ISSN 1676-8868
Revista de Educação Matemática – vol. 13, número 15, 2011
© Sociedade Brasileira de Educação Matemática – Regional São Paulo

# CRIPTOGRAFIA E O CURRÍCULO DE MATEMÁTICA NO ENSINO MÉDIO[i]

## CRYPTOGRAPHY AND CURRICULUM OF HIGH SCHOOL MATHEMATICS

Claudia Lisete Oliveira Groenwald[ii] - Universidade Luterana do Brasil
claudiag@ulbra.br
Clarissa de Assis Olgin[iii] - Prefeitura Municipal de Porto Alegre

**RESUMO:** Este trabalho apresenta o tema Criptografia como motivador de situações didáticas para alunos do Ensino Médio. Apresenta, também, atividades didáticas que aliam os conteúdos matemáticos ao tema proposto, envolvendo os assuntos: aritmética, funções linear, quadrática, logarítmica, exponencial e matrizes. Esse artigo é fruto da pesquisa Teoria dos Números que vem sendo desenvolvida na Universidade Luterana do Brasil (ULBRA), desde 2002, e está vinculada ao Grupo de Estudos Curriculares em Educação Matemática (GECEM).
**Palavras-chave**: Educação Matemática. Currículo de Matemática. Criptografia. Ensino Médio. Atividades didáticas.

**ABSTRACT:** This paper presents Cryptography as an agent of the motivation of didactic situations for high school pupils. Also, didactic activities that associate mathematics contents to the theme proposed are presented on the subjects: arithmetic; linear, quadratic, logarithmic, exponential functions; and matrices. This paper is part of the research Theory of Numbers, which has been developed in Lutheran University of Brazil (ULBRA) since 2002 and is linked to the Group of Curricular Studies on Mathematics Education (GECEM).
**Keywords**: Mathematics Education. Mathematics Curriculum. Cryptography. Calculators. High school Curriculum. Didactic Activities.

## 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 (GROENWALD e FRANKE, 2007). Para as autoras a Matemática se torna interessante e motivadora para a aprendizagem quando desenvolvida de forma integrada e relacionada a outros conhecimentos já desenvolvidos na escola, trazendo o desafio de desenvolver competências e habilidades formadoras.

Segundo os Parâmetros Curriculares Nacionais do Ensino Médio (BRASIL, 1998) nessa etapa da escolaridade, o ensino da Matemática deve ir além de seu caráter instrumental, colocando-se como Ciência, com características próprias de investigação e de linguagem e com um papel integrador, tendo um caráter importante junto às demais Ciências da Natureza.

Este artigo apresenta a pesquisa desenvolvida sobre o tema Criptografia e os conteúdos matemáticos do Ensino Médio, visando salientar a importância da utilização de atividades didáticas que possibilitem aos alunos: resolver problemas, levantar hipóteses, ter autonomia no processo de resolução e verificação de suas hipóteses, trabalharem em grupo e cooperativamente. Na pesquisa envolvendo o tema Criptografia e os conteúdos matemáticos, apresenta-se este tema como motivador e gerador de situações didáticas que permitem o aprofundamento da compreensão dos conceitos[1] matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas.

[1] Conceitos, segundo Coll, Pozo, Sarabia e Valls (1998) são os conteúdos desenvolvidos nas escolas, nas diferentes disciplinas, onde os conteúdos são divididos em conceitos e fatos.

## Justificativa do tema Criptografia no Currículo de Matemática do Ensino Médio

O nome Criptografia vem das palavras gregas *kriptós* que significa escondido, oculto e *graphein* que significa escrita (SINGH, 2003). A Criptografia é denominada de arte de escrever em códigos (TAMAROZZI, 2001), de forma a permitir que somente o destinatário a decifre e compreenda. A criptografia torna possível o envio de mensagens incompreensíveis para uma terceira pessoa que, eventualmente, venha interceptá-las, mas que poderão ser lidas pelo seu destinatário, que conhece o critério para decifrar o texto encriptado (TERADA, 1998; TAMAROZZI, 2001; SCHEINERMAN, 2003; ZATTI e BELTRAME, 2009).

A Criptografia tem um papel importante nos dias atuais, pois é utilizada 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 moderna.

Para Terada (1988), o meio de comunicação digital, controlado por computadores, trouxe flexibilidade e eficiência em gravação, recuperação e distribuição de informações, sendo utilizado em sistemas de transações bancárias *on-line*, sistema de compras a distância, saques e transferências de fundos com cartões eletrônicos. Porém, segundo o autor, à medida que se intensificam as transmissões de numerosas informações (como transferência de fundos, registros financeiros, médicos, militares etc.) através de meios eletrônicos (satélites, linhas telefônicas, fitas magnéticas, etc.), as possibilidades de quebra de segurança e de privacidade aumentam, pois essas transações podem ser modificadas, gerando fraudes. A maneira mais segura de ter uma garantia de que informações transmitidas não serão copiadas, modificadas ou falsificadas é o uso da Criptografia.

Esse tema pode, também, servir como um instrumento de ensino e aprendizagem no Ensino Médio, contribuindo para enriquecer as aulas de Matemática, pois coloca à disposição do professor atividades e jogos de codificação e decodificação (GROENWALD, FRANKE e OLGIN, 2009). De acordo com Cantoral et al. (2000), a Criptografia pode ser um elemento motivador para o processo de ensino e aprendizagem da Matemática. Para Tamarozzi (2001), exemplos elementares de processos criptográficos podem constituir, para os professores, um material útil para exercícios de revisão e fixação de conteúdos matemáticos.

As atividades apresentadas neste artigo envolvem os conteúdos: aritmética, funções linear, quadrática, exponencial e logarítmica e matrizes. Tais atividades possibilitam aos alunos revisitarem os conceitos de aritmética já estudados no Ensino Fundamental, observarem as relações e as propriedades algébricas das funções, abrindo espaço para discussões sobre os conceitos de domínio, contradomínio, imagem e função inversa, bem como, revisar os conteúdos de matrizes.

O desenvolvimento das atividades aqui propostas possibilita, também, o uso de calculadoras na sala de aula. Segundo Krist (1995), as calculadoras podem servir de laboratório para os alunos, pois, com esse recurso, eles podem realizar experiências e desenvolver suas próprias ideias e estratégias. O professor de Matemática pode utilizá-la em sala de aula, de forma planejada, e, assim, a calculadora pode tornar-se um recurso que contribui para o aprendizado dos conteúdos matemáticos, liberando tempo e energia gastos em operações repetitivas, possibilitando que o foco da aula seja a resolução de problemas. Para D'Ambrosio (2009), a calculadora permite a primazia do raciocínio qualitativo (criatividade – busca do novo) sobre o raciocínio quantitativo (rotina). Segundo Silva (1991), a calculadora deve fazer parte dos recursos que os professores devem utilizar em sala de aula, acompanhada da reflexão das suas potencialidades e de um profundo exame da Matemática que se ensina, por que ensinamos e a forma como ensinamos.

**Objetivo da investigação**

O objetivo geral deste trabalho foi investigar o tema Criptografia e suas aplicações para o desenvolvimento de atividades didáticas aplicáveis no currículo de Matemática do Ensino Médio.

**Metodologia da investigação**

Este trabalho foi desenvolvido em duas etapas. A primeira, desenvolvida através de reuniões semanais de estudo, em torno dos conceitos de Criptografia, sua história e utilização na vida moderna. A segunda etapa foi a pesquisa e análise de atividades didáticas aliando o tema em estudo aos conteúdos matemáticos e, também, o desenvolvimento de atividades didáticas para o Ensino Médio. Foi realizada uma ampla revisão bibliográfica em livros, revistas da área de Educação Matemática, anais de congressos e documentos on-line.

**Atividades didáticas utilizando códigos e senhas**

Um exemplo de atividade envolvendo a descoberta de números são os criptogramas, onde cada letra indica um algarismo, letras iguais representam algarismos iguais, e letras diferentes representam algarismos diferentes. O professor pode revisitar os conceitos de aritmética, propondo a seguinte atividade: descubra o valor de cada letra no criptograma

$$\begin{array}{r} N\ O\ V\ E \\ +\ T\ R\ \hat{E}\ S \\ \hline D\ O\ Z\ E \end{array}.$$

Nessa atividade espera-se que o aluno resolva a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para a resolução.

Informação relevante: S = 0 porque E + S = E.

Hipóteses: 1. Como O + R = O, então O + R > 10 pois S já é zero; 2. V + E > 10 para confirmar a hipótese 1.

Prevendo resultados: se S = 0, O = 8 e R = 9, então: E = 5, V = 6, Z = 1, N = 2, T = 4 e D = 7.

Uma das primeiras formas de codificar foi o *Citale* Espartano (SINGH, 2003), que era um aparelho criptográfico militar, que consistia em um bastão de madeira, onde se enrolava uma tira de couro e se escrevia a mensagem em todo o comprimento desse bastão. Segundo o autor, 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, conforme figura 1.

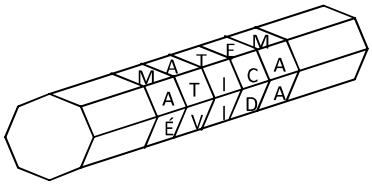



**Figura 1:** exemplo de *Citale* Espartano.

A cifra monoalfabética, caracterizada pela substituição de uma letra por outra ou por um símbolo, era outra opção utilizada para criptografar uma mensagem. Uma das primeiras cifras monoalfabéticas era a utilizada por Júlio César, servia para fins militares e consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto. Esse método de criptografia ficou conhecido como Cifra de César.

Para codificar utilizando a Cifra de César desloca-se cada letra do alfabeto original três casas a frente, conforme apresentado na figura 2:

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

**Figura 2:** Quadro do método de substituição utilizado por Júlio César.
Fonte: Adaptado de Singh (2003, p.27)

Utilizando a figura 2 e considerando como texto original a frase "A VIDA É BELA", tem-se o seguinte texto cifrado: "DYLGDHEHOD", de onde foram retirados os espaços entre as palavras para dificultar a decodificação.

Outro exemplo de Cifra de substituição monoalfabética, foi a Cifra do Chiqueiro 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 3.

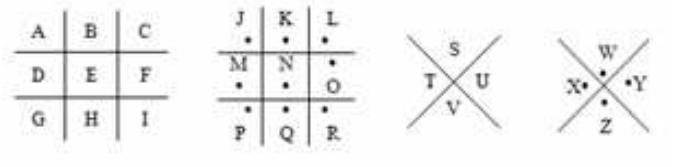
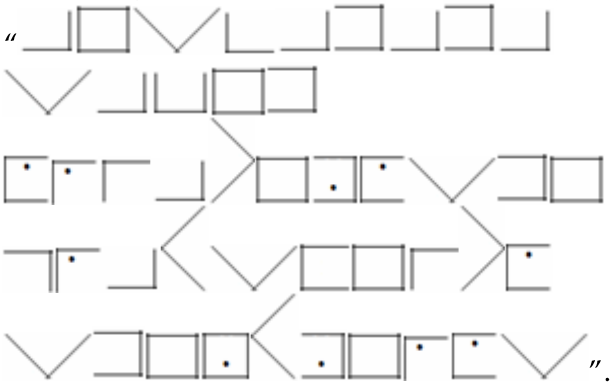



**Figura 3:** exemplo do padrão utilizado pela Cifra do Chiqueiro.

A codificação da Cifra do Chiqueiro é realizada encontrando a posição da letra em uma das quatro grades da figura 3 e desenhando a porção da grade que representa a letra a ser codificada, por exemplo, a letra **E** corresponde ao símbolo  .

Um exemplo de atividade é a decodificação da mensagem, utilizando a Cifra do Chiqueiro "  ".

Como a Cifra de César era de substituição de letras, facilmente decodificada por criptoanalistas por apresentar 26 chaves em potencial, a solução encontrada no século XVI, foi a cifra polialfabética, criada pelo diplomata francês Blaise Vigenère, denominada Cifra de Vigenère e que seguia o mesmo princípio da Cifra de César, porém eram utilizados 26 alfabetos cifrados para codificar e decodificar uma mensagem, conforme mostra a figura 4.

| Alfabeto Normal | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| 2 | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| 3 | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| 4 | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| 5 | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| 6 | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| 7 | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| 8 | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| 9 | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| 10 | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| 11 | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| 12 | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| 13 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 14 | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 15 | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 16 | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| 17 | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| 18 | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| 19 | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| 20 | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| 21 | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| 22 | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| 23 | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| 24 | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| 25 | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |
| 26 | 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 |

**Figura 4:** exemplo do quadro da Cifra de Vigenère.

No Quadrado de Vigenère, há o alfabeto normal, seguido de 26 alfabetos cifrados. Cada alfabeto tem um deslocamento de uma casa à frente no mesmo alfabeto, seguindo o princípio do Código de César. De acordo com Singh (2003), para escrever uma mensagem codificada pelo Quadrado de Vigenère, combina-se uma palavra-chave, por exemplo: **VIDA**. Para cifrar a palavra ÁLGEBRA, é preciso escrever a palavra-chave quantas vezes for necessário, pois cada letra da palavra **VIDA** equivale a uma letra da palavra álgebra (figura 5).

| | | | | | | |
|---|---|---|---|---|---|---|
| V | I | D | A | V | I | D |
| A | L | G | E | B | R | A |

**Figura 5:** exemplo do uso da Cifra de Vigenère.

Para codificar as letras da frase é necessário usar a linha correspondente à letra da palavra-chave relacionada. Para V, por exemplo, utiliza-se o alfabeto da linha 26 e a coluna da letra A. Assim, a primeira letra "A" será traduzida como U, que é intersecção entre "V e A". Para I, usaremos a linha 8 e o "L" será traduzido como "S" e continua-se a cifragem, conforme a figura 6.

| Palavra-chave | V | I | D | A | V | I | D |
|---|---|---|---|---|---|---|---|
| Texto Normal | A | L | G | E | B | R | A |
| Texto Cifrado | U | S | I | D | V | Y | C |

**Figura 6:** cifragem utilizando a Cifra de Vigenère.

Como os jovens apaixonados da Inglaterra vitoriana não podiam expressar seu amor publicamente, eles 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.

A Cifra de Playfair 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 7.

| | | | | |
|---|---|---|---|---|
| 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 7:** 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 8 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 8:** 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 9.

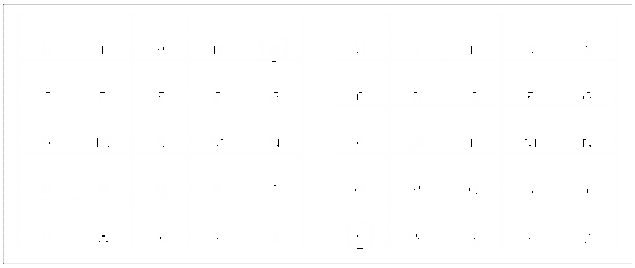


**Figura 9:** exemplo da cifragem do par AD utilizando a Cifra de Playfair.

Em 1918, foi introduzido o ADFGVX, uma cifra de guerra que se acreditava dar maior segurança às mensagens a serem enviadas, pois se tratava de uma cifra de substituição e transposição (consiste em rearranjar as letras da mensagem, gerando um anagrama). 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 10.

| | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | 8 | p | 3 | d | 1 | 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 10:** quadro da Cifra ADFGVX.

Inicia-se a codificação substituindo cada letra da mensagem a ser enviada, localizando a sua posição na grade, e substitindo-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 11.

| Palavra original | Lógica |
|---|---|
| Palavra codificada | DADGGVVGFGDV |

**Figura 11:** 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 12.

| | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | 8 | p | 3 | d | 1 | 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 |

l = DA

**Figura 12:** exemplo de codificação da Cifra ADFGVX.

De acordo com Singh (2003), com o avanço da Criptografia, Alberti foi o criador da primeira máquina criptográfica, o Disco de Cifras (figura 13). São dois discos de cobre, um maior que o outro, com as letras do alfabeto fixas ao longo dos discos, onde uma letra do texto normal se transformava em outra letra no texto cifrado.

**Figura 13:** exemplo de Disco de Cifras.

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.

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).

Um dos códigos, utilizados nos dias atuais, é o "Código de verificação ISBN" (*International Standard Book Number*). Este código é escrito como quatro blocos de dígitos separados por hífens ou por espaços em branco. Lendo-se da esquerda para a direita, o primeiro bloco identifica o país, a área ou a área da língua entre os participantes, o segundo bloco identifica as editoras daquele grupo e o terceiro bloco é o número atribuído pela editora para a obra. O último bloco, consiste em um único dígito de 0 a 9 ou um X, que representa $a_{10}$. Sendo os 9 primeiros dígitos do ISBN: $a_1$, $a_2$, $a_3$, $a_4$, $a_5$, $a_6$, $a_7$, $a_8$, $a_9$. Para calcularmos o dígito verificador do código ISBN, utilizamos a seguinte fórmula: $\left[\sum_{i=1}^{9} i(a_i)\right] \text{mod} 11$. Para encontrar o dígito verificador do código ISBN 852440124-X, procede-se da seguinte forma:

$$X = \left[\sum_{i=1}^{9} i(a_i)\right] \text{mod} 11$$

$X = [1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9]$ mod11

$X = [1.8 + 2.5 + 3.2 + 4.4 + 5.4 + 6.0 + 7.1 + 8.2 + 9.4]$ mod11

$X = [8 + 10 + 6 + 16 + 20 + 0 + 7 + 16 + 36]$ mod11

$X = 119$ mod 11

$X = 9$

Assim, o dígito verificador é 9.

## Atividades envolvendo os conteúdos de Matemática do Ensino Médio

a) Código com função linear

Atividade: Considere a figura 14 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 14:** Valor numérico de cada letra utilizada na criptografia para função.

Resolução da atividade: Primeiro relaciona-se cada letra do alfabeto a um número, conforme a figura 14.

Assim, tem-se a função codificadora: $f(x) = 5x + 1$. O texto a ser criptografado é: A vida é bela. A sequência numérica do texto é: 1 – 22 – 9 – 4 – 1 – 5 – 2 – 5 – 12 – 1.

Criptografa-se a mensagem a ser transmitida, realizando o calculo da imagem da função, conforme se observa a seguir:

| | | |
|---|---|---|
| $f(1) = 5.1 + 1 = 6$ | $f(22) = 5.22 + 1 = 111$ | $f(9) = 5.9 + 1 = 46$ |
| $f(4) = 5.4 + 1 = 21$ | $f(5) = 5.5 + 1 = 26$ | $f(2) = 5.2 + 1 = 11$ |
| $f(12) = 5.12 + 1 = 61$ | | |

Encontrando como texto codificado a sequência numérica: 6 – 111 – 46 – 21 – 6 – 26 – 11 – 26 – 61 – 6.

Para decodificar a mensagem o receptor calcula a imagem, dos elementos utilizando a função inversa: $f^{-1}(x) = \frac{x-1}{5}$.

a) Código com função quadrática

Atividade: Considere a figura 27 e codifique a palavra "O livro é uma caixa mágica.", utilizando o Código com Função Quadrática, sabendo que a função codificadora é $f(x) = x^2 + 2x + 6$.

Resolução da atividade: Primeiro relaciona-se cada letra do alfabeto a um número, conforme a figura 14.

Assim, tem-se a função codificadora: $f(x) = x^2 + 2x + 6$. O texto a ser criptografado é: O livro é uma caixa mágica. A sequência numérica do texto 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, calcula-se a imagem da função para cada número, da sequência numérica, na função escolhida.

| | | |
|---|---|---|
| $f(15) = 15^2 + 2.15 + 6 = 261$ | $f(18) = 18^2 + 2.18 + 6 = 366$ | $f(1) = 1^2 + 2.1 + 6 = 9$ |
| $f(12) = 12^2 + 2.12 + 6 = 174$ | $f(5) = 5^2 + 2.5 + 6 = 41$ | $f(3) = 3^2 + 2.3 + 6 = 21$ |
| $f(9) = 9^2 + 2.9 + 6 = 105$ | $f(21) = 21^2 + 2.21 + 6 = 489$ | $f(24) = 24^2 + 2.24 + 6 = 630$ |
| $f(22) = 22^2 + 2.22 + 6 = 534$ | $f(13) = 13^2 + 2.13 + 6 = 201$ | $f(7) = 7^2 + 2.7 + 6 = 69$ |

Sendo a sequência 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.

Para decodificar a mensagem o receptor recebe a mensagem e calcula a imagem dos elementos,k utilizando a função inversa: $f^{-1}(x) = \frac{-2 \pm \sqrt{-20+4x}}{2}$, como $x \in Z$ e $1 \leq x \leq 26$, então $f^{-1}(x) = \frac{-2+\sqrt{-20+4x}}{2} = -1+\sqrt{-5+x}$.

b) Código com função exponencial e logarítmica

Atividade: Codifique e decodifique a palavra "MATEMÁTICA", utilizando a figura 28, sabendo que a função codificadora é $f(x) = 2^x$.

Resolução da atividade: Primeiramente relaciona-se para cada letra do alfabeto um número, que corresponderá aos valores de x na função, conforme a figura 14.

Assim, tem-se a função codificadora: $f(x) = 2^x$. A palavra a ser criptografada é: Matemática. A sequência numérica do texto é: 13 – 1 – 20 – 5 – 13 – 1 – 20 – 9 – 3 – 1.

Para codificar calcula-se a imagem da função para cada algarismo da sequência numérica do texto a ser codificado, como se observa a seguir.

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

Para decifrar o texto, calcula-se a imagem da inversa da função codificadora, conforme se observa a seguir.

| 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 |

c) Código com matrizes

Atividade: Considere a tabela da figura 14 e codifique a palavra "FELICIDADE", sabendo que a matriz codificadora é $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$.

Resolução da atividade: Primeiramente relaciona-se para cada letra do alfabeto um número, conforme a figura 14. Escolhe-se uma matriz A, que corresponde a matriz $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ e a matriz inversa $A^{-1}$, que corresponde a matriz $A^{-1} = \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix}$.

Assim, tem-se a matriz codificadora: $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$. A palavra a ser criptografada é: Felicidade. A sequência numérica da palavra é: 6 – 5 – 12 – 9 – 3 – 9 – 4 – 1 – 4 – 5.

Para codificar monta-se a matriz M que corresponde à sequência numérica da mensagem que se deseja enviar, $M = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$. Em seguida, multiplica-se as matrizes A e M para encontrar a sequência numérica da palavra codificada. Veja:

$$AM = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix}.$$

Para decodificar utiliza-se a identidade matricial, isto é, calcula-se a matriz: $M = A^{-1}(AM) =$

$$\begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix} \cdot \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}.$$

Obs.: Se o número de letras na mensagem for ímpar dobra-se a última letra.

## Conclusão

Entende-se que o tema Criptografia pode e deve ser incluído nos currículos de Matemática do Ensino Médio. Porém, algumas considerações devem ser observadas:

- as atividades com o tema Criptografia devem ser motivadoras e relacionadas aos conteúdos desenvolvidos em sala de aula;
- é necessário conhecer os conhecimentos prévios dos alunos para que as atividades não sejam nem muito fáceis nem muito difíceis;
- a metodologia resolução de problemas é indicada para o desenvolvimento de atividades didáticas com o tema Criptografia, sendo importante que os futuros professores de Matemática, durante a sua formação, desenvolvam atividades didáticas que envolvam os conceitos matemáticos do Ensino Superior relacionados com os temas desenvolvidos no Ensino Médio, como a atividade apresentada nesse artigo com o tema Criptografia, permitindo a reflexão da importância e da necessidade da realização de uma transposição didática adequada ao Ensino Médio.

**Referências**


BRASIL, Ministério da Educação, Secretaria de Educação Média e Tecnológica (Semtec). **Parâmetros Curriculares Nacionais para o Ensino Médio.** Brasília: MEC/Semtec, 1998.

CANTORAL, Ricardo et al. **Desarrollo del pensamiento matemático**. México, Trillas: ITESM, Universidade Virtual, 2003.

D'AMBROSIO, Ubiratan. **O uso da calculadora.** Disponível em: www.ima.mat.br/ubi/pdf/uda_006.pdf. Acesso em 26 ago. 2009.

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.

KRIST, Betty J. Logaritmos, **Calculadoras e o Ensino de Álgebra Intermediária.** In: COXFORD, A. F.; SHULTE, A. P. As ideias da álgebra. São Paulo: Atual, 1995.

SCHEINERMAN, Edward R. **Matemática discreta:** uma introdução. São Paulo: Thompson, 2003.

SILVA, A. V. **A calculadora no percurso de formação de professores de Matemática.** Portugal: APM, 1991.

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). Nº 12, 1º semestre de 1988, 1-6.

ZATTI, Sandra Beatriz; 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 26 ago. 2009.


---

[i] Pesquisa vinculada ao convênio ULBRA – HP Calculadoras.

[ii] Doutora em Ciências da Educação. Professora do Programa de pós-graduação em Ensino de Ciências e Matemática. Universidade Luterana do Brasil

[iii] Mestra em Ciências da Educação. Professora do Programa de pós-graduação em Ensino de Ciências e Matemática. Universidade Luterana do Brasil