtidos nas análises *a priori* e *a posteriori* que, segundo Machado (2008), possibilita ao professor/pesquisador avaliar a sua proposta metodológica.

6. FASES DA ENGENHARIA DIDÁTICA COM O TEMA CRIPTOGRAFIA

Apresenta-se a seguir as quatro fases da Engenharia Didática e o Currículo do Ensino Médio.

6.1. Fase das Análises Preliminares

Segundo Pais (2005), para as análises preliminares, é necessária a referência de um quadro teórico, sobre o qual o pesquisador fundamenta suas principais categorias. Considera, também, que, para melhor organizar a análise preliminar, é recomendável proceder a uma descrição das principais dimensões que definem o fenômeno a ser estudado e que se relacionam com o sistema de ensino.

As análises preliminares foram realizadas através de pesquisa em livros didáticos, artigos de congressos, revistas da área de Matemática, buscando aplicações e atividades didáticas do tema em estudo para o Ensino Médio. Nessa fase, também foi realizada a análise de artigos: Revista do Professor de Matemática (RPM), Educação Matemática em Revista – RS, Revista Latinoamericana de Investigación en Matemática Educativa (RELIME), livros didáticos, Banco de Questões das Olimpíadas Brasileiras de Matemática, dissertações de mestrado, artigos de congresso e seminários. O objetivo deste estudo bibliográfico foi pesquisar atividades didáticas que aliassem o tema em estudo aos conteúdos matemáticos do Ensino Médio, para verificar a possibilidade da elaboração de uma sequência didática que permitisse aos alunos revisar e ampliar os seus conhecimentos com relação aos conteúdos abordados.

Como exemplo, dos conteúdos realizados na fase de análises preliminares tem-se a análise referente ao artigo “Código e senhas no Ensino Básico”, das autoras Groenwald, Franke e Olgin, publicado na revista Educação Matemática em Revista, do Rio Grande do Sul, publicado em 2009, onde apresenta aplicações do tema Criptografia ao longo da história, com atividades envolvendo a Cifra de César, a Cifra de Vigenère, a Cifra Chiqueiro e o Código ISBN, que trabalha com aritmética modular, um conteúdo pouco explorado no Ensino Médio.

Após as atividades para introduzir o tema, tem-se atividades didáticas que aliam os temas aos conteúdos matemáticos de função quadrática, função exponencial e função logarítmica. A atividade explorada referente a esse artigo é o

código com função exponencial e logaritmo (figura 8), por ser um conteúdo que apresenta poucas atividades didáticas envolvendo aplicabilidades. Na atividade, as autoras mostram como o professor pode explorar esse conteúdo, trabalhando com imagem da função para codificar, com o cálculo da função inversa exponencial e logarítmica, onde se pretende que o aluno compreenda que as funções exponenciais e logarítmicas são funções inversas.

Primeiro, relaciona-se cada letra do alfabeto a um número, conforme observa-se a seguir.

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

Crie uma mensagem a ser enviada: **MATEMÁTICA**
 Cifre esta mensagem, utilizando a função escolhida.
 Entregue a mensagem cifrada para que seu colega a decifre.
 Seja a função $f(x) = 2^x$, calcula-se a imagem da função para cada algarismo da sequência numérica:

Letra	Sequência Numérica	Imagem da função $f(x) = 2^x$
M	13	$f(x) = 2^x = 2^{13} = 8192$
A	1	$f(x) = 2^x = 2^1 = 2$
T	20	$f(x) = 2^x = 2^{20} = 1048576$
E	5	$f(x) = 2^x = 2^5 = 32$
I	9	$f(x) = 2^x = 2^9 = 512$
C	3	$f(x) = 2^x = 2^3 = 8$

Seja a função inversa $x = \log_2 y$, calcula-se a imagem da função para cada algarismo da sequência numérica:

Sequência Numérica Recebida	Imagem da inversa da função codificadora $x = \log_2 y$	Letra encontrada no alfabeto inicial
8192	$2^x = 8192 \rightarrow x = 13$	M
2	$2^x = 2 \rightarrow x = 1$	A
1048576	$2^x = 1048576 \rightarrow x = 20$	T
32	$2^x = 32 \rightarrow x = 5$	E
8192	$2^x = 8192 \rightarrow x = 13$	M
2	$2^x = 2 \rightarrow x = 1$	A
1048576	$2^x = 1048576 \rightarrow x = 20$	T
512	$2^x = 512 \rightarrow x = 9$	I
8	$2^x = 8 \rightarrow x = 3$	C
2	$2^x = 2 \rightarrow x = 1$	A

(FRANKE; GROENWALD; OLGIN, 2009, p. 47).

Figura 8: exemplo de atividades de Criptografia envolvendo função exponencial e logarítmica.

A atividade didática apresentada pelos autores pode ser um recurso para trabalhar em sala de aula de forma a exercitar e revisar o conteúdo matemático de

função exponencial e logarítmica, onde o professor pode explorar a idéia de função e função inversa em uma mesma atividade.

6.2. Fase da concepção e análise *a priori*

Para realizar a fase de concepção e análise *a priori*, foi necessário utilizar o referencial bibliográfico obtido na fase das análises preliminares, pois foi nessa fase que se verificou que é possível aliar os conteúdos matemáticos do Ensino Médio ao tema Criptografia para o desenvolvimento de atividades didáticas. As atividades didáticas apresentadas pelos autores, na fase das análises preliminares, possibilitaram verificar que é possível elaborar atividades envolvendo o conteúdo de aritmética do Ensino Fundamental, através das atividades de Criptogramas, o conteúdo de funções e matrizes, pois permitem codificar e decodificar as mensagens, utilizando na decodificação o conteúdo de função inversa e matriz inversa. A fase da concepção e análise *a priori* deu-se em dois momentos. O primeiro foi o planejamento e organização da sequência didática, onde as atividades propostas procuraram trabalhar com as aplicações do tema Criptografia, através de atividades envolvendo Cifra de César, Cifra do Chiqueiro e a Cifra de Playfair. Também, apresentou atividades envolvendo criptogramas, para introduzir o tema e revisar os conceitos de Aritmética, já trabalhados no Ensino Fundamental e atividades envolvendo o Dígito Verificador do Código ISBN, visando introduzir o conteúdo de Aritmética Modular. Os conteúdos matemáticos de funções e matrizes foram escolhidos, pois dentre os abordados no Ensino Médio observou-se que o tema em estudo permite explorar esses conteúdos e suas propriedades, de forma a revisar e ampliar os conhecimentos dos alunos para os mesmos, possibilitando-lhes aplicar o conteúdo de função inversa e matriz inversa em atividades didáticas de decodificação.

O segundo momento foi a análise das possíveis resoluções dos alunos às atividades didáticas presentes na sequência elaborada, pois, de acordo com Artigue (1995), na análise *a priori*, descrevem-se as características da situação que se pretende aplicar, procurando prever as ações dos alunos.

A seguir apresentam-se exemplos de análise da possível resolução dos alunos na atividade didática envolvendo o tema Criptografia e os conteúdos de Função Linear e Matrizes.

Atividade 1: Considere a figura 9 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e codifique a mensagem “A vida é bela.”, utilizando o Código com Função Linear, sabendo que a função codificadora é $f(x) = 5x + 1$.

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

Figura 9: quadro do valor numérico de cada letra.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: $A = 1, B = 2, C = 3, \dots$ e $f(x) = 5x + 1$

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: $1 - 22 - 9 - 4 - 1 - 5 - 2 - 5 - 12 - 1$.

Cálculo da imagem de cada algarismo da sequência:

$$f(1) = 5 \cdot 1 + 1 = 6 \quad f(22) = 5 \cdot 22 + 1 = 111 \quad f(9) = 5 \cdot 9 + 1 = 46$$

$$f(4) = 5 \cdot 4 + 1 = 21 \quad f(5) = 5 \cdot 5 + 1 = 26 \quad f(2) = 5 \cdot 2 + 1 = 11$$

$$f(12) = 5 \cdot 12 + 1 = 61$$

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: $6 - 111 - 46 - 21 - 6 - 26 - 11 - 26 - 61 - 6$

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = 5x + 1$ é:

$$f(x) = 5x + 1$$

$$f(x) - 1 = 5x$$

$$\frac{f(x)-1}{5} = x$$

Logo, a função inversa corresponde a $f^{-1}(x) = \frac{x-1}{5}$.

Atividade 2: Considere a tabela da figura 9 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26, que considera como zero a letra Z, e decodifique a mensagem “16 – 3 – 21 – 9 – 43 – 42 – 24 – 27 – 33 – 42 – 39 – 57 – 51 – 54 – 30 – 15 – 55 – 60 – 36 – 27 – 49 – 42 – 36 – 45 – 16 – 3 – 25 – 9 – 13 – 12 – 25 – 36 – 61 – 60 – 1 – 0”, sabendo que a matriz codificadora é a matriz transposta de A e a matriz $A = \begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix}$.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora, transposta de A, que é $A^t = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$.

Em seguida, deverá saber que deve realizar o cálculo da matriz inversa da matriz A^t :

$$A^{-1} = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

Para decodificar, o aluno deverá realizar multiplicação de matrizes, multiplicando a matriz A^{-1} com a matriz AM, que corresponde a matriz da mensagem codificada:

$$A^{-1} \cdot (AM) = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 16 & 21 & 43 & 24 & 33 & 39 & 51 & 30 & 55 & 36 & 16 & 25 & 13 & 25 & 61 & 1 \\ 3 & 9 & 42 & 27 & 42 & 57 & 54 & 15 & 60 & 45 & 3 & 9 & 12 & 36 & 60 & 0 \end{pmatrix}$$

$$A^{-1} \cdot (AM) = \begin{pmatrix} 14 & 15 & 15 & 6 & 5 & 1 & 15 & 20 & 15 & 18 & 21 & 6 & 14 & 19 & 5 & 1 & 21 & 1 \\ 1 & 3 & 14 & 9 & 44 & 19 & 18 & 5 & 20 & 9 & 14 & 15 & 1 & 3 & 4 & 12 & 20 & 0 \end{pmatrix}$$

Assim, localizando na figura 1 as letras correspondentes aos algarismos da matriz resultante de $A^{-1} \cdot (AM)$ encontrará como a frase “Não confie na sorte. O triunfo nasce da luta.”.

6.3. Fase da Experimentação

O experimento foi aplicado em uma turma do 3º ano do Ensino Médio da Escola Técnica Estadual 31 de Janeiro, no município de Campo Bom, no Rio Grande do Sul, no turno da manhã, em dois períodos a cada dia, totalizando 14 horas aula, no período de agosto a setembro de 2010.

A turma era formada por 44 alunos, sendo 29 do sexo feminino e 15 do sexo masculino, na faixa etária de entre 16 e 18 anos. Nessa classe, um aluno repetiu a 1ª série do Ensino Médio e outro parou de estudar um ano, 17 trabalham no turno da tarde com carga horária entre 5 e 6 horas diárias.

Nesta fase, foram explicados aos alunos os objetivos e as condições necessárias para a realização do experimento e foi aplicada a sequência elaborada, conforme a figura 10.

AULAS DA FASE DA EXPERIMENTAÇÃO	
1ª Aula	Foram distribuídas as apostilas com as atividades didáticas envolvendo o tema Criptografia aos conteúdos matemáticos do Ensino Médio. Nesta aula os alunos organizaram-se em grupos para realização das atividades. Em seguida, introduziu-se a história da Criptografia e foram desenvolvidas as atividades envolvendo Criptogramas, Cifra de César e a Cifra do Chiqueiro.
2ª Aula	Os alunos realizaram as atividades envolvendo a Cifra de Playfair, o Código ISBN e Código com Função Linear. A atividade envolvendo o conteúdo de função linear, cujo objetivo era revisar e reforçar o conceito de função, imagem da função, cálculo de função inversa.
3ª Aula	Na terceira aula os alunos continuaram a atividade de codificação e decodificação com Código com Função Linear.
4ª Aula	Resolução das atividades didáticas envolvendo o conteúdo de função quadrática, cujo objetivo era revisar e reforçar o conceito de função, imagem da função, cálculo de função inversa.
5ª Aula	Resolução das atividades didáticas envolvendo o conteúdo de função exponencial e logarítmica, que tinham por objetivo revisar as propriedades da potenciação, equações exponenciais, cálculo da imagem de uma função e logaritmo mudança de base.
6ª Aula	Os alunos continuaram a resolução da atividade de codificação com função exponencial e logarítmica. Após, iniciaram as atividades de código com matrizes, que tinham o objetivo de revisar o conceito de matriz, multiplicação de matrizes, operações com matrizes, matriz transposta, cálculo de matriz inversa.
7ª Aula	Deu-se prosseguimento a atividade didática de codificação e decodificação com matrizes.

Figura 10: desenvolvimento das aulas da fase de experimentação.

6.4. Fase da análise *a posteriori* e validação

Nesta fase foram analisados os dados obtidos na fase de experimentação. Na atividade didática envolvendo Código com Matrizes, após a introdução da atividade realizada pela professora/pesquisadora, os alunos atribuíram para cada letra da mensagem um algarismo e construíram a matriz mensagem.

A atividade proposta foi: *codifique a mensagem "Conhecer o caminho não é o mesmo que o percorrer!"*, sabendo que a matriz codificadora é $A = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$. Para codificar, os alunos multiplicaram a matriz mensagem pela matriz codificadora, como se observa na figura 11.

Resolução do grupo C

$$\text{Am} \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 3 & 14 & 5 & 5 & 15 & 1 & 8 & 8 & 14 & 15 & 15 & 5 & 13 & 17 & 5 \\ 15 & 18 & 3 & 18 & 3 & 13 & 14 & 15 & 1 & 5 & 13 & 18 & 5 & 21 & 15 \\ 16 & 18 & 15 & 18 & 18 \\ 5 & 3 & 18 & 5 & 18 \end{pmatrix}$$

$2 \cdot 3 + 4 \cdot 15 = 66$	$1 \cdot 3 + 5 \cdot 15 = 78$
$2 \cdot 14 + 4 \cdot 8 = 60$	$1 \cdot 14 + 5 \cdot 8 = 54$
$2 \cdot 5 + 4 \cdot 3 = 22$	$1 \cdot 5 + 5 \cdot 3 = 20$
$2 \cdot 5 + 4 \cdot 18 = 82$	$1 \cdot 5 + 5 \cdot 18 = 95$
$2 \cdot 15 + 4 \cdot 3 = 42$	$1 \cdot 15 + 5 \cdot 3 = 30$
$2 \cdot 1 + 4 \cdot 13 = 54$	$1 \cdot 1 + 5 \cdot 13 = 66$
$2 \cdot 8 + 4 \cdot 14 = 74$	$1 \cdot 8 + 5 \cdot 14 = 78$
$2 \cdot 8 + 4 \cdot 15 = 76$	$1 \cdot 8 + 5 \cdot 15 = 83$
$2 \cdot 14 + 4 \cdot 1 = 32$	$1 \cdot 14 + 5 \cdot 1 = 19$
$2 \cdot 15 + 4 \cdot 5 = 50$	$1 \cdot 15 + 5 \cdot 5 = 40$
$2 \cdot 15 + 4 \cdot 13 = 82$	$1 \cdot 15 + 5 \cdot 13 = 80$
$2 \cdot 5 + 4 \cdot 18 = 86$	$1 \cdot 5 + 5 \cdot 18 = 100$
$2 \cdot 13 + 4 \cdot 15 = 86$	$1 \cdot 13 + 5 \cdot 15 = 88$
$2 \cdot 17 + 4 \cdot 21 = 118$	$1 \cdot 17 + 5 \cdot 21 = 122$
$2 \cdot 5 + 4 \cdot 15 = 70$	$1 \cdot 5 + 5 \cdot 15 = 80$
$2 \cdot 16 + 4 \cdot 5 = 52$	$1 \cdot 16 + 5 \cdot 5 = 41$
$2 \cdot 18 + 4 \cdot 3 = 48$	$1 \cdot 18 + 5 \cdot 3 = 33$
$2 \cdot 15 + 4 \cdot 18 = 102$	$1 \cdot 15 + 5 \cdot 18 = 105$
$2 \cdot 18 + 4 \cdot 5 = 56$	$1 \cdot 18 + 5 \cdot 5 = 43$
$2 \cdot 18 + 4 \cdot 18 = 108$	$1 \cdot 18 + 5 \cdot 18 = 98$

$$\text{Am} \begin{pmatrix} 66 & 60 & 22 & 82 & 42 & 54 & 74 & 76 & 32 & 50 & 82 & 86 & 26 & 118 \\ 78 & 50 & 20 & 95 & 30 & 66 & 78 & 83 & 19 & 40 & 80 & 100 & 88 & 122 \\ 70 & 52 & 48 & 102 & 56 & 102 \\ 80 & 41 & 33 & 105 & 43 & 108 \end{pmatrix}$$

Figura 11: exemplo da resolução da atividade de codificação com matrizes.

Ainda, na atividade didática envolvendo o conteúdo de matrizes, os alunos se organizaram para codificar e decodificar. Cada aluno do grupo ficou responsável pela codificação de uma parte da frase para otimizar o tempo de resolução da atividade. Isso oportunizou que cada membro do grupo fizesse a atividade. Na atividade de decodificação envolvendo o conteúdo de matrizes, por exemplo: *decodifique a mensagem "10/ 106/ 132/ 54/ -60/ 86/ 58/ 98/ -70/ 94/ 86/ 30/ 108/ 58/ 81/ 72/ 15/ 26/ 5/ 34/ 121/ 40/ 16/ 10/ 38/ 114/ 10/ 106/ 87/ 90/ 50/ 112/ -73/ 66/ -88/ 78/ 113/ 54/ 10/ 106"*, sabendo que a matriz codificadora é $A = \begin{pmatrix} 7 & -5 \\ 2 & 4 \end{pmatrix}$. O grupo começou a decodificação, encontrando a matriz inversa da matriz A (figura 12). Depois realizaram a multiplicação da matriz inversa com a matriz da mensagem codificada, encontraram a matriz decodificada, substituíram os números pelas letras, conforme o quadro dado e encontraram a mensagem.

Resolução do grupo A

$$A^{-1} = \begin{pmatrix} 7 & -5 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$7a - 5c = 1 \quad 7b - 5d = 0$$

$$2a + 4c = 0 \quad 2b + 4d = 1$$

$$2a = -4c$$

$$a = \frac{-4c}{2} = -2c = -2 \cdot \left(-\frac{1}{19}\right) = \frac{2}{19}$$

$$7 \cdot (-2c) - 5c = 1$$

$$-14c - 5c = 1$$

$$-19c = 1$$

$$c = \frac{-1}{19}$$

$$7b - 5d = 0 \Rightarrow 7b = 5d$$

$$2b + 4d = 1 \quad b = \frac{5d}{7}$$

$$2 \cdot \frac{5d}{7} + 4d = 1$$

$$\frac{10d}{7} + 4d = 1 \quad \frac{5 \cdot 7}{7}$$

$$\frac{10d + 28d}{7} = \frac{7}{7} \quad b = \frac{38}{7}$$

$$38d = 7 \quad b = \frac{5}{38}$$

$$d = \frac{7}{38}$$

$$A^{-1} \begin{pmatrix} \frac{2}{19} & \frac{5}{38} \\ \frac{1}{19} & \frac{7}{38} \end{pmatrix}$$

Figura 12: exemplo da resolução da atividade envolvendo o conteúdo de matrizes.

Constatou-se, ainda, através das análises dos dados coletados, durante o experimento, que os alunos compreenderam a proposta das atividades e

conseguiram resolvê-las, demonstrando interesse e concentração durante a realização das mesmas, conforme a figura 13.



Figura 13: imagem dos alunos resolvendo as atividades.

Durante as atividades didáticas envolvendo os conteúdos matemáticos, percebeu-se que os alunos conseguiram desenvolver os conteúdos, mas é importante salientar que alguns foram desenvolvidos com mais facilidade do que em outros, pois as atividades de codificação com função linear, nas quais os alunos deveriam ter conhecimento de imagem da função e cálculo da função inversa foi facilmente lembrada pelos alunos. Porém, na atividade didática que envolvia codificação e decodificação com função quadrática, para codificar, os alunos utilizaram o conhecimento de função linear e calcularam a imagem, mas para decodificar não lembraram como realizar o cálculo da função inversa quadrática, o que teve que ser explicado pela professora/pesquisadora, que também chamou a atenção dos mesmos para a questão do domínio da função, visto que na função quadrática os alunos encontram duas variáveis.

Na atividade didática: *decodifique a mensagem "5, 509, 93, 23, 5, 33, 9, 33, 159, 5", sabendo que a função codificadora é $f(x) = x^2 + x + 3$* . O grupo realizou o cálculo da função inversa e calculou a imagem de cada letra (figura 14), em seguida, observou o quadro que atribui para cada letra um número e encontrou o texto decodificado. Esse foi um conteúdo novo que foi desenvolvido com a atividade proposta, pois o grupo de alunos não conhecia esse conteúdo e foi necessário a professora/pesquisadora introduzir o conceito de inversa de uma função quadrática.

Resolução do grupo C

$$f(x) = x^2 + x + 3$$

$$x^2 + x + 3 - y = 0$$

$$\Delta = b^2 - 4ac$$

$$\Delta = (-1)^2 - 4 \cdot 1 \cdot (3 - y)$$

$$\Delta = 1 - 12 + 4y$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-1 \pm \sqrt{1 - 12 + 4y}}{2 \cdot 1}$$

$$x = \frac{-1 \pm \sqrt{-11 + 4y}}{2}$$

$$f^{-1}(x) = \frac{-1 \pm \sqrt{-11 + 4x}}{2}$$

$$f^{-1}(5) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 5}}{2} = \frac{-1 \pm \sqrt{9}}{2} = \frac{-1 \pm 3}{2} = 1 \text{ a}$$

$$f^{-1}(509) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 509}}{2} = \frac{-1 \pm \sqrt{2025}}{2} = \frac{-1 \pm 45}{2} = 22 \text{ v}$$

$$f^{-1}(93) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 93}}{2} = \frac{-1 \pm \sqrt{361}}{2} = \frac{-1 \pm 19}{2} = 9 \text{ i}$$

$$f^{-1}(33) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 33}}{2} = \frac{-1 \pm \sqrt{121}}{2} = \frac{-1 \pm 11}{2} = 5 \text{ e}$$













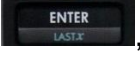
$$f^{-1}(9) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 9}}{2} = \frac{-1 \pm \sqrt{25}}{2} = \frac{-1 \pm 5}{2} = 2 \text{ b}$$

$$f^{-1}(23) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 23}}{2} = \frac{-1 \pm \sqrt{81}}{2} = \frac{-1 \pm 9}{2} = 4 \text{ d}$$

$$f^{-1}(159) = \frac{-1 \pm \sqrt{-11 + 4 \cdot 159}}{2} = \frac{-1 \pm \sqrt{625}}{2} = \frac{-1 \pm 25}{2} = 12 \text{ .}$$

Figura 14: exemplo da resolução da atividade do Código com Função Quadrática.

Nessa atividade, o grupo utilizou a calculadora científica da seguinte forma:

primeiro, apertaram a tecla dos parênteses , em seguida, digitaram o algarismo 1, a tecla , a tecla de deslocamento para direita , a operação de adição , a tecla dos parênteses , a operação de radiciação , a tecla dos parênteses , o algarismo 11, a tecla , a operação de adição , o algarismo 4, a tecla da operação de multiplicação , o algarismo 5, a tecla de deslocamento para direita  até sair de todos os parênteses. Apertaram na operação de divisão , no algarismo 2 e, para encontrar o resultado, apertaram a tecla , encontrando na calculadora a expressão da figura 15, que

apresenta parte da expressão no primeiro visor e outra parte no segunda visor, conforme foi visualizado pelos alunos que deslocavam o cursor para direita ou esquerda, para visualizar toda expressão.

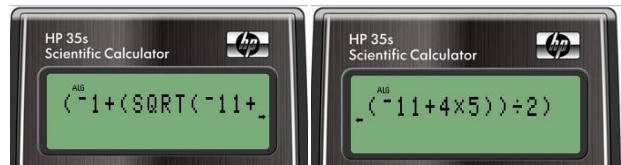


Figura 15: exemplo da atividade resolvida com a calculadora 35s da HP.

As atividades didáticas com funções exponenciais e logarítmicas possibilitaram aos estudantes compreenderem que essas funções são inversas, pois, para codificar, realizaram o cálculo da imagem da função e, para decodificar, envolvendo essas funções, a professora/pesquisadora teve que auxiliá-los, para que eles encontrassem a função inversa e conseguissem dar continuidade à atividade proposta. Essa atividade possibilitou a ampliação da compreensão desse conteúdo, conforme indicação dos alunos.

Os alunos resolveram as atividades didáticas envolvendo função exponencial e logarítmica, explorando os recursos da calculadora científica. Na atividade *codifique a mensagem “Por mais longa que seja a caminhada, o mais importante é dar o primeiro passo.”*, utilizando a função cifradora $f(x) = \log_2 x$, os alunos utilizaram logaritmo mudança de base, conforme a figura 16. Nesta atividade, quando encontravam dificuldades, os alunos discutiam entre os grupos para solucionar o problema. Se a dúvida persistisse, solicitavam o auxílio da professora.

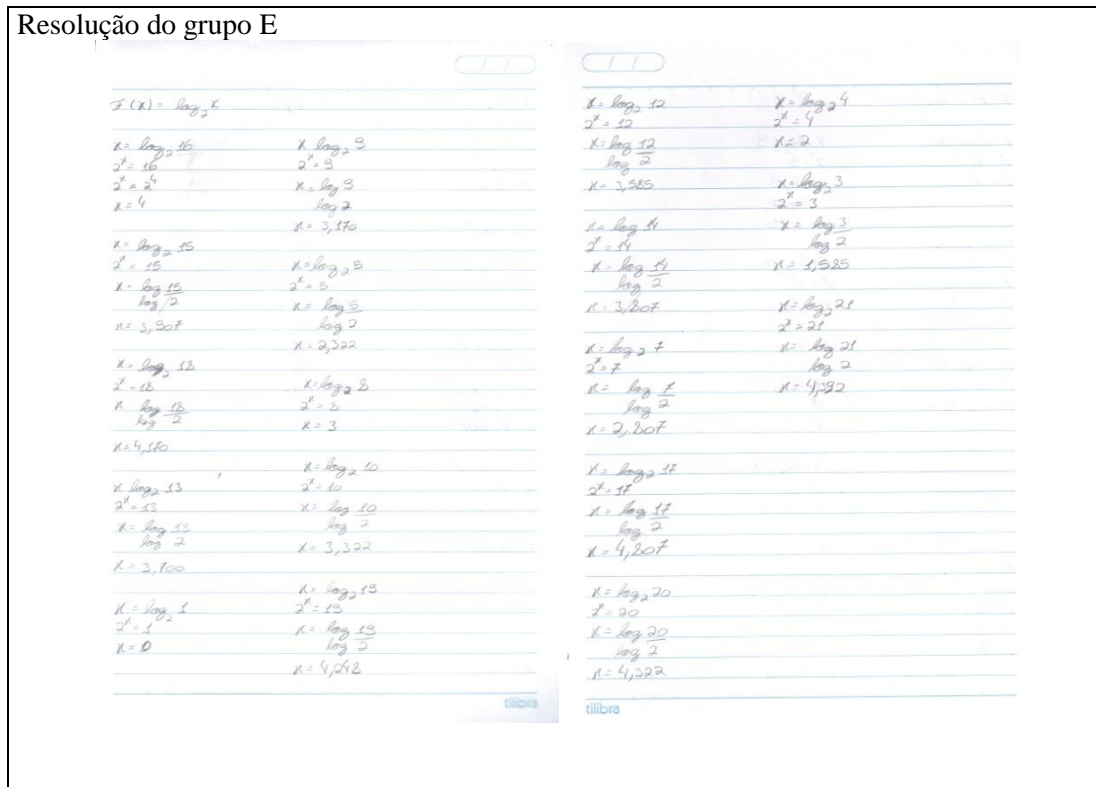



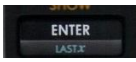


Figura 16: exemplo da resolução da atividade envolvendo função exponencial e logarítmica.

Utilizaram a calculadora da seguinte forma: primeiro, apertaram a tecla,  para habilitar função logaritmo, a tecla do logaritmo de base 10 , o algarismo 15, a tecla da operação de divisão, a tecla , o algarismo 2 e apertaram a tecla , encontrando na calculadora a expressão da figura 17.

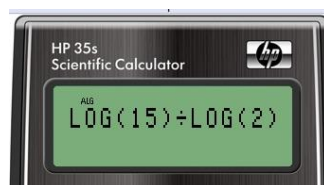


Figura 17: exemplo da atividade resolvida com a calculadora 35s da HP.

Nas atividades didáticas envolvendo matrizes, eles realizaram o cálculo de multiplicação de matrizes, matriz transposta, adição de matrizes e matriz inversa, sem encontrar dificuldades. Quando ocorria alguma dúvida, os próprios alunos se ajudavam e tentavam encontrar a razão da diferença nos resultados.

Também, foi possível perceber, durante a aplicação das atividades didáticas, na turma 231, que houve o diálogo, o trabalho em equipe e a troca de conhecimento entre os alunos, conforme a figura 18.



Figura 18: imagem dos alunos realizando as atividades.

Percebeu-se, ainda, que as atividades, com esse tema, abrem a discussão acerca da introdução, em sala de aula, da utilização de tecnologias da informação e comunicação, como a calculadora, que no experimento serviu de facilitador para cálculos longos. Esse item também foi uma ampliação aos conhecimentos dos alunos, pois já utilizavam a calculadora, mas, não sabiam utilizar as teclas de potência, parênteses, cursores e não a utilizavam para resolver expressões.

Pode-se constatar que, na turma em que foi realizada a aplicação das atividades com o tema Criptografia, desenvolvidas para o Ensino Médio, permitiu que os alunos revisitassem conteúdos estudados no Ensino Médio, ampliando a compreensão daqueles já desenvolvidos, os quais foram abordados na sequência didática.

As atividades didáticas desenvolvidas no experimento relacionaram o tema proposto aos conteúdos matemáticos do Ensino Médio, que são: função linear, função quadrática, função exponencial, função logarítmica e matrizes, além das atividades envolvendo a Cifra de César, Cifra do Chiqueiro e Cifra de Playfair.

Portanto, as atividades didáticas propostas na sequência elaborada pela professora/pesquisadora, possibilitou trabalhar com um tema de interesse dos estudantes, aliando os conteúdos matemáticos a um tema atual, tornando possível ampliar e revisar conteúdos já desenvolvidos. As atividades didáticas da forma, como foram conduzidas pelas professora/pesquisadora, em sala de aula, proporcionaram o trabalho em grupo e cooperativo.

CONCLUSÃO

A metodologia de Engenharia Didática possibilitou que a pesquisa fosse analisada internamente, verificando a validade das atividades desenvolvidas.

Na fase das análises preliminares, da Engenharia Didática com o tema Criptografia, foi possível verificar que o tema permite desenvolver atividades didáticas com os conteúdos matemáticos de funções e matrizes, explorando atividades de codificação e decodificação, o que possibilitou o desenvolvimento de uma sequência didática para esta etapa do Ensino Básico.

Na fase de experimentação, verificou-se que as atividades didáticas envolvendo códigos e senhas possibilitaram aos alunos trabalhar o conceito de Criptografia, aliado aos conteúdos de Matemática do Ensino Médio. Também tornou viável desenvolver as capacidades de concentração nas atividades, trabalho em grupo, desenvolver estratégias de resolução de problemas e validação das mesmas. As atividades didáticas desenvolvidas aliam os conteúdos matemáticos a um tema atual, apresentando diferentes situações e aplicações, bem como a utilização desse tema ao longo da história.

Atividades envolvendo o tema Criptografia e os conteúdos matemáticos do Ensino Médio são exemplos de material didático que pode ser utilizado pelos professores para exercitar, aprofundar, fixar e revisar conteúdos, fazendo uso de códigos e senhas, conforme as indicações de Tamarozzi (2001) e Cantoral (2003).

Pode-se verificar que as hipóteses propostas, foram alcançadas, através da sequência didática proposta para o 3º ano do Ensino Médio e das análises realizadas na fase de análise *a posteriori* e validação. Também se observa que, durante o desenvolvimento da Engenharia Didática, foram alcançados os objetivos traçados na investigação, em que se investigou a relação do tema em estudo com os conteúdos de Matemática. Foram pesquisadas atividades didáticas com o tema Criptografia, elaborada uma sequência didática envolvendo o tema e os conteúdos matemáticos do Ensino Médio, realizado um experimento em uma turma do 3º ano do Ensino Médio, onde verificou-se através da fase de análises *a posteriori* e validação que nas atividades desenvolvidas os alunos estabelecem relações com o tema.

Entende-se que a busca de temas de interesse que permitem o desenvolvimento de atividades didáticas devem ser incentivadas, pois o Currículo de Matemática a ser desenvolvido no Ensino Médio necessita ser de interesse do aluno, motivador e que o incentive ao estudo dos conteúdos.

REFERÊNCIAS

- ARTIGUE, Michèle; DOUADY, Régine; MORENO, Luis. **Ingeniería Didáctica en Educación Matemática: Un esquema para la investigación y la innovación en La enseñanza y el aprendizaje de las matemáticas.** Venezuela: Pedro Gómez, 1995.
- BRASIL. Lei 9394, de 20 de dezembro de 1996. **Diretrizes e Bases da Educação Nacional.**
- CANTORAL, Ricardo et al. **Desarrollo del pensamiento matemático.** México, Trillas: ITESM, Universidade Virtual, 2003.
- COLL, César. **Psicologia e Currículo: uma aproximação psicopedagógica à elaboração do currículo escolar.** São Paulo: Ática, 1999.
- D'AMBROSIO, Ubiratan. **Educação Matemática: da teoria à prática.** 2. Ed. Campinas: Papyrus, 1997.
- GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber. **Currículo de Matemática e o tema Criptografia no Ensino Médio.** Educação Matemática em Revista – RS. 2008, 51-57.
- GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber; OLGIN, Clarissa de Assis. **Códigos e senhas no Ensino Básico.** Educação Matemática em Revista – RS. 2009, 41-50.
- GROENWALD, Claudia Lisete Oliveira; RUIZ, Lorenzo Moreno. **Formação de professores de Matemática: uma proposta de ensino com novas tecnologias.** Revista de Ciências Naturais e Exatas. ACTA – SCIENTIAE. Volume 8. Número 2. Julho/Dezembro 2006, 19 – 28.
- KRIST, Betty J. **Logaritmos, Calculadoras e o Ensino de Álgebra Intermediária.** In: As Idéias da Álgebra, organizadores: Arthur F. Coxford e Alberto P. Shulte; traduzido por Hygino H. Domingues. São Paulo: Atual, 1995.
- MACHADO, Silvia Dias Alcântara et al. **Educação Matemática: uma (nova) introdução.** 2.ed. São Paulo: EDUC, 2008.
- PAIS, Luiz Carlos. **Didática da Matemática – Uma análise da influência francesa.** 2.ed. Belo Horizonte: Autêntica, 2005.
- PANNUTI, M.R.V. Caminhos da prática pedagógica. TVE Brasil. Rio de Janeiro, p. 01- 05, jun. 2004.
- PIRES, C. M. C. **Currículo de Matemática: da organização linear à idéia de rede.** São Paulo: FTD, 2000.
- SCHEINERMAN, Edward R. **Matemática Discreta: uma introdução.** São Paulo: Thompson, 2003.
- BRASIL. Secretaria de Educação Básica. **Orientações curriculares para o ensino médio.** Brasília: Ministério da Educação, Secretaria de Educação Básica, 2006.

- SINGH, Simon. **O Livro dos Códigos: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica**. Rio de Janeiro: Record, 2003.
- TAMAROZZI, Antônio Carlos. **Codificando e decifrando mensagens**. In Revista do Professor de Matemática 45, São Paulo: Sociedade Brasileira de Matemática, 2001.
- TERADA, Routo. **Criptografia e a importância das suas aplicações**. Revista do Professor de Matemática (RPM). Nº12, 1º semestre de 1988. São Paulo: Sociedade Brasileira de Matemática, 1988.
- ZABALA, Antoni. **A prática educativa: como ensinar**. Porto Alegre: ARTMED, 1998.
- ZATTI, Sandra Beatriz e BELTRAME, Ana Maria. **A presença da álgebra linear e da teoria dos números na criptografia**. Disponível em: www.unifra.br/eventos/.../2006/matematica.htm acesso em 26 de agosto de 2009.

Submetido: julho de 2011

Aprovado: setembro de 2011