Criptografia e os conteúdos matemáticos do Ensino Médio

Clarissa de Assis **Olgin**
Universidade Luterana do Brasil
Brasil
clarissa_olgin@yahoo.com.br

Resumo

Os pressupostos educacionais da Educação Matemática salientam a importância do desenvolvimento do processo de ensino e aprendizagem com atividades didáticas envolvendo temas atuais, com assuntos de interesse dos alunos, que estimulem a curiosidade e que desencadeiem um processo cognitivo que permita a construção de novos conhecimentos. Nesse sentido, acredita-se que a Matemática se torna interessante e motivadora, para a aprendizagem, quando desenvolvida de forma integrada e relacionada a outros conhecimentos. Nesta oficina sugere-se o tema Criptografia como gerador de atividades didáticas que permitem o aprofundamento dos conteúdos matemáticos desenvolvidos no Ensino Médio, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas. O objetivo desta oficina é apresentar atividades didáticas que relacionem os conteúdos matemáticos do Ensino Médio ao tema Criptografia.

Palavras chave: Ensino Médio, Criptografia, Funções, Matrizes, Atividades Didáticas.

Introdução

O ponto de referência do processo de ensino e aprendizagem, da Matemática, deve ser a abordagem de assuntos que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos. Acredita-se que o tema Criptografia pode ser utilizado como gerador de atividades didáticas que permitem revisar, exercitar, fixar e aprofundar os conteúdos matemáticos desenvolvidos no Ensino Médio.

Esta oficina visa salientar a importância da utilização de atividades didáticas adequadas para o desenvolvimento do pensamento matemático, no Ensino Médio, apresentando o tema Criptografia para o desenvolvimento de situações didáticas que permitem o aprofundamento da compreensão dos conceitos matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas.

Esse trabalho é um recorte da pesquisa Teoria dos Números que vem sendo desenvolvida na Universidade Luterana do Brasil, desde 2002, e está vinculada ao GECEM-Grupo de Estudos Curriculares em Educação Matemática.

Os conteúdos que serão desenvolvidos nesta oficina com o tema em estudo serão: Função do 1º grau, Função do 2º grau, Função exponencial, Função logarítmica e Matrizes.

Justificativa do tema

O tema Criptografia tem um papel importante nos dias atuais, tendo em vista que é utilizado na auditoria eletrônica, na autenticação de ordens eletrônicas de pagamentos, no código de verificação do ISBN, nos navegadores de internet, entre outras situações da vida cotidiana (TERADA, 1988).

Este tema, também, pode servir como um instrumento de ensino e aprendizagem no Ensino Médio, contribuindo para enriquecer as aulas de Matemáticas. Segundo Tamarozzi (2001) este tema coloca a disposição do professor atividades e jogos de codificação e decodificação envolvendo conteúdos matemáticos que são trabalhados no Ensino Médio. Ainda, de acordo com Cantoral et al (2000) a Criptografia pode ser um elemento motivador para o processo de ensino da Matemática.

Nesta oficina serão trabalhados os conteúdos de funções e matrizes, pois o tema apresenta atividades didáticas que possibilitam ao aluno observar as relações e propriedades algébricas das funções, abrindo espaço para discussões em sala de aula sobre conceitos como domínio, contra-domínio, imagem e função inversa. Além disso, permite revisar e exercitar os conteúdos de multiplicações de matrizes e matrizes inversas.

Histórico do tema

A criptografia é uma arte bastante antiga, que já estava 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.

O citale espartano foi o primeiro aparelho criptográfico militar, utilizado durante o século V a.C.. O citale era um bastão de madeira, onde enrolava-se 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 a 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 freqüência de cada letra, no texto cifrado, surge 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. 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, e 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 (SINGH, 2003).

Em 1943, foi projetado o Colossus, esse computador foi utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela Enigma. O Colossus deu início a uma era moderna da criptografia, onde 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 começou-se a utilizar os computadores. Os computadores utilizavam criptografias complexas, mas não apresentavam ainda a segurança necessária para não serem invadidos por pessoas que não deveriam tem acesso aos códigos de criptagem contidos nele. Para solucionar este problema foram criados dois algoritmos de codificação o DES (sistema de chave secreta) e RSA (sistema de chave pública).

A DES é um algoritmo de criptografia em blocos, composto da substituição de caracteres em blocos de 64 bits, utilizando uma chave de 56 bits. Sua estrutura é composta de 16 estágios de criptografia, executando, durante todo o processo, séries de transposições e substituições de caracteres, bem como, a recombinação de blocos.

A adoção da DES resolveu um problema de padronização, encorajando as empresas a utilizarem a criptografia para sua segurança. A DES era suficientemente forte para garantir a segurança contra ataques de rivais comerciais, pois era impossível para uma empresa com um computador civil, quebrar uma mensagem cifrada com a DES, porque o número de chaves possíveis era suficientemente grande. O problema do algoritmo DES é a distribuição de chaves, pois a chave de codificação é a mesma de decodificação. O DES não se baseia em manter o segredo do seu algoritmo de codificação, mas o segredo da chave usada para codificar uma mensagem específica. A tecnologia DES tem sido utilizada em vários produtos comerciais e é o algoritmo de criptografia escolhido pelos usuários comerciais. Várias companhias utilizam o DES, dentre elas estão: a General Eletric, a IBM e a Motorola.

Segundo Coutinho (2000), o mais conhecido dos métodos de criptografia é o RSA. Este código foi inventado 1978, por R. L Rivest, A. Shamir, e L. Adleman. As letras RSA correspondem as iniciais dos inventores do algoritmo. O RSA é atualmente o mais usado em aplicações comerciais. Este método é utilizado, por exemplo, no netscape, um dos mais populares softwares de navegação da internet.

O RSA é o primeiro algoritmo de chave pública completo, um algoritmo que funciona para criptografia e assinaturas digitais.

O algoritmo RSA é de fácil compreensão, pois usa como base o fato de que é extremamente difícil fatorar um número que seja o resultado da multiplicação de dois números primos com muitos algarismos.

O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém encontre um método rápido para fatorar estes números primos, mas a grande vantagem desse sistema, de chave pública, é que ela acaba com os problemas da distribuição de chaves.

Objetivo

O objetivo desta oficina é apresentar atividades didáticas que relacionem os conteúdos matemáticos do Ensino Médio ao tema Criptografia, possibilitando ao aluno de Matemática do Ensino Médio, aplicar os conteúdos estudados e estabelecer estratégias mentais na resolução de situações problemas.

Pressupostos Teóricos

A Criptografia transforma textos originais, chamados texto original (plaintext) ou texto claro (cleartext), em uma informação transformada, chamada texto cifrado (ciphertext), texto código (codetext) ou simplesmente cifra (cipher), que usualmente tem a aparência de um texto randômico ilegível. A Criptografia é conhecida como a arte ou ciencia de escrever em cifra ou em código, de forma a permitir que somenteo destinatário a compreenda (SINGH, 2003).

Segundo Shokranian (2005), enviar uma mensagem em código pode servir para dois objetivos: enviar uma mensagem secreta e proteger o conteúdo da mensagem contra fontes não autorizadas; e servir para uma forma melhor de comunicação e transmissão de informações entre duas fontes.

Cifrar é o ato de transformar dados em alguma forma ilegível. Seu propósito é o de garantir a privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados.

Decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível.

Para cifrar ou decifrar uma mensagem, necesita-se de informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para criptografar como para decriptografar mensagens, enquanto outros mecanismos utilizam senhas diferentes.

Os conteúdos matemáticos de funções e matrizes podem ser utilizados como chaves cifradoras e decifradoras, apresentando atividades didáticas, onde o aluno do Ensino Médio aplica os conceitos matemáticos em situações práticas de Criptografia.

Exemplos de Atividades Didáticas

A seguir apresentam-se exemplos de atividades didáticas que podem ser utilizadas pelos professores do Ensino Médio apresentando o tema Criptografia como um recurso didático no Ensino da Matemática.

Atividade didática 1 – Código com função do 1º grau

Primeiro relacionamos para cada letra do alfabeto um número, conforme podemos observar na figura 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 1. Quadro apresentando o valor numérico de cada letra do alfabeto.

A função chave é: $f(x) = 4x + 7$

Texto Normal: T u d o é m a t e m á t i c a

Seqüência Numérica: 20 21 4 15 5 13 1 20 5 13 1 20 9 3 1

Criptografa-se a mensagem a ser transmitida substituindo cada número na função escolhida. Sendo a seqüência numérica a imagem da função, isto é:

87 91 23 67 27 59 11 87 27 59 11 87 43 19 11

Para decodificar a mensagem o receptor recebe a mensagem e calcula a imagem, dos elementos utilizando a função inversa: $f^{-1} = \frac{x-7}{4}$.

Atividade didática 2 – Código com função do 2º grau

Primeiro relaciona-se para cada letra do alfabeto a um número, conforme a figura 1.

A seguir, escolhe-se uma função cifradora, que pode ser, por exemplo, a função: $f(x) = ax^2 + bx + c$

Escolhe-se então um texto qualquer para ser criptografado: Liberdade

A seqüência numérica que corresponde ao texto é: 12 – 9 – 2 – 5 – 18 – 4 – 1 – 4 – 5

A mensagem a ser transmitida ao receptor deve ser a seqüência numérica obtida pela imagem da função.

A seguir apresenta-se um exemplo: depois de relacionar para cada letra do alfabeto um número, escolhe-se uma função chave: $f(x) = x^2 + 2x + 6$

O texto a ser criptografado é: O livro é uma caixa mágica.

A seqüência numérica é: 15 – 12 – 9 – 22 – 18 – 15 – 5 – 21 – 13 – 1 – 3 – 1 – 9 – 24 – 1 – 13 – 1 – 7 – 9 – 3 – 1.

Para criptografar a mensagem a ser transmitida, substituem-se cada número, da sequência numérica, na função escolhida. Por exemplo: A letra *O* corresponde ao número 15, portanto calcula-se $f(15) = 15^2 + 2.15 + 6$

$f(15) = 225 + 30 + 6$

$f(15) = 261$

Sendo a seqüência numérica a imagem da função, isto é: 261 – 174 – 105 – 534 – 366 – 261 – 41 – 489 – 201 – 9 – 21 – 9 – 105 – 630 – 9 – 201 – 9 – 69 – 105 – 21 – 9.

Atividade didática 3 – Código com funções exponencial e logarítmica

Primeiramente relaciona-se para cada letra do alfabeto um número, que corresponderá aos valores de x na função, conforme a figura 1.

A seguir, escolhe-se uma função exponencial cifradora, que pode ser, por exemplo, a função: $f(x) = 2^x$

Exemplo de um texto para ser criptografado: Nem tudo são flores.

A seqüência numérica do texto é 14 – 5 – 13 – 20 – 21 – 4 – 15 – 19 – 1 – 15 – 6 – 12 – 15 – 18 – 5 – 19

A mensagem a ser transmitida ao receptor deve ser a seqüência numérica obtida pela imagem da função, para cada letra do texto criptografado.

Criptografando a letra N, temos que a seqüência numérica de N é 14. A imagem da função $f(x) = 2^{14}$ é $f(x) = 16384$.

Para decodificar a mensagem o receptor receberá a mensagem e irá calcular a sua imagem através da função inversa.

O receptor sabe a função codificadora que é $f(x) = 2^x$, logo ele terá de calcular a inversa dessa função que é $x = \log_2 y$.

Então para 16384, a inversa é:

$x = \log_2 y$

$x = \log_2 16384$

$2^x = 16384$

$2^x = 2^{14}$

$x = 14$

E assim, se codifica e decodifica cada letra do texto cifrado.

Atividade didática 4 – Código com matrizes

Relaciona-se para cada letra do alfabeto um número, conforme a figura 1. Escolhe-se uma matriz A e a matriz inversa A^{-1}.

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

Texto Normal: M E I O A M B I E N T E
Seqüência Numérica: 13 5 9 15 1 13 2 9 5 14 20 5
Monta-se a matriz M com a seqüência numérica da mensagem que se quer enviar.

$$M = \begin{pmatrix} 13 & 9 & 1 & 2 & 5 & 20 \\ 5 & 15 & 13 & 9 & 14 & 5 \end{pmatrix}$$

Para codificar a mensagem calcula-se a matriz AM.

$$AM = \begin{pmatrix} 2 & 1 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} 13 & 9 & 1 & 2 & 5 & 20 \\ 5 & 15 & 13 & 9 & 14 & 5 \end{pmatrix} = \begin{pmatrix} 31 & 33 & 15 & 13 & 24 & 45 \\ 54 & 72 & 42 & 33 & 57 & 75 \end{pmatrix}$$

Para decodificar utiliza-se a identidade matricial, calculando a matriz $M = A^{-1}(AM)$.

$$M = A^{-1}(AM) = \begin{pmatrix} 1 & -\frac{1}{3} \\ -1 & \frac{2}{3} \end{pmatrix} \cdot \begin{pmatrix} 31 & 33 & 15 & 13 & 24 & 45 \\ 54 & 72 & 42 & 33 & 57 & 75 \end{pmatrix} = \begin{pmatrix} 13 & 9 & 1 & 2 & 5 & 20 \\ 5 & 15 & 13 & 9 & 14 & 5 \end{pmatrix}$$

Conclusão

Entende-se que o tema Criptografia apresenta material útil para exercícios de fixação de conteúdos, apresentando atividades e jogos de codificação (TAMAROZZI, 2001) que poder ser utilizados pelos profesores de Matemática do Ensino Médio. E também, oportuniza, ao professor, desenvolver diversas atividades de forma a motivar seu aluno ao estudo dos conceitos de Matemática. Ainda, deve ser levando em consideração que:

- as atividades com o tema Criptografia devem ser relacionadas a outros conhecimentos de Matemática;
- se faz necessário conhecer os conhecimentos prévios dos alunos, para que as atividades propostas estejam de acordo com os conhecimentos do estudante;
- a metodologia resolução de problemas é indicada para o desenvolvimento de atividades didáticas com o tema Criptografia.

As atividades didáticas apresentadas são sugestões para o professor de Matemática utilizar para revisar, exercitar e aprofundar os conteúdos de relação e propriedades algébricas das Funções do 1º Grau, Funções do 2º Grau, Funções Exponencial e Logarítmica e Matrizes de forma contextualizada.

Bibliografia e referências

Tamarozzi, A. C. (2003).Codificando e decifrando mensagens. In Revista do Professor de Matemática 45, São Paulo: *Sociedade Brasileira de Matemática*.

Cantoral, R. et al. (2003). Desarrollo del pensamiento matemático. México, Trillas: *ITESM, Universidade Virtual*.

Singh, S. (2003).O Livro dos Códigos: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: *Record*.

Shokranian, S; Soares, M & Godinho, H. (1999).*Teoria dos Números*. Brasília: UnB.

Terada, R. (1988). *Criptografia e a importância das suas aplicações.* Revista do Professor de Matemática (RPM). Nº 12, 1º semestre de 1988, 1-6.

Anexo A

Guias de trabalho

Esquema das atividades didáticas envolvendo o tema Criptografia e os conteúdos matemáticos do Ensino Médio, que serão abordados na oficina.

Atividades didáticas que serão exploradas na oficina	
Atividade Introdutória – Criptogramas	O objetivo dessa atividade é introduzir o tema proposto e revisar o conteúdo de aritmética, já trabalhado no Ensino Fundamental.
Atividade Didática envolvendo código com função do 1º grau	O objetivo dessa atividade é revisar e reforçar o cálculo da imagem da função linear e função linear inversa.
Atividade didática envolvendo código com função do 2º grau	O objetivo dessa atividade é revisar e reforçar o cálculo da imagem da função quadrática e função quadrática inversa.
Atividade Didática envolvendo código com função exponencial e logarítmica	O objetivo dessa atividade é revisar as propriedades da potenciação, calcula da imagem da função e logaritmo mudança de base.
Atividade Didática envolvendo código com matrizes	O objetivo dessa atividade didática é revisar multiplicação de matrizes e cálculo de matrizes inversas.

Anexo B

Informação Geral

Informação referente à oficina envolvendo o tema Criptografia e os conteúdos matemáticos do Ensino Médio.

Informação Geral	
Título da oficina	Criptografia e os conteúdos matemáticos do Ensino Médio
Nome da autora	Clarissa de Assis Olgin
Instituição da autora	Universidade Luterana do Brasil
País da autora	Brasil
Número de horas conveniente	2 horas
Nível de escolarização para o qual será dirigido o Painel (Educação infantil/Preescolar, Anos iniciais do Ensino Fundamental/Primária, Anos finais do Ensino Fundamental/Secundária, Ensino Superior, ou geral.	Ensino Médio
Número máximo de pessoas	30 pessoas
Equipamentos audiovisuais ou informáticos necessários (Projetor multimídia, TV grande, laboratório de informática, conexão à internet).	Projetor multimídia