REMATEC
Revista de Matemática, ensino e cultura
Modelagem Matemática

UMA ANÁLISE DO USO DA CRIPTOGRAFIA NOS LIVROS DIDÁTICOS DE MATEMÁTICA DO ENSINO MÉDIO

AN ANALYSIS OF THE CRYPTOGRAPHY USE IN MATHEMATICS TEXTBOOKS OF HIGH SCHOOL

Beatriz Fernandes Litoldo
Henrique Lazari

RESUMO
A proposta deste artigo é apresentar uma análise dos Livros Didáticos selecionados pelo PNLD 2012 acerca da inserção do tema Criptografia nos conceitos matemáticos do Ensino Médio, verificando se este tema é abordado, como é feita essa abordagem e em que conceitos matemáticos ele é utilizado. Tal análise se deu a partir de uma leitura dos livros das coleções, dando mais atenção aos conteúdos de álgebra. O tema foi encontrado em duas das cinco coleções analisadas, sendo utilizado como uma aplicação da teoria abordada em seções como *Saiba Mais* e *Contexto*. Este artigo ao estudar um tipo de aplicação utilizada em livros didáticos, visa possibilitar que projetos de modelagem sejam desenvolvidos, utilizando a Criptografia e conceitos matemáticos associados.

Palavras-chaves: Educação Matemática. Livro Didático. Criptografia. Ensino Médio.

ABSTRACT
The purpose of this article is to present an analysis of the textbooks selected by the PNLD 2012 regarding the inclusion of the topic Cryptography in mathematical concepts taught in high school to verify whether this topic is addressed, how it is approached and in which mathematical concepts it is used. This analysis was performed based on a reading of books of the collections, giving more attention to the content of algebra. The theme was found in two of the five collections analyzed, being used as an application of the theory discussed in sections as *Saiba Mais* and *Contexto.* This article, while studying a type of application used in textbooks, aims to enable modeling projects to be developed using Cryptography and mathematical concepts associated with it.

Keywords: Mathematical Education. Text Book. Criptography. High School.

Introdução

As pessoas estão cada vez mais conectadas com as tecnologias digitais e como consequência tiram proveito delas das mais diferentes formas. Tais tecnologias constantemente em evolução, proporcionam às pessoas a comodidade e facilidade de acessar a internet e navegar por inúmeros *sites* a qualquer hora. Atividades *on-line*, como compra e venda, transações bancárias, auditorias eletrônicas, entre outros, são exemplos de

situações da vida moderna que necessitam o uso da Criptografia. Logo, embora a maioria desconheça, a Criptografia faz parte de sua vida.

Por ser um assunto interessante que está intimamente vinculado ao cotidiano das pessoas, este tema pode ser, segundo Groenwald, Franke e Olgin (2009, p. 42) "motivador e gerador de situações didáticas que permitam o aprofundamento da compreensão dos conceitos matemáticos [...] e também, servir como um instrumento de ensino e aprendizagem no ensino básico".

Desse modo, além de permitir a aprendizagem da Criptografia em si, a inserção desse tema dentro das salas de aula propicia a conexão entre o cotidiano dos alunos e de suas famílias em relação à segurança de informação de cartões bancários, compra e venda *on-line*, entre outros, a temas como números primos, congruência modulo p, matrizes, funções lineares, exponenciais, logarítmicas, etc. A Criptografia ainda permite ao professor o desenvolvimento de atividades diferenciadas com seus alunos. Seu uso motiva e incentiva os alunos a estudarem matemática em sala de aula, contribuindo para que eles pesquisem, estudem e utilizem essa ciência em suas vidas (FINCATTI, 2010). Os argumentos levantados por Fincatti (2010) vêm ao encontro do que se propõe a Modelagem Matemática. Na concepção de Bassanezi (2002, pg. 16) a Modelagem Matemática consiste na "arte de transformar problemas da realidade em problemas matemáticos e resolvê-los interpretando suas soluções na linguagem do mundo real". Entretanto, como trazer para dentro da sala de aula a Criptografia e suas aplicações na matemática por meio dessa concepção?

A resposta a esta pergunta será dividida neste artigo em duas vertentes. A primeira vertente leva em conta o conhecimento do professor em relação à Criptografia e de toda sua flexibilidade em ser relacionada com os conteúdos do ensino básico, além de conhecer e compreender as concepções da Modelagem Matemática. A segunda seria a apresentação da Criptografia e suas aplicações na matemática por meio dos livros didáticos, e é neste ponto que daremos mais ênfase, pois a primeira opção não aborda a realidade dos professores atuantes na escola, já a segunda contempla todos aqueles atuantes no ensino escolar. Deste modo, apresentar a Criptografia e suas aplicações para os alunos, explorando o seu potencial como ferramenta de ensino, se apresenta conveniente quando atividades envolvendo este tema estão inseridas nos livros didáticos de matemática. Mais ainda, ao apresentar uma aplicação não utilizada regularmente nos projetos de modelagem no Brasil, espera-se que no futuro tal área possa se transformar em projetos de modelagem desenvolvidos por pesquisadores e professores.

Neste sentido, observa-se que o livro didático aparece no cenário escolar como uma ferramenta que auxilia o professor a compartilhar seus conhecimentos com os alunos, assumindo o papel de coadjutor da prática docente, mediando a construção do

conhecimento. Ele se constitui no principal recurso de direcionamento de professores e alunos em sua prática pedagógica e atividades escolares (SILVA e CARVALHO, 2004), sendo utilizado pelo professor como o principal manual de orientação e instruindo os alunos na realização de suas tarefas (exercícios, pesquisas, estudos) em sala de aula, bem como se tornando um referencial de pesquisa fora dela (SILVA e CARVALHO, 2004). O livro didático possibilita ainda que o aluno estabeleça novas ideias, complemente ou finalize o entendimento dos conteúdos abordados pelo professor, além de uma melhor fixação da matéria estudada (GONÇALVES, 2007). Assim sendo, além do livro didático auxiliar o professor nas atividades dentro da sala de aula, ele permite aos alunos a busca dos conteúdos sempre que sentirem essa necessidade.

Pensando especificamente nos livros didáticos de matemática, Gonçalves (2007, p. 24) afirma que estes devem "promover a compreensão dos conteúdos e levar o aluno a investigar, refletir, concluir, generalizar e aplicar os conhecimentos, através de problemas matemáticos ligados a realidade". De acordo com Borba (2013) os autores e editores exercem um papel fundamental na escolha dos conteúdos a serem ensinados e a maneira como estes devem ser aprendidos, bem como a ordem e ênfase dada a cada área do conteúdo. As atividades a serem desenvolvidas, propostas nos livros didáticos dependem muito da relevância que autores e editores atribuem ao conteúdo, levando em consideração a opinião direta e indireta de sujeitos externos.

Tendo em vista que os autores e editores de tais livros vivem em uma constante busca de novos recursos para o ensino e contextualização de seus conceitos em situações da vida moderna e que as abordagens diferenciadas desses conteúdos são cada vez mais essenciais para estimular o interesse dos alunos em aprender matemática, acredita-se que o tema Criptografia, vinculado aos conceitos matemáticos sob uma concepção da Modelagem Matemática, apresenta-se como um excelente recurso que pode ser incorporado nos livros didáticos de matemática como ferramenta para o ensino de tais conceitos. Nesse sentido, este artigo apresenta uma pesquisa realizada acerca da inserção da Criptografia com conceitos matemáticos nos livros didáticos de matemática do Ensino Médio e como tal inserção é feita olhando sob a luz da Modelagem Matemática. Essa pesquisa concentrou-se em analisar com que frequência a Criptografia é utilizada como recurso para o ensino ou aplicação de algum conceito matemático, de que maneira isso ocorre e em quais conceitos estão sendo utilizados. Cabe ressaltar que essa pesquisa faz parte de um projeto maior coordenado pelo segundo autor deste artigo, que vincula Criptografia e suas aplicações à Educação Matemática do Ensino Médio e Universitário.

Criptografia

Etimologicamente a palavra Criptografia, deriva das palavras gregas *kriptós* que significa escondido, oculto e *gráphein* que significa escrever, e pode ser considerada a arte ou a ciência de escrever mensagens em cifras ou em códigos, possibilitando exclusivamente apenas à pessoa autorizada decifrar e ler as mensagens (TAMAROZZI, 2000).

Há milhares de anos a Criptografia permeia as trocas de mensagens humanas de maneira sigilosa. Tais trocas sempre foram indispensáveis na história da humanidade, principalmente para os governantes, que dependiam de meios de comunicação eficientes para governar seus territórios, comandar seus exércitos, etc. Sua importância se intensificava em épocas de guerra, quando a eficiência e o sigilo na comunicação poderiam determinar a glória ou a ruína de um povo. Toda essa importância impulsionou o desenvolvimento de técnicas para camuflar as mensagens, de modo que somente o destinatário pudesse ler seu conteúdo, levando ao surgimento das cifras, que são maneiras de codificar as mensagens permitindo que apenas a pessoa que tenha o "segredo" para decifrar tal código possa ler as mesmas.

A Criptanálise, arte de tentar descobrir o texto cifrado e/ou a lógica utilizada na cifração, surge na história como uma contrapartida da Criptografia. Uma cifra deixava de ser segura quando alguém a decifrava, impulsionando assim, a criação de uma nova cifra. Esse embate entre Criptógrafos e Criptoanalista tem ocorrido desde a antiguidade até os dias de hoje.

Atualmente a Criptografia assume uma função também importante, nesta que é conhecida como a Era da Informação – uma era pós-industrial na qual a informação é a mercadoria mais valiosa. A utilização da informação digital cresce a cada dia, tornando-se parte de nossa sociedade. Tiramos proveito da internet trocando e-mails, efetuando compra e venda, realizando transações bancárias, entre outras atividades que podem exigir um nível de segurança maior ou menor. O sucesso e a eficiência de tais transações dependem essencialmente da capacidade de proteger essas informações enquanto elas fluem ao redor do mundo e isso depende principalmente do poder da Criptografia.

De acordo com Singh (2010) os matemáticos assumem na atualidade um papel extremamente importante nessa Era da Informação, já que estes se encontram à frente da criação e desenvolvimento das cifras para a proteção de informações militares e também estão no comando da decifração das mesmas. Ele observa que, se a Primeira Guerra Mundial foi atribuída aos químicos, devido ao gás de mostarda e ao cloro, e a Segunda Guerra Mundial aos físicos devido à bomba atômica, é aos matemáticos que é conferida

uma possível Terceira Guerra Mundial, já que a próxima grande arma de guerra será o controle e acesso a informação.

O poder de segurança da informação sempre esteve em evolução, a partir do momento que a cifra era quebrada, novas técnicas criptográficas eram desenvolvidas a fim de continuar a proteger as informações. Um grande salto na história da Criptografia em termos de proteção de mensagem ocorreu por volta de 1977 através dos cientistas de computação Rivest e Shamir e do matemático Adleman. Utilizando as ideias publicadas por Diffie e Hellman em 1975[32] acerca da busca por uma função de mão única, que se enquadrasse nos critérios exigidos para uma cifra assimétrica[33] é que o pesquisador Rivest se empenhou até descobrir a função apropriada para esse tipo de cifra. Shamir e Adleman contribuíram com essa descoberta, desenvolvendo então o sistema conhecido como RSA.

Este sistema, chamado RSA (Rivest, Shamir e Adleman), é um sistema de Criptografia assimétrica, também conhecido como *criptografia de chave pública*[34]. Hoje em dia a Criptografia RSA é altamente empregada, podendo ser encontrada em vários locais como, por exemplo, nos sistemas de correios eletrônicos, já que esse sistema permite um bom nível de segurança. A Criptografia de Chave Pública garante aos remetentes e aos destinatários a garantia da privacidade das mensagens juntamente com a assinatura das mesmas.

Como o sistema RSA é constituído basicamente das propriedades dos números inteiros, a principal segurança desse sistema é dada pela dificuldade em se conseguir fatorar números inteiros com grande velocidade. A partir do momento que esta fatoração passar a acontecer de forma rápida o sistema RSA se tornará inútil. Entretanto, por muitos anos os matemáticos vêm buscando o aumento nessa rapidez de fatoração, porém até então nenhum avanço nesta direção foi obtido. Assim, a fatoração ainda continua sendo um cálculo muito trabalhoso e em certos momentos uma tarefa muito difícil, logo o sistema RSA estará seguro por um bom tempo.

Livro Didático

Segundo Azevedo (2005, p. 5) "o livro didático no Brasil se estabeleceu no processo de ensino e aprendizagem de tal forma que adquiriu centralidade na transmissão do conhecimento para a grande maioria do professorado". Gonçalves (2007, p. 14) afirma que

[32] DIFFIE, Whitfield; HELLMAM, Martin E. **New directions in cryptography**. IEEE Trans. Inform. Theory, IT22, p. 644–654, Nov1976. Disponível em: < http://www.cs.berkeley.edu/~christos/classics/diffiehellman.pdf >.

[33]Utilização de chaves diferentes para cifração e decifração. Para mais informações ver em:
RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. CACM, l21, p. 120–126, 1978. Disponível em: < http://people.csail.mit.edu/rivest/Rsapaper.pdf >.

[34] Para mais informações ver Souza (2013) – Criptografia de Chave Pública, Criptografia RSA.

"devido às políticas públicas brasileiras, o livro didático foi produzido a fim de atender a parcela carente que correspondia e ainda corresponde à maioria da população, com a intenção de compensar as desigualdades sociais". O livro didático também foi tomado como um recurso pedagógico destinado a promover melhorias na organização, apresentação e complementação nos conteúdos curriculares, além de proporcionar uma orientação para o professor acerca do seu planejamento de aula e ter se tornado um recurso para pesquisas escolares (GONÇALVES, 2007).

Antigamente, os livros didáticos eram vistos apenas como uma ferramenta pedagógica secundária na prática do professor, entretanto atualmente esse material passou a ser um instrumento pedagógico essencial na sala de aula e fundamental na escolarização e letramento de nossos alunos. A relação de interdependência entre professor, aluno e livro didático interfere diretamente no ensino, sendo o livro impresso a principal fonte de informação utilizada em grande parte pelos professores e alunos de nosso país (LIMA, 2012; AZEVEDO, 2005).

Em qualquer disciplina, a utilização do livro didático é fundamental, visto que, em muitos casos este é o único instrumento pelo qual os alunos têm acesso à leitura e à cultura letrada (Guia de Livros Didáticos – PNLD[35] 2012) e, em diversas circunstâncias, é o único material pedagógico utilizado pelo professor em suas aulas (AZEVEDO, 2005). Borba (2013) ainda ressalta que o livro didático contribui na continuidade de formação dos professores acerca da construção de seus conhecimentos conceituais, didáticos e pedagógicos em relação ao ensino e aprendizagem da matemática.

Mesmo em tempos modernos, onde novos e diversos recursos tecnológicos designados à transmissão do conhecimento estão cada vez maiores, no ambiente escolar "o livro impresso ainda é o material que melhor atende às necessidades dos professores e alunos das escolas públicas brasileiras" (Guia de Livros Didáticos – PNLD 2012, p. 7). Com o objetivo de auxiliar na formação educacional, social e cultural do indivíduo o livro didático ainda traz muitas vantagens e é por causa delas que sua utilização continua crescendo e se devolvendo a cada dia (GONÇALVES, 2007).

Dentre as vantagens de se ter um livro impresso, que pode ser portado com a pessoa, de modo que esta pode consultá-lo sempre que julgar necessário, Gonçalves (2007) ressalta que a utilização do livro didático amplia expressivamente a capacidade de leitura, desenvolvendo no aluno o hábito de ler. A autora ainda complementa que o livro didático proporciona ao aluno a possibilidade de rever o conteúdo estudado, ressaltando os pontos importantes e elaborando ideias com maior facilidade, além de exercer um papel informativo ao leitor, podendo ao mesmo tempo diverti-lo também.

[35] Programa Nacional do Livro Didático

Em meio a essas vantagens, o livro didático assume um papel essencial na construção do aprendizado, pois através dele pode se formar uma conexão entre o trabalho do professor e dos alunos em sala de aula. Ele é um meio no qual se pode transmitir e se transferir conhecimento, vincular ideias e difundir valores, além de relacionar conhecimentos de senso comum a conhecimentos cientificamente aceitos (SILVA e CARVALHO, 2004).

Neste sentido, o professor precisa estar atento à sua prática docente, tendo consciência de que através de sua prática, aliada ao livro didático, ele deve proporcionar aos alunos o desenvolvimento da criticidade, da investigação, da reflexão, da criatividade e de sua capacidade de raciocínio. Para isso, o professor também precisa contar com um bom livro didático que, para assim ser considerado, deve atender a algumas características como, por exemplo, conteúdo objetivo, linguagem de fácil compreensão e relacionada à realidade do aluno, com exercícios que auxiliam no aprendizado, entre outros (GONÇALVES, 2007).

Visando disponibilizar livros didáticos de boa qualidade nas escolas públicas brasileiras, o Ministério da Educação do Brasil (MEC) iniciou em 1929 um programa do governo voltado à distribuição de livros didáticos a estudantes de escola pública. Anos mais tarde este programa foi intitulado como Programa Nacional do Livro Didático – PNLD (PNLD)[36]. No início do programa, apenas livros voltados para o ensino fundamental eram analisados e avaliados pelo PNLD, mas em 2004 este programa se ampliou, passando a analisar e a avaliar também livros didáticos para o ensino médio (Guia de Livros Didáticos – PNLD 2012).

O PNLD tem como principal objetivo contribuir com os professores na escolha de livros didáticos de qualidade, dentre os disponíveis no mercado, que serão distribuídos aos alunos da educação básica. Após a avaliação das obras, um Guia de Livros Didáticos é publicado pelo MEC oferecendo aos professores as resenhas das coleções aprovadas pelo programa. O Guia de Livros Didáticos visa auxiliar o professor na escolha do mesmo, sendo considerado como um instrumento de apoio a este processo. Após sua publicação, o guia é encaminhado às escolas para que possam escolher, dentre as obras apresentadas, aquelas que melhor se enquadram no seu projeto político pedagógico. Essa avaliação ocorre em períodos trienais, sendo que a cada ano o MEC adquire e distribui livros didáticos para todos os alunos (Portal MEC). Em sua edição atual, sete coleções foram aprovadas pelo PNLD 2012[37]. Os livros do PNLD 2012 selecionados pelos professores

[36] Para maiores informações sobre a história do PNLD ver em: < http://www.fnde.gov.br/programas/livro-didatico/livro-didatico-historico >.
[37] PNLD 2012 / Matemática. Disponível em: < http://www.fnde.gov.br/programas/livro-didatico/guia-do-livro/item/2988-guia-pnld-2012-ensino-m%C3%A9dio >.

serão válidos para os anos 2013, 2014 e 2015, sendo que em 2015 uma nova avaliação será feita para selecionar os livros para os próximos três anos.

Criptografia, Livro Didático e Modelagem Matemática

De acordo com Bassanezi (2002, pg. 36) "o desenvolvimento de novas teorias matemáticas e suas apresentações como algo acabado e completo acabam conduzindo seu ensino nas escolas de maneira desvinculada da realidade". O esquema:

"enunciado → demonstração → aplicação",

representa claramente essa estrutura tradicional de ensino, entretanto, a construção dessa ordem, segundo esse autor, deveria ser invertida, isto é, partir de sua motivação (externa ou não a matemática), ocorre-se a formulação de hipótese, permeando entre suas validações e de novos questionamentos, chegando finalmente em seu enunciado (BASSANEZI, 2002). Assim, por esse novo fio condutor, é que o processo da modelagem aconteceria e juntamente com ele, o ensino e aprendizagem.

Meyer, Caldeira e Malheiros (2011) corroboram com essa inversão de abordagem. Segundo eles, a Modelagem Matemática segue um procedimento dividido em três passos principais, a saber, o da formulação, o do estudo de resolução e o de avaliação, sempre se apoiando em um diálogo, em uma negociação e acordo entre os alunos a respeito de tais passos. Algumas perguntas como: "Pra que serve isso" e "Pra que serve a Matemática" são frequentemente feitas pelos alunos. Como resposta, a Modelagem Matemática se insere no contexto da sala de aula para que os alunos possam fazer uso dela, e, a partir disso, compreender mais sua realidade e sua situação de vida (MEYER, CALDEIRA e MALHEIROS, 2011). Essa compreensão da realidade destacada por esses autores vem da maneira como os conteúdos são trazidos, abordados e desenvolvidos em sala de aula. De acordo com eles, o processo de ensino e aprendizado na Modelagem Matemática, se inicia somente quando são os próprios alunos que trazem os problemas da realidade a serem trabalhados em sala de aula.

A autonomia e liberdade dada aos alunos para em conjunto, escolherem um tema de sua realidade e a partir dele desenvolver os conteúdos matemáticos do currículo, contribui para desenvolver a curiosidade e motivação dos alunos para levá-los à compreensão da matemática e de seu uso no cotidiano. Entretanto, quando se volta para o material didático essa liberdade de escolha infelizmente desaparece, pois seu conteúdo e a maneira como ele será apresentado já esta estabelecida. Porém, o livro didático pode constituído na concepção de Modelagem Matemática olhar para as aplicações e para as matemáticas que tais aplicações necessitam.

Demonstrar aos alunos que a matemática é utilizada por todas as pessoas por diferentes razões e propósitos e ajudar a fornecer significado e interpretações para problemas reais que utilizam a matemática são concepções da Modelagem Matemática da qual o livro didático pode ser constituído. Segundo Niss, Blum e Galbraith (2007) essas concepções promovem a "motivação dos alunos para se empenhar nos estudos de matemática, pois ajuda a moldar suas crenças a atividades em relação a ela"[38]. Assim, o ponto de partida no processo de ensino e aprendizagem da Matemática deve ser dado na busca do elo entre o interesse do aluno e sua formação cidadã.

O currículo de matemática deve levar em consideração uma abordagem a fim de proporcionar ao aluno a visualização da aplicação dos conteúdos matemáticos em situações da história ou do cotidiano, dentro e fora da escola. Escolher temas que propiciem atividades pedagógicas, que possibilitem uma abordagem de ensino e aprendizagem da Matemática que desencadeiam o processo de criticidade matemática e autonomia durante a aprendizagem, que estimule a curiosidade do aluno e que o leve à construção do conhecimento de forma a desenvolver suas competências e habilidades, são desafios que a Educação Matemática vem tentando superar (GROENWALD, FRANKE e OLGIN, 2009; OLGIN, 2011). Neste sentido, a Criptografia pode ser um tema que consegue relacionar os conteúdos desenvolvidos ao longo do ensino básico com situações práticas. Este tema, também proporciona ao professor diversas atividades e jogos de codificação que podem ser usados para a fixação e exploração dos conteúdos matemáticos (TAMAROZZI, 2001).

Certamente muitos alunos já ouviram falar em Criptografia, pois além de seu uso prático, ela também está presente em obras literárias[39] e cinematográficas[40]. Deste modo, pode-se utilizá-la como um tema diferenciado para atrair e cativar o interesse dos alunos, já que ela está intrinsicamente ligada aos sistemas de segurança eletrônicos da vida moderna. Assim, além de enriquecer o ensino de matemática, ela pode despertar a curiosidade e aguçar a imaginação dos estudantes (BORGES, 2008) contribuindo para diminuir a existência de aulas mecânicas de um ensino maçante da matemática tradicional (OLIVEIRA e KRIPKA, (2011); PAROLINE e TOSINI, (2009)).

A flexibilidade que este tema oferece para ser trabalhado com os conceitos matemáticos do currículo escolar, pode servir como um aliado para o ensino e

[38] "providing motivation for students to engage in the study of mathematics by helping to shape their beliefs and attitudes towards it".
[39] Júlio Verne em *Viagem ao centro da Terra*; Sir Arthur Conan Doyle nas aventuras de *Sherlock Holmes*; Edgar Allan Poe em *O escaravelho de ouro*, entre outros.
[40] Ver mais em Eiras, Luiz. C. S.; **Criptografia na Ficção** – Técnicas antigas e fantasias modernas. Revista: Prodemge – Tecnologia de Minas Gerais. p. 14-15, 2004..

aprendizagem no Ensino Médio, contribuindo para um enriquecimento das aulas de matemática. Os conceitos de aritmética, funções lineares, quadráticas, exponenciais, logarítmicas, matrizes, entre outras, podem ser abordados em contextos criptográficos envolvendo um mistério atraente para os alunos, podendo ser então, um gerador de motivação e interesse, instigando, desafiando e convidando os alunos a "brincar" com a arte de cifrar/ decifrar mensagens e, dessa maneira, aprender/fixar o conceito envolvido.

Alguns trabalhos como: Currículo de Matemática no Ensino Médio: atividades didáticas com o tema Criptografia (GROENWALD e OLGIN, 2011), Criptografia e os Conteúdos Matemáticos do Ensino Médio (OLGIN, 2011), Criptografia e o Currículo de Matemática no Ensino Médio (GROENWALD e OLGIN, 2011) abordam o tema Criptografia vinculados a alguns conceitos matemáticos do Ensino Médio. Esses trabalhos apresentam como sugestões ao professor, atividades didáticas para serem trabalhadas e desenvolvidas com os alunos. Segundo esses autores, tais atividades, além de possibilitarem aos alunos um trabalho sobre o conceito de Criptografia, podem ser usadas para exercitar, aprofundar, fixar e revisar conteúdos matemáticos, contribuindo com o desenvolvimento das capacidades de concentração, trabalho em grupo e estratégias de raciocínio, concluindo que existe uma grande relevância deste tema quando acoplado a alguns conceitos matemáticos no ensino e aprendizagem. Oliveira e Kripka, (2011) afirmam que, com o entrelaçamento deste tema aos conteúdos matemáticos em sala de aula, é possível proporcionar ao aluno uma ponte entre os acontecimentos da atualidade com fatos importantes da história e suas contribuições, além de poder tornar o aprendizado da matemática mais fácil, produtivo e significativo, contribuindo para a formação e desenvolvimento da vida escolar, social e pessoal do aluno.

Nesse sentido, levando em conta que o livro didático é uma ferramenta que apoia e auxilia a tarefa do professor na formação de seus alunos, a inserção do tema Criptografia como ferramenta de ensino/aplicação através dos livros didáticos de matemática torna-se extremamente conveniente, visto que isso poderia ampliar o potencial do livro didático como ferramenta de apoio. Do mesmo modo, considera-se que os livros didáticos de matemática podem ser o vínculo que leve o professor e os alunos ao tema Criptografia, apresentando possíveis atividades pedagógicas que envolvam conceitos matemáticos do Ensino Médio, como funções, matrizes, entre outros e que sejam relacionadas à Criptografia, difundindo assim esse tema que apesar de tão presente em nossas vidas, é tão pouco conhecido e explorado.

Metodologia

Este trabalho foi desenvolvido em três etapas. A primeira se deu através de estudos e discussões a respeito da Criptografia e seus possíveis alinhamentos com os conteúdos matemáticos. Na segunda etapa ocorreu a seleção dos livros didáticos que seriam analisados. Como o intuito é analisar os livros que estão ou estarão disponíveis na rede pública de ensino, recorremos ao material sugerido pelo PNLD. Visto que a análise dos livros para o ano que vem foi feita esse ano, escolheram-se para analise as coleções[41] aprovadas no PNLD 2012. A terceira etapa foi marcada pela leitura e análise das coleções apresentadas pelo PNLD 2012, verificando se o tema Criptografia era abordado e de que maneira essa abordagem ocorria.

Dentre as coleções aprovadas pelo PNLD 2012, por questões de logística, foram analisadas apenas aquelas que estavam disponíveis no acervo da Biblioteca da UNESP[42] de Rio Claro/SP, as quais estão descritas mais detalhadamente na tabela abaixo (Tabela 1) e ilustradas na figura 1.

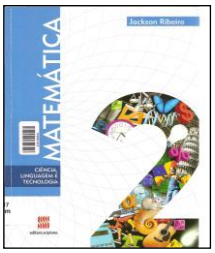
Tabela 1 - Coleções aprovadas pelo PNLD 2012 que foram utilizadas nessa pesquisa.

Título	Autor	Edição	Cidade	Editora	Ano
Matemática – Contexto & Aplicações	Luiz Roberto Dante	v. 1 – 4º v. 2 – 4º v. 3 – 3º	São Paulo	Ática	2007
Matemática Ciência e Aplicações	David Degenszajn, Gelson Iezzi, Nilze de Almeida, Osvaldo, Roberto Périgo	v. 1 – 5 º v. 2 – 5º v. 3 – 5º	São Paulo	Saraiva	2010
Matemática Ciência, Linguagem e Tecnologia	Jackson Ribeiro	v. 1 – 1 º v. 2 – 1º v. 3 – 1º	São Paulo	Scipione;	2010
Novo Olhar – Matemática	Joamir Souza	v. 1 – 1 º v. 2 – 1º v. 3 – 1º	São Paulo	FTD	2011
Conexões com a Matemática	Juliane Matsubara Barroso	Volume único - 1º	São Paulo	Moderna	2012

Fonte: Organizada pela autora a partir da das coleções dos livros didáticos aprovadas pelo PNLD – 2012.

[41] Entende-se aqui por coleção, todo(s) (os) livro(s) que contempla(m) os conteúdos do Ensino Médio de cada autor.
[42] Universidade Estadual Paulista.

Figura 1 - a) Jackson Ribeiro. v. 2; b) Joamir Souza. v.1 e c) Joamir



A coleção *Matemática Ciência, Linguagem e Tecnologia* de Jackson Ribeiro faz uso do tema Criptografia no volume 2 do capítulo 4, mais especificamente no estudo de matrizes nas páginas 152-153. A seção selecionada para tratar desse assunto é o *Saiba mais* (Figura 2), que é um espaço no final de cada capítulo destinado a complementar o conteúdo estudado.

Figura 2 - Imagem da seção *Saiba Mais*, onde a Criptografia é utilizada como uma ferramenta para se trabalhar as propriedades multiplicativas e inversas de matrizes.

Saiba mais

Criptografar mensagens utilizando matrizes

O envio e o recebimento de informações sigilosas é uma necessidade antiga. Com o advento da internet, que propicia a troca de informações de maneira precisa e ágil, a criptografia tornou-se importante para que essa troca seja extremamente confidencial.

A criptografia consiste em um conjunto de princípios e técnicas para cifrar uma mensagem, tornando-a incompreensível, de forma que somente o remetente e o destinatário possam lê-la (decodificá-la). Para isso, define-se um **protocolo**, que deve ser conhecido apenas pelo remetente e pelo destinatário, denominado "chave".

Vocabulário

protocolo: conjunto de normas e especificações técnicas que regem a transmissão de dados entre computadores.

Remetente — chave — T (texto original) — algoritmo — ? — texto cifrado — algoritmo — ? — chave — Destinatário — T (texto original)

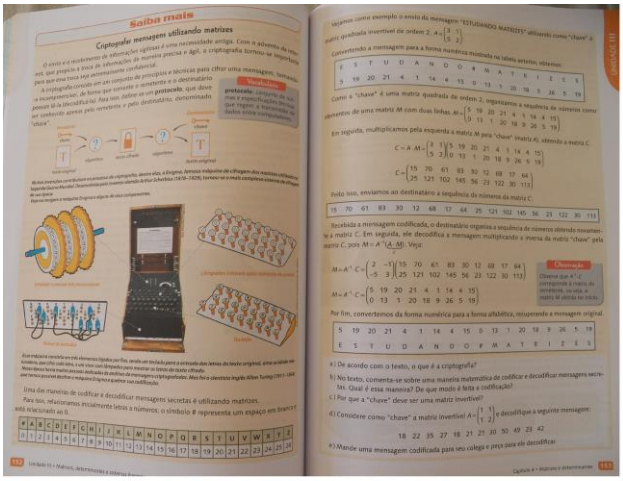
Muitas invenções contribuíram no processo de criptografia, dentre elas, a Enigma, famosa máquina de cifragem dos nazistas utilizada na Segunda Guerra Mundial. Desenvolvida pelo inventor alemão Arthur Scherbius (1878–1929), tornou-se o mais complexo sistema de cifragem de sua época.
Veja na imagem a máquina Enigma e alguns de seus componentes.

Unidade contendo três misturadores
Lâmpadas (visíveis após remoção do painel)
Painel de tomadas
Teclado

Essa máquina consistia em três elementos ligados por fios, sendo um teclado para a entrada das letras do texto original, uma unidade misturadora, que cifra cada letra, e um visor com lâmpadas para mostrar as letras do texto cifrado.
Nessa época havia muitas pessoas dedicadas às análises de mensagens criptografadas. Mas foi o cientista inglês Allan Turing (1911–1954) que tornou possível decifrar a máquina Enigma e quebrar sua codificação.

Este autor introduz o tema para o aluno apresentando a sua importância na segurança das transmissões de mensagens via ciberespaço. Em seguida ele traz uma definição básica sobre a Criptografia exibindo um esquema criptográfico e apresenta a máquina Enigma[43] através de uma imagem fiel descrevendo todo o seu sistema de funcionamento de modo resumido (Figura 3).

Figura. 3 - Introdução do tema Criptografia, apresentado logo em seguida um esquema criptográfico e a máquina enigma com seu funcionamento.



Dando continuidade a proposta da seção, em seguida ele argumenta que as matrizes podem ser uma das maneiras de se criptografar mensagens secretas. Para isso, é preciso fixar o alfabeto, relacionando as letras a números e designando o símbolo # para representar o espaço entre as palavras (Figura 4).

Figura 4 - Relação estabelecida entre letras e números.

Uma das maneiras de codificar e decodificar mensagens secretas é utilizando matrizes.

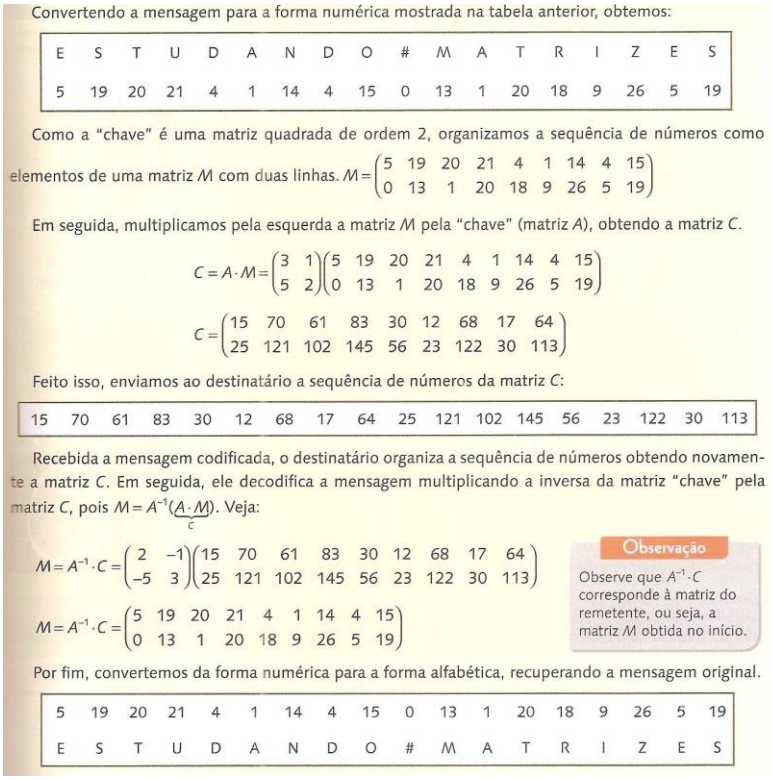
Para isso, relacionamos inicialmente letras a números; o símbolo # representa um espaço em branco e está relacionado ao 0.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

[43] Enigma foi uma famosa máquina de cifragem utilizada pelos militares alemães durante a II Guerra Mundial. Criada pelo inventor alemão Arthur Scherbius (1878-1929) esta máquina se tornou o sistema mais sofisticado de cifração de sua época.

Para exemplificar este processo, o livro propõe a cifração da mensagem "ESTUDANDO MATRIZES" através de uma matriz A quadrada invertível de ordem 2. A matriz A utilizada como "chave" para essa cifração será $A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$. Na Figura 5 observa-se todo o processo de codificação e de decodificação da mensagem. Esse exemplo apresenta o método de cifração e decifração por matrizes destacando consideravelmente suas operações e atentando-se ao conceito de matriz invertível.

Figura 5 - Processo de cifração e decifração utilizando matrizes.



Convertendo a mensagem para a forma numérica mostrada na tabela anterior, obtemos:

E	S	T	U	D	A	N	D	O	#	M	A	T	R	I	Z	E	S
5	19	20	21	4	1	14	4	15	0	13	1	20	18	9	26	5	19

Como a "chave" é uma matriz quadrada de ordem 2, organizamos a sequência de números como elementos de uma matriz M com duas linhas. $M = \begin{pmatrix} 5 & 19 & 20 & 21 & 4 & 1 & 14 & 4 & 15 \\ 0 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 \end{pmatrix}$

Em seguida, multiplicamos pela esquerda a matriz M pela "chave" (matriz A), obtendo a matriz C.

$$C = A \cdot M = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 5 & 19 & 20 & 21 & 4 & 1 & 14 & 4 & 15 \\ 0 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 \end{pmatrix}$$

$$C = \begin{pmatrix} 15 & 70 & 61 & 83 & 30 & 12 & 68 & 17 & 64 \\ 25 & 121 & 102 & 145 & 56 & 23 & 122 & 30 & 113 \end{pmatrix}$$

Feito isso, enviamos ao destinatário a sequência de números da matriz C:

15	70	61	83	30	12	68	17	64	25	121	102	145	56	23	122	30	113

Recebida a mensagem codificada, o destinatário organiza a sequência de números obtendo novamente a matriz C. Em seguida, ele decodifica a mensagem multiplicando a inversa da matriz "chave" pela matriz C, pois $M = A^{-1}(\underbrace{A \cdot M}_{C})$. Veja:

$$M = A^{-1} \cdot C = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 15 & 70 & 61 & 83 & 30 & 12 & 68 & 17 & 64 \\ 25 & 121 & 102 & 145 & 56 & 23 & 122 & 30 & 113 \end{pmatrix}$$

$$M = A^{-1} \cdot C = \begin{pmatrix} 5 & 19 & 20 & 21 & 4 & 1 & 14 & 4 & 15 \\ 0 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 \end{pmatrix}$$

Observação

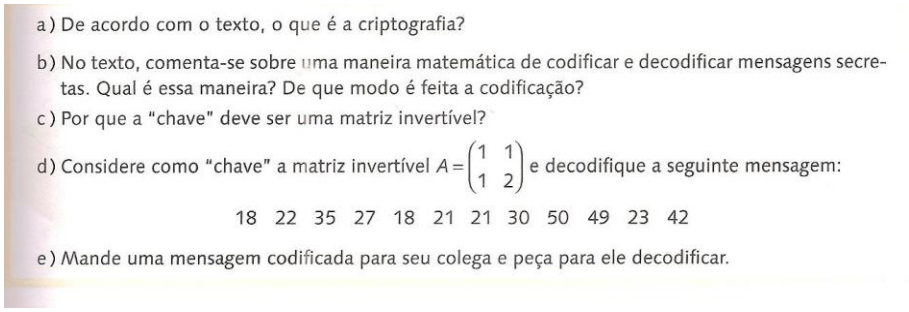
Observe que $A^{-1} \cdot C$ corresponde à matriz do remetente, ou seja, a matriz M obtida no início.

Por fim, convertemos da forma numérica para a forma alfabética, recuperando a mensagem original.

5	19	20	21	4	1	14	4	15	0	13	1	20	18	9	26	5	19
E	S	T	U	D	A	N	D	O	#	M	A	T	R	I	Z	E	S

Por último, a seção termina propondo ao aluno algumas questões (Figura 6) que abordam tanto o conceito sobre o que é criptografia, assim como a importância das matrizes serem invertíveis. O livro também apresenta um problema de decodificação e ainda convida os alunos a cifrarem e enviarem uma mensagem para algum colega para que este a decifre.

Figura 6 - Atividades para o aluno sobre a Criptografia, cifração e decifração de mensagens por meio de matrizes.



a) De acordo com o texto, o que é a criptografia?

b) No texto, comenta-se sobre uma maneira matemática de codificar e decodificar mensagens secretas. Qual é essa maneira? De que modo é feita a codificação?

c) Por que a "chave" deve ser uma matriz invertível?

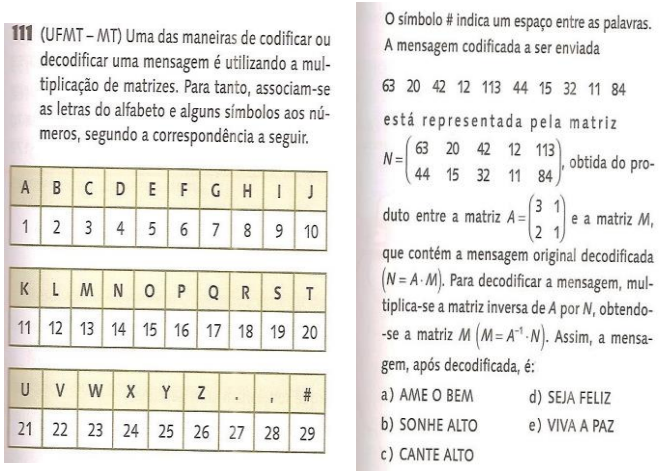
d) Considere como "chave" a matriz invertível $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ e decodifique a seguinte mensagem:

18 22 35 27 18 21 21 30 50 49 23 42

e) Mande uma mensagem codificada para seu colega e peça para ele decodificar.

Na seção *Prepare-se - Atividades, testes e questões para você aplicar o conhecimento construído*, o autor apresenta uma questão na página 157 da UFMT - MT[44] (Figura 7) na qual o aluno precisa decifrar uma mensagem codificada por uma matriz. Este problema traz consigo a matriz utilizada como chave para a codificação e ainda argumenta sobre como se utilizar a matriz invertível para se decifrar a mensagem. Uma curiosidade deste problema é que todas as alternativas formam frases com sentido, dificultando ainda mais uma decodificação superficial. Assim, para se chegar à frase original é preciso realmente empregar a multiplicação da matriz decodificadora. Deixarei para o leitor se aventurar neste enigma a fim de descobrir qual é a mensagem do referido problema.

Figura 7 - Problema apresentado pela UFMT – MT envolvendo cifração e decifração de uma mensagem por uma matriz.



111 (UFMT – MT) Uma das maneiras de codificar ou decodificar uma mensagem é utilizando a multiplicação de matrizes. Para tanto, associam-se as letras do alfabeto e alguns símbolos aos números, segundo a correspondência a seguir.

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10

K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z	.	,	#
21	22	23	24	25	26	27	28	29

O símbolo # indica um espaço entre as palavras. A mensagem codificada a ser enviada

63 20 42 12 113 44 15 32 11 84

está representada pela matriz $N = \begin{pmatrix} 63 & 20 & 42 & 12 & 113 \\ 44 & 15 & 32 & 11 & 84 \end{pmatrix}$, obtida do produto entre a matriz $A = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$ e a matriz M, que contém a mensagem original decodificada $(N = A \cdot M)$. Para decodificar a mensagem, multiplica-se a matriz inversa de A por N, obtendo-se a matriz M $(M = A^{-1} \cdot N)$. Assim, a mensagem, após decodificada, é:

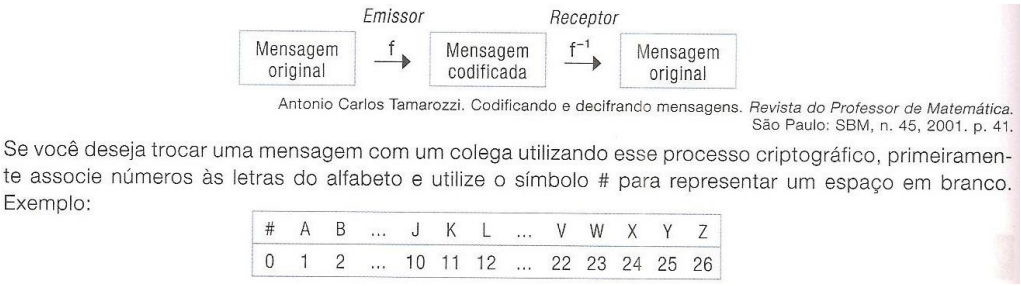
a) AME O BEM
b) SONHE ALTO
c) CANTE ALTO
d) SEJA FELIZ
e) VIVA A PAZ

[44] Universidade Federal de Mato Grosso.

Já a coleção, *Novo Olhar – Matemática* de Joamir Souza, embora não apresente em nenhuma seção de testes ou questões de vestibular, problemas que envolvam Criptografia vinculada a algum conceito matemático, utiliza o tema Criptografia em dois de seus três volumes. No volume 1 o tema aparece no capítulo 2, página 72, o qual foi atribuído o conceito de função e no volume 2 o tema aparece no capítulo 4, página 139 designado a matrizes e determinantes. Em ambos os livros a associação do tema Criptografia com o conceito matemático ocorreu em uma seção chamada *Contexto*, aparecendo sempre no espaço designado a *Atividades*, posteriormente à teoria utilizada na atividade proposta nessa seção.

Nos dois volumes, juntamente com uma introdução sobre a utilização da Criptografia nos dias de hoje, o livro traz uma breve explicação sobre o significado da Criptografia, além de abordar problemas e atividades acerca da cifração e decifração de mensagens por meio do conceito de função e de matrizes. No volume 1 um esquema criptográfico é apresentado, exemplificando um sistema de cifração e decifração. Em seguida o texto sugere que para se trocar mensagens, uma relação entre números e as letras do alfabeto deve ser estipulada, assim como o espaço entre as palavras (Figura 8).

Figura 8 - Esquema criptografia e associação estabelecida entre letras e números.



Antonio Carlos Tamarozzi. Codificando e decifrando mensagens. *Revista do Professor de Matemática*. São Paulo: SBM, n. 45, 2001. p. 41.

Se você deseja trocar uma mensagem com um colega utilizando esse processo criptográfico, primeiramente associe números às letras do alfabeto e utilize o símbolo # para representar um espaço em branco. Exemplo:

#	A	B	...	J	K	L	...	V	W	X	Y	Z
0	1	2	...	10	11	12	...	22	23	24	25	26

Para elucidar como utilizar o esquema criptográfico o livro escolhe a frase "ESTUDE MATEMATICA" para cifrar e, para isso, define uma função *f* real como sendo $f(x) = 3x - 1$. Na Figura 9 encontra-se o processo de cifração desta mensagem junto com uma argumentação de sua decifração. Como atividade para o aluno, o texto questiona em que outras situações há a necessidade de se usar a Criptografia, bem como seu objetivo. Também apresenta um problema de decodificação de uma mensagem e lança aos alunos o desafio de criptografar uma mensagem escolhida através de uma determinada função e distribuir para algum colega a mensagem e a função para que este descubra a função inversa e consequentemente a mensagem original (Figura 10).

Figura 9 - Cifração e decifração da mensagem "ESTUDEMATEMÁTICA"

Depois, defina a função por meio da qual a mensagem será criptografada. Suponha que seja *f* de $\mathbb{R}$ em $\mathbb{R}$, cuja lei de formação é $f(x)=3x-1$. Em seguida, escolha a mensagem a ser transmitida e associe cada letra da mensagem ao seu número correspondente. A mensagem ESTUDE MATEMATICA, por exemplo, é representada do seguinte modo:

5	19	20	21	4	5	0	13	1	20	5	13	1	20	9	3	1
E	S	T	U	D	E	#	M	A	T	E	M	A	T	I	C	A

Para transmiti-la ao seu colega, obtenha então a imagem de cada um desses valores por meio da função *f*, ou seja,

14	56	59	62	11	14	−1	38	2	59	14	38	2	59	26	8	2
f(5)	f(19)	f(20)	f(21)	f(4)	f(5)	f(0)	f(13)	f(1)	f(20)	f(5)	f(13)	f(1)	f(20)	f(9)	f(3)	f(1)

Ao receber a mensagem, ele terá de determinar, primeiramente, a imagem desses números pela função inversa de *f*, que neste caso é f^{-1} de $\mathbb{R}$ em $\mathbb{R}$, definida por $f^{-1}(x)=\frac{x+1}{3}$, e, em seguida, associar cada número obtido às letras do alfabeto para poder decifrá-la.

Por exemplo:

$$f^{-1}(14)=\frac{14+1}{3}=5,$$ e o número 5 corresponde à letra *E*.

No fim do processo, ele obterá a mensagem original que você enviou.

Figura 10 - Atividades propostas aos alunos sobre o a Criptografia e sobre o processo de cifração e decifração de mensagens através de uma função real

a) Apresente exemplos de situações que necessitam da criptografia para a comunicação confidencial de informações.

b) Qual o objetivo em um processo criptográfico?

c) Suponha que você esteja recebendo a mensagem abaixo criptografada por meio da função *f* de $\mathbb{R}$ em $\mathbb{R}$, dada por $f(x)=2x+1$, na qual as letras do alfabeto estão associadas conforme apresentado anteriormente. Determine a mensagem original que lhe foi enviada.

45 19 3 15 11 27 1 39 3 5 3 9 31

d) Escolha uma mensagem, determine uma função por meio da qual ela possa ser criptografada e escreva todos os passos do processo criptográfico. Depois, entregue a um colega a mensagem criptografada e a função utilizada, para que ele determine a função inversa e decifre a mensagem.

No volume 2 para dar início a exemplificação da cifração de uma mensagem por meio de matrizes o livro fixa, como exemplo, as letras do alfabeto com os números primos (Figura 11).

Figura 11 - Fixação das letras do alfabeto com os números primos.

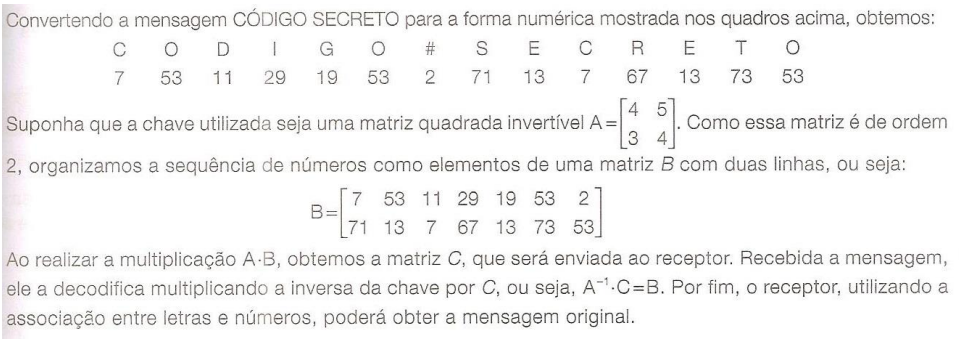
#	A	B	C	D	E	F	G	H	I	J	K	L	M
2	3	5	7	11	13	17	19	23	29	31	37	41	43

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
47	53	59	61	67	71	73	79	83	89	97	101	103

Com essa relação estabelecida à mensagem escolhida pare ser cifrada é "CÓDIGO SECRETO" e a matriz quadrada invertível escolhida para ser a "chave" de cifração é

A = $\begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix}$. A Figura 12 apresenta o processo de conversão e organização dos números em uma matriz B de ordem 2 e, em seguida o livro argumenta como obter a matriz codificada e depois de recebida como decodificá-la.

Figura 12 - Conversão da mensagem "CÓDIGO SECRETO" em uma matriz e o processo de cifração e decifração da mensagem.



Convertendo a mensagem CÓDIGO SECRETO para a forma numérica mostrada nos quadros acima, obtemos:

C	O	D	I	G	O	#	S	E	C	R	E	T	O
7	53	11	29	19	53	2	71	13	7	67	13	73	53

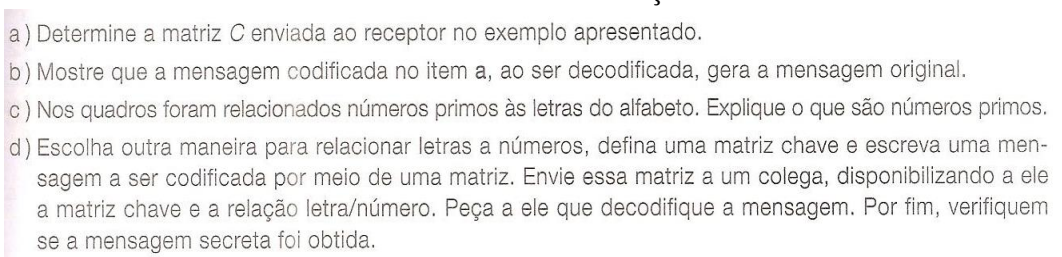
Suponha que a chave utilizada seja uma matriz quadrada invertível $A=\begin{bmatrix} 4 & 5 \\ 3 & 4 \end{bmatrix}$. Como essa matriz é de ordem 2, organizamos a sequência de números como elementos de uma matriz *B* com duas linhas, ou seja:

$$B=\begin{bmatrix} 7 & 53 & 11 & 29 & 19 & 53 & 2 \\ 71 & 13 & 7 & 67 & 13 & 73 & 53 \end{bmatrix}$$

Ao realizar a multiplicação A·B, obtemos a matriz *C*, que será enviada ao receptor. Recebida a mensagem, ele a decodifica multiplicando a inversa da chave por *C*, ou seja, $A^{-1}\cdot C=B$. Por fim, o receptor, utilizando a associação entre letras e números, poderá obter a mensagem original.

O trabalho de encontrar a matriz codificada e verificar a sua veracidade é deixada para o aluno como atividade. Uma das questões propostas ao aluno é em relação ao significado dos números primos, já que neste exemplo, esse tipo de número foi utilizado. Para fechar esta seção o livro propõe ao aluno que escolha outros tipos de relação entre o alfabeto e números e que codifique uma mensagem através de uma matriz, para distribuir essa mensagem para um amigo e pedir que sua decifração seja realizada (Figura 13). Neste volume, a imagem de uma máquina Enigma é apresentada junto com pequeno texto informativo sobre ela e sua utilização. Vale ressaltar que, na análise desta coleção, pode-se observar certa preocupação em parte do autor em trazer para os alunos em ambos os volumes a definição da palavra Criptografia e uma pequena discussão sobre sua utilização e importância nos dias de hoje.

Figura 13 - Questões apresentadas aos alunos para uma maior fixação e exploração do conteúdo desenvolvido nessa seção.



a) Determine a matriz *C* enviada ao receptor no exemplo apresentado.

b) Mostre que a mensagem codificada no item a, ao ser decodificada, gera a mensagem original.

c) Nos quadros foram relacionados números primos às letras do alfabeto. Explique o que são números primos.

d) Escolha outra maneira para relacionar letras a números, defina uma matriz chave e escreva uma mensagem a ser codificada por meio de uma matriz. Envie essa matriz a um colega, disponibilizando a ele a matriz chave e a relação letra/número. Peça a ele que decodifique a mensagem. Por fim, verifiquem se a mensagem secreta foi obtida.

Como conclusão desses resultados observa-se que essas duas coleções se preocuparam em trazer para os alunos uma definição sobre o termo Criptografia, bem como uma breve introdução sobre sua utilização nos dias atuais. Os problemas abordados sobre funções inversas e matrizes invertíveis foram fortemente trabalhados em conjunto com suas propriedades de operação. Esses problemas possibilitam que os alunos trabalhem individualmente ou em grupos e permite ao professor explorar e aprofundar questões sobre matrizes e funções, bem como alguns conjuntos numéricos como, por exemplo, números primos, números pares, entre outros.

Considerações Finais

Ponderando a forte presença do tema Criptografia em atividades da vida diária das pessoas, bem como o vínculo do assunto com fatos administrativos e políticos, é possível considerar que a inserção adequada de atividades ligadas a este tema pode ter um impacto positivo no processo de ensino e aprendizagem dos alunos. Em uma primeira abordagem, propriedades de funções como injetividade e sobrejetividade e famílias específicas de funções como logaritmos, por exemplo, podem ser um ambiente adequado para testar esta proposta.

Entretanto com a presente pesquisa conclui-se que embora o tema Criptografia esteja presente nos sistemas eletrônicos digitais da vida moderna e que a segurança destes depende exclusivamente da capacidade de proteção da cifra usada para se Criptografar, este assunto encontra-se pouco presente nos Livros Didáticos.

Conforme já citado, o PNLD 2012 aprovou sete coleções, que para a análise deste artigo, apenas cinco foram encontradas no acervo da Biblioteca de Rio Claro/SP. Dentre as cinco coleções apenas duas apresentaram seções envolvendo a Criptografia com um conceito matemático. A coleção, *Matemática Ciência, Linguagem e Tecnologia* de Jackson Ribeiro, apresenta em sua seção *Saiba Mais*, do volume 2 nas páginas 152-153, o tema Criptografia envolvendo as propriedades de multiplicação e inversão de matrizes, tendo na página 157 um problema de aplicação de matrizes na cifração de uma mensagens pela UFMT-MT. A coleção, *Novo Olhar – Matemática* de Joamir Souza aborda o tema na seção *Contexto* em dois de seus três volumes. No volume 1, na página 72, o livro utiliza a Criptografia para fixar e complementar o aprendizado de função, dando ênfase na propriedade da função inversa. Já no volume 2, na página 139, o livro proporciona ao aluno uma atividade envolvendo matrizes e suas operações de multiplicação e inversão.

Nota-se que o tema considerado nestas coleções não ocorre de forma significativa, nunca como parte de algum programa, raramente como conhecimento conexo a algum conteúdo e a sua importância nos dias de hoje. A Criptografia vem tendo destaque nas

notícias da atualidade, aproximando ainda mais os alunos, e a população em geral deste tema, o que pode estimular a difusão entre os autores dos Livros Didáticos da sua conexão com alguns conceitos matemáticos. Esta pesquisa possibilitará que o professor - ao conhecer o que se encontra no livro didático - possa desenvolver projetos de modelagem envolvendo temas e alguns tópicos de matemática que não tem sido utilizado em projetos de modelagem.

Referências

AZEVEDO, Edeílson Matias de. Livro didático: uma abordagem histórica e reflexões a respeito de seu uso em sala de aula. **Cadernos da FUCAMP**, Monte Carmelo, v. 4, n. 4, 2005.

BASSANEZI, Rodney C. **Ensino-aprendizagem com Modelagem Matemática.** São Paulo: Contexto, 2002.

BLUM, Werner; GALBRAITH, Peter L.; HENN, Hans-Wolfgang; NISS, Mogens. **Modelling and Applications in Mathematics Education**. New ICMI Study Series. v. 10. Springer. 2007.

BORBA, Rute.; SELVA, Ana. Analysis of the role of the calculator in Brazilian textbooks. **The International Journal on Mathematics Education**. v. 45, n. 5, p. 737 – 750, 2013**.**

BORGES. Fábio. Criptografia como Ferramenta para o Ensino de Matemática. In: XXXI Congresso Nacional de Matemática Aplicada e Computacional, 31, 2008, Belém. **Anais...** Belém, 2008. Disponível em: < http://www.sbmac.org.br/eventos/cnmac/xxxi_cnmac/PDF/189.pdf > Acesso em: 22 nov. 2013.

BRASIL. Ministério da Educação. Guia de livros didáticos: PNLD 2012: Apresentação / Brasília, Secretaria de Educação Básica, 2011. Disponível em: < http://www.fnde.gov.br/programas/livro-didatico/guia-do-livro/item/2988-guia-pnld-2012-ensino-m%C3%A9dio > acesso em: 14 ago. 2013.

BRASIL, Ministério da Educação. Disponível em: < http://portal.mec.gov.br/index.php?option=com_content&view=article&id=12391&Itemid=668 > Acesso em: 23 nov. 2013.

CARVALHO, Marlene A.; SILVA, Robson C. O livro didático como instrumento de difusão de ideologias e o papel do professor intelectual transformador**.** In: III Encontro de Pesquisa em Educação da UFPI/II Congresso Internacional em Educação, 3/2, 2004. **Anais...** 2004. Disponível em: < http://www.ufpi.br/subsiteFiles/ppged/arquivos/files/eventos/evento2004/GT.2/GT2_24_2004.pdf > acesso em: 29 out. 2013

FINCATTI, Camilla Á. **Criptografia como agente motivador na aprendizagem da matemática em sala de aula.** São Paulo: Universidade Presbiteriana Mackenzie/ Centro de Ciências e Humanidades, 2010. 82 p. Trabalho de Conclusão de Curso.

GONÇALVES, Ruth G. **O emprego do livro didático de matemática no ensino fundamental da rede pública estadual.** Criciúma: Universidade do Extremo Sul Catarinense (UNESC). 2007. 39 p.

GROENWALD, Claudia L. O.; FRANKE, Rosvita F.; OLGIN, Clarissa A. Códigos e Senhas no Ensino Básico**. Educação Matemática em Revista**, Rio Grande do Sul, v. 2, n. 10, p. 41–50, 2009.

GROENWALD, Claudia L. O.; OLGIN, Clarissa A. Currículo de Matemática no Ensino Médio: atividades didáticas com o tema Criptografia. In: XIII Conferência Interamericana de Educação Matemática, 13, 2011, Recife. **Anais...** Recife, 2011**.** Disponível em: < http://www.cimm.ucr.ac.cr/ocs/files/conferences/1/schedConfs/1/papers/691/submission/review/691-1818-1-RV.pdf > Acesso em: 03 nov. 2013.

GROENWALD, Claudia L. O.; OLGIN, Clarissa A. Criptografia e o Currículo de Matemática no Ensino Médio. **Revista de Educação Matemática**: Sociedade Brasileira de Educação Matemática, São Paulo, v. 13, n. 15, p. 69 – 78, 2011.

LIMA, Elício G. Para compreender o Livro Didático como objeto de Pesquisa. **Educação e Fronteiras *On-line***, Dourado, v. 2, n. 4, p. 143–155, 2012. Disponível em: < http://www.periodicos.ufgd.edu.br/index.php/educacao/article/viewFile/1563/pdf_116 > Acesso em: 22 nov. 2013.

MEYER, João F. C. A.; CALDEIRA, Ademir D.; MALHEIROS, Ana P. S. **Modelagem em Educação Matemática**. Belo Horizonte: Autêntica, 2011.

OLGIN, Clarissa A. Criptografia e os conteúdos matemáticos do Ensino Médio. In: XIII Conferência Interamericana de Educação Matemática, 13, 2011, Recife. **Anais...** Recife, 2011**.** Disponível em: < http://lematec.net/CDS/XIIICIAEM/artigos/2092.pdf > Acesso em: 03 nov. 2013.

OLIVEIRA, Daiane de; KRIPKA, Rosana M. L. O uso da criptografia no ensino de Matemática. In: XIII Conferência Interamericana de Educação Matemática, 13, 2011, Recife. **Anais...** Recife, 2011**.** Disponível em: < http://www.cimm.ucr.ac.cr/ocs/files/conferences/1/schedConfs/1/papers/1817/submission/review/1817-4607-1-RV.pdf > Acesso em: 23 nov. 2013.

PAROLIN, Radael S.; TOSINI, Fernando. Criptografia no Ensino de Matemática. X Encontro Gaúcho de Educação Matemática, 2009. Disponível em: < http://www.projetos.unijui.edu.br/matematica/cd_egem/fscommand/MC/MC_24.pdf > Acesso em: 23 nov. 2013.

RIBEIRO, Jackso. **Matemática Ciência, Linguagem e Tecnologia**. São Paulo: Scipione, 2010.

SINGH, Simon. **Livro dos Códigos: a ciência do sigilo do antigo Egito para a criptografia quântica**. 7º ed. Rio de Janeiro: Recorde, 2010.

SOUZA, Joamir. **Novo Olhar – Matemática**. São Paulo: FTD, 2011.

TAMAROZZI, Antônio C. Codificando e decifrando mensagens. **Revista do Professor de Matemática**, São Paulo v. 45, p. 41 – 43, 2000.

Beatriz Fernanda Litoldo
Universidade Estadual Paulista Júlio de Mesquita Filho – UNESP/Rio Claro - Brasil
E-mail: beatrizfernanda_rc@hotmail.com

Henrique Lazari
Universidade Estadual Paulista Júlio de Mesquita Filho – UNESP/Rio Claro - Brasil
E-mail: hlazari@rc.unesp.br