CÓDIGOS E SENHAS: SEQUÊNCIA DIDÁTICA COM O TEMA CRIPTOGRAFIA NO ENSINO FUNDAMENTAL

Claudia Lisete Oliveira Groenwald
Universidade Luterana do Brasil
claudiag@ulbra.br

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

Resumo: O presente artigo apresenta o tema Criptografia para o desenvolvimento de atividades didáticas com o uso de Códigos e Senhas, que incentivem o manuseio de calculadoras no Currículo de Matemática do Ensino Fundamental. Hoje, a Criptografia é utilizada em várias atividades da vida cotidiana, como em auditorias eletrônicas, na autenticação de ordens eletrônicas de pagamento, no código de verificação do ISBN, pelos navegadores de Internet, entre outras situações É importante que o professor trabalhe com temas atuais, que propiciem ao educando o contato com as calculadoras, tendo em vista, que elas possibilitam que o estudante dedique maior concentração nas estratégias para resolução de problemas, no lugar de dedicar tempo a cálculos longos e repetitivos que não é o objetivo das atividades.
Palavras-chave: Educação Matemática; Criptografia; Calculadoras; Currículo no Ensino Fundamental.

Introdução

Neste artigo, apresenta-se o tema Criptografia como motivador de situações problemas para o processo de ensino e aprendizagem, visto que este tema proporciona ao professor de Matemática desenvolver atividades didáticas de Códigos e Senhas no Currículo de Matemática do Ensino Fundamental de forma a proporcionar aos alunos o uso da calculadora.

Apresenta, também, as atividades propostas durante um experimento desenvolvido com alunos do Ensino Fundamental, relacionando os conteúdos de expressões algébricas de grau 2, potenciação, radiciação, operações com frações e operações com números naturais com o tema em estudo.

Trabalhar com atividades metodológicas utilizando Códigos e Senhas oportunizam aos alunos reforçar os conteúdos matemáticos já estudados, utilizar a calculadora como um recurso facilitador para cálculos longos, e ainda favorece o trabalho de grupo.

1 JUSTIFICATIVA DO TEMA

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 ou ciência de escrever em códigos (TAMAROZZI, 2001), de forma a permitir que somente o destinatário a decifre e compreenda. Para Shokranian (2005), enviar uma mensagem em código pode servir para dois objetivos, que são: enviar uma mensagem secreta e proteger o conteúdo da mensagem contra pessoas não autorizadas.

Ao longo da história, foram utilizados diversos mecanismos de codificação e decodificação, denominados códigos, cifras e senhas, um exemplo é o *Citale* Espartano (SINGH, 2003), que foi 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.

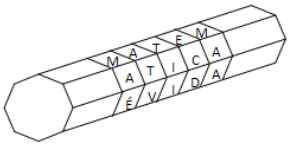


Figura 1: exemplo de *Citale* Espartano.

Outra forma de codificação foi a cifra monoalfabética[1], 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 deslocam-se no alfabeto original três casas, conforme apresentado na figura 2:

[1] A cifra monoalfabética utiliza um alfabeto para codificar uma mensagem (SINGH, 2003).

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, adaptado de Singh (2003)

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

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[2], 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 3.

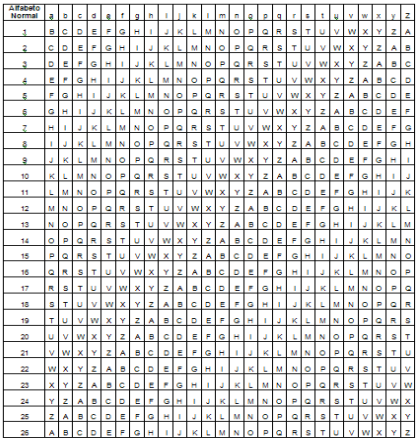


Figura 3: quadro de Vigenère, segundo Singh(2003, p. 66)

Segundo Singh (2003), para codificar uma mensagem pelo Quadro de Vigenère, primeiramente, escolhe-se uma palavra-chave, por exemplo: **FLOR.** A frase a ser codificada será "LUCIANA ADORA ROMÃ". Para codificar a mensagem, temos que escrever a palavra-chave quantas vezes forem necessárias, pois cada letra da palavra **FLOR** equivale a uma letra na frase, conforme apresentado na figura 4.

F	L	O	R	F	L	O	R	F	L	O	R	F	L	O	R
L	U	C	I	A	N	A	A	D	O	R	A	R	O	M	Ã

Figura 4: 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 "F", por exemplo, usaremos o alfabeto da linha 5, assim, o

[2] A cifra polialfabética utiliza mais de um alfabeto para codificar (SINGH, 2003).

primeiro “L” da frase será traduzido como “Q”. Para “L”, usaremos a linha 11 e o “U” seria traduzido como “F”. A frase codificada ficará conforme a figura 5.

Palavra Chave	F	L	O	R	F	L	O	R	F	L	O	R	F	L	O	R
Mensagem	L	U	C	I	A	N	A	A	D	O	R	A	R	O	M	Ã
Mensagem codificada	Q	F	Q	Z	F	Y	O	R	I	Z	F	R	W	Z	A	R

Figura 5: exemplo do uso da Cifra de Vigenère.

Constata-se, através dos exemplos mostrados, que a Criptografia, foi utilizada no decorrer da história. Outras abordagens desse tema são as aplicações em auditoria eletrônica, na autenticação de ordens eletrônicas de pagamento, nos navegadores de Internet, entre outras situações da vida cotidiana, o que demonstra ser esse um recurso de vasta aplicabilidade. No Brasil, segundo Terada (1988), recentemente se tem utilizado a Criptografia para proteger os sistemas eletrônicos e as informações sigilosas, contra modificações e falsificações dos dados eletrônicos no país.

A Criptografia é um tema atual que possibilita o desenvolvimento de atividades didáticas (Tamarozzi, 2001), que podem ser desenvolvidas no Ensino Fundamental, que levem os alunos a aprimorarem seus conhecimentos, levando-os a adquirirem as habilidades e competências de resolver problemas, criar estratégias de resolução, autonomia durante o processo de aprendizagem, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades e buscando interligar os conteúdos matemáticos às situações do mundo real (GROENWALD e FRANKE, 2008).

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 instrumento eles podem realizar experiências e desenvolverem suas próprias idéias e estratégias. O professor de Matemática pode se utilizar da calculadora em sala de aula de forma planejada e, assim, ela pode se tornar 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. Ainda, segundo os Parâmetros Curriculares Nacionais (1998), o professor de matemática deve fazer uso da calculadora sempre que achar necessário ao aprendizado do aluno, porque ela contribui para um repensar do processo de aprendizagem da disciplina de Matemática.

2 OBJETIVO DA INVESTIGAÇÃO

O objetivo geral foi investigar o tema Criptografia e suas aplicações através da história, aplicando uma seqüência didática elaborada a partir desse tema no currículo de Matemática do Ensino Fundamental.

3 METODOLOGIA DA INVESTIGAÇÃO

A metodologia utilizada na investigação foi a Engenharia Didática, pois segundo Pais (2005) traz credibilidade à pesquisa e reforça a defesa do vínculo com a realidade da sala de aula e apresenta quatro fases: as análises preliminares, a concepção e análise *a priori* das situações didáticas, a experimentação e a análise *a posteriori* e validação.

Na fase das análises preliminares é realizada a análise do objeto em estudo e o educador deve levar em consideração as constatações empíricas, as concepções do aprendiz e compreender as condições através das quais será exposta a experiência, procurando, desta forma, destacar as principais descrições do tema Criptografia relacionando-o com o Currículo de Matemática.

Na fase da concepção e análise *a priori*, delimitaram-se as variáveis microdidáticas, que são o tema Criptografia e os conteúdos de Matemática do Ensino Fundamental, pois estas são relevantes para a pesquisa.

A aplicação da seqüência didática foi a fase onde se conseguiu aproximar os resultados práticos com a análise teórica, foram determinados os objetivos e as condições necessárias aos alunos para a realização do experimento.

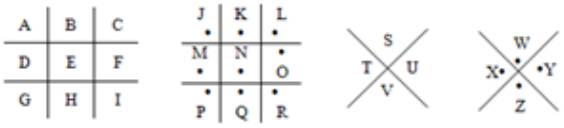
Na fase das análises *a posteriori,* foram analisados os dados da aplicação da seqüência didática obtidos através dos recursos: a observação direta do pesquisador, a gravação de áudio, a gravação de vídeo, questionários aplicados nos alunos participantes do experimento, a análise dos registros desses alunos.

A validação foi o processo de comparação dos objetivos pré-estabelecidos com os resultados obtidos nas análises a *priori* e a *posteriori*.

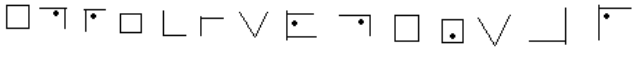
4 ATIVIDADES DIDÁTICAS DA INVESTIGAÇÃO

Atividade 1: Considere a seguinte mensagem: “O mundo é dos números!”. Utilize as cifras, abaixo relacionadas, para cifrar a mensagem.

a) Cifra de César; b) Cifra do chiqueiro



Atividade 2: Decifre cada uma das seguintes mensagens utilizando o código indicado: a) A cifra de César: HV WX GD UI DC EH P; b) A cifra do chiqueiro:



Atividade 3: Utilize o código a seguir para realizar as atividades.

A é divisível por 2, tal que A é $\left(\frac{3}{2}\right)^{2}+\frac{39}{4}$

B é primo, sendo B o número $169^{\frac{1}{2}}$

C é $2^{13}:2^{10}$

D é $8^{\frac{1}{3}}$

E é $\left(\frac{1}{2}\right)^{-4}$

F é $(0{,}01)^{0}$

G é $\sqrt{\frac{225}{25}}$

H é $\left(\frac{1}{10}\right)^{-1}$

I é $\sqrt[3]{8}.\sqrt{100}$

J é $5^{-4}.5^{6}$

K é $\left(\frac{1}{2}\right)^{-2}$

L é $5^{3}:\sqrt{625}$

M é $3^{-2}:3^{-4}$

N é $6^{7}.6^{-6}$

O é $\sqrt{11^{3}.11^{-1}}$

P é $289^{\frac{1}{2}}$

Q é $\sqrt{2^{3}+16^{3}+8^{3}}$

R é $7^{-2}.7^{6}.7^{-3}$

S é $\left(\frac{1}{3}\right)^{-1}\left(\frac{1}{7}\right)^{-1}$

T é $\sqrt{3^{2}}.\sqrt{9^{2}}$

U é $\left(\frac{1}{3}.\frac{1}{10}\right)^{-1}$

V é $\left(\frac{1}{2}\right)^{-2}.6$

X é $\left(\frac{1}{2}\right)^{-1}.\sqrt{2^{4}}$

Y é $\left(\frac{1}{6}\right)^{-1}:\frac{1}{7}$

Z é $4^{5}:2^{4}$

a) Descreva como encontrou o valor das letras C, D, G, L e Q, utilizando a calculadora.

b) Decodifique a mensagem: 21 – 16 – 9 – 17 – 16 – 9 – 12 – 27 – 16 – 9 – 12 – 27 – 20 – 8 – 12

Atividade 4: Seja o alfabeto abaixo, onde:

A é igual $\left(\frac{1}{5}\right)^2+\left(\frac{2}{5}:\frac{1}{2}\right)$

B é igual $\left(3+\frac{1}{2}\right).\left(2-\frac{3}{4}\right)$

C é igual $\frac{2}{3}\left(-\frac{1}{2}\right)+\frac{2}{5}$

D é igual $\left(-2+\frac{1}{3}\right)^2:\left(\frac{2}{3}-3\right)$

E é igual $\left(-2+\frac{1}{2}\right)^3.\left(\frac{3}{2}-\frac{1}{4}\right)$

F é igual $\left(-\frac{3}{2}\right)^2:\left[\left(-\frac{1}{4}\right)+\frac{1}{2}\right]$

G é igual $\frac{1}{2}:\left[2-\left(\frac{2}{3}+\frac{1}{4}\right)\right]$

H é igual $\frac{5}{3}-\left[\frac{1}{2}+\left(\frac{3}{4}:2\right)\right]$

I é igual $\left[\frac{7}{3}:\left(\frac{3}{2}+\frac{1}{3}\right)\right].\frac{2}{3}$

J é igual $\left[\left(\frac{1}{4}\right)^2+\left(\frac{1}{2}\right)^3\right]:\frac{2}{3}$

K é igual $\left[\left(\frac{1}{2}\right)^2+\left(\frac{1}{3}\right)^3\right].\left(2+\frac{6}{7}\right)$

L é igual $\left[\left(\frac{2}{7}\right)^2:\frac{1}{49}\right]+\left(\frac{1}{4}\right)^2$

N é igual $4-3\frac{4}{7}+\frac{1}{14}$

O é igual $3-1\frac{1}{6}+\frac{2}{3}$

P é igual $\frac{3}{4}-\left[\frac{1}{5}+\left(\frac{1}{2}\right)^3\right]:\frac{3}{5}$

Q é igual $\left(3-\frac{5}{3}\right)\left(2+\frac{1}{4}\right)$

R é igual $2\frac{1}{5}-1\frac{2}{5}$

S é igual $\left(\frac{23}{16}+\frac{5}{12}-\frac{49}{48}\right):\frac{6}{5}$

T é igual $\left(\frac{1}{4}+\frac{1}{6}\right)\left(\frac{1}{8}-\frac{1}{10}\right)$

U é igual $\left(1+\frac{1}{3}\right):1\frac{1}{7}$

V é igual $\frac{2}{3}+\frac{4}{5}.\frac{5}{7}-\frac{6}{21}$

W é igual $\frac{3}{5}:\left(\frac{1}{4}+\frac{1}{2}.\frac{2}{3}\right)$

X é igual $\left(\frac{1}{2}\right)^3+\frac{1}{4}+\left(5\frac{1}{6}\right)^0$

Y é igual $\sqrt{\frac{9}{16}}+\left[2-\left(\frac{1}{3}+\frac{1}{9}.\frac{6}{4}\right)\right]$

Z é igual $\sqrt[3]{\frac{1}{64}}+\frac{3}{4}-\left(\frac{1}{2}\right)^2$

a) Descubra o valor de cada letra; b) Codifique o seu primeiro nome; c) Utilizando somente as letras com denominadores múltiplos de 2, escreva uma palavra; d) Utilizando somente as letras com numeradores divisíveis por 5, escreva uma palavra.

5 ANÁLISE DOS DADOS

A fase de experimentação foi aplicada na turma 83, 8ª série da escola Estadual de Ensino Fundamental, no turno da manhã, em dois períodos a cada dia, totalizando dezesseis horas aula, no período de setembro a outubro de 2009. As calculadoras utilizadas no experimento foram cedidas pelo Laboratório de Matemática da Universidade Luterana do Brasil, pelo convênio ULBRA/HP Calculadoras.

Para realização das atividades didáticas propostas na fase da experimentação os alunos trabalharam em grupos, formando-se na turma 8 grupos, que foram denominados grupos: A, B, C, D, E, F e G. O trabalho em grupo possibilitou que os alunos interagissem entre si e entre os grupos para realização das atividades didáticas. Através das análises dos dados coletados, durante o experimento, pode-se constatar que os alunos compreenderam a proposta das atividades e conseguiram resolvê-las, demonstrando entusiasmo na realização das mesmas.

Na realização das atividades didáticas, os alunos não encontraram dificuldade na resolução da atividade 1, o que se pode observar na figura 6.

Resolução do grupo C: Para cifrar utilizando a Cifra de César, o grupo utilizou a tabela dada na atividade e escreveu a frase a ser codificada em cima e abaixo escreveu o texto codificado, como se observa na figura 7.

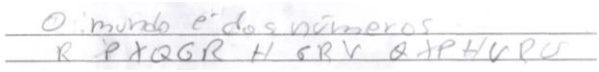


Figura 7: exemplo de atividade realizada pelo grupo C.

Figura 6: exemplo da resolução da atividade.

Também, se observou que os alunos se concentraram na resolução das atividades envolvendo a utilização da calculadora, pois era necessário que eles conhecessem esse recurso, conforme figura 8, onde dois alunos do grupo F estão tentando resolver a atividade.

Figura 8: imagem dos alunos resolvendo as atividades.

As atividades que foram aplicadas com o uso da calculadora oportunizaram aos alunos adquirirem conhecimento sobre esse tipo de tecnologia, conforme comentários dos grupos na figura 9.

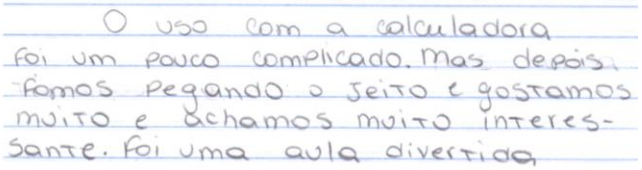
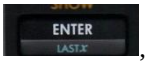


Figura 9: exemplo comentário do grupo A referente ao uso da calculadora 35s.

Além disso, permitiu que a explorassem e a utilizassem melhor, como exposto na figura 10.

Resolução do grupo C: Para encontrar o valor da letra A o grupo resolveu da seguinte forma na calculadora científica 35s

A é igual a $\left(\frac{1}{5}\right)^2 + \left(\frac{2}{5}.\frac{1}{2}\right)$

Primeiro apertaram a tecla do parêntese  , em seguida digitaram 1 ÷5 apertaram a tecla da seta para esquerda  , depois apertaram a tecla da potência  e em seguida, apertou a tecla do algarismo 2 e da operação de adição, apertaram novamente a tecla do parêntese  e digitaram 2 ÷5 x 1 ÷2 e apertaram a tecla  , conforme observa-se na figura 11.

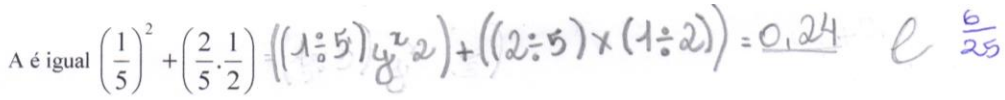


Figura 11: resolução da decodificação da letra A utilizando a calculadora 35s.

Como a calculadora estava programada para dar o valor em número decimal, os alunos tiveram a oportunidade de aprender a transformar o número decimal em fração utilizando a calculadora científica 35s, da seguinte forma: Após obter o valor decimal os alunos apertaram a tecla da seta amarela  e a tecla $/c$  , para voltar ao número decimal, apertavam a tecla da seta azul  e a tecla  .

Figura 10: exemplo da atividade de codificação com frações e o uso da calculadora 35s.

Importante observar que os alunos não demonstraram dificuldades no uso da calculadora 35s da HP.

Conclusão

Pode-se observar que as atividades de códigos e senhas possibilitaram aos alunos trabalhar o conceito de Criptografia, desenvolver a capacidade de concentração nas atividades e criar estratégias de resolução de problemas. As atividades didáticas desenvolvidas aliam os conteúdos matemáticos a um tema atual, apresentando diferentes situações e aplicações. As atividades desenvolvidas e aplicadas são exemplos de material didático que pode ser utilizado pelos professores para exercitar, aprofundar, fixar e revisar conteúdos, fazendo uso de códigos e senhas, conforme as indicações de Tamarozzi (2001).

A seqüência didática desenvolvida permitiu que os alunos explorassem os diversos recursos da calculadora científica, facilitando nos cálculos longos e na compreensão de conceitos matemáticos.

Referências

BRASIL, SECRETARIA DA EDUCAÇÃO FUNDAMENTAL. *Parâmetros Curriculares Nacionais:* Matemática. Brasília: MEC/SEF, 1998.

GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber. *Currículo de Matemática e o tema Criptografia no Ensino Médio.* Educação Matemática em Revista – RS. 2007, 51-57.

KRIST, Betty J. *Logaritmos, Calculadoras e o Ensino de Álgebra Intermediária.* In: *As Idéias da Álgebra*, organizadores: Arthur F. Coxford e Alberto P. Shulte; traduzido por Hygino H. Domingues. São Paulo: Atual, 1995.

PAIS, Luiz Carlos. *Didática da Matemática – Uma análise da influência francesa.* 2.ed. Belo Horizonte: Autêntica, 2005.

SHOKRANIAN, Salahoddin. *Criptografia para Iniciantes.* Brasília: UnB, 2005.

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.