

CRIOGRAFIA: UMA INVESTIGAÇÃO DAS POTENCIALIDADES COMO FERRAMENTA DE ESTUDO DA FUNÇÃO AFIM NO ENSINO MÉDIO

Josenaide Apolonia de Oliveira Silva¹; Suzana Ferreira da Silva²; Hugo Gustavo³

Universidade de Pernambuco, naydeoliveira@gmail.com¹;

Universidade de Pernambuco, suzanasilva.sf@gmail.com²;

Universidade de Pernambuco, hugo.lira.gomes@gmail.com³

Resumo: A escola básica precisa de um tema que traga significado e interesse do alunado, que também possibilite desenvolver conteúdos novos e clássicos da matemática no nível de escolaridade em que se está trabalhando. Esta necessidade está de acordo com os Parâmetros Curriculares Nacionais (PCN's) onde diz que é preciso existir contextualização nos conteúdos ensinados, pois todo conhecimento envolve uma relação entre sujeito e objeto, ou seja, entre o aluno e a matéria, assim se o conhecimento é trabalhado do modo contextualizado a escola irá retirar o aluno da sua condição de espectador passivo e fazer com que ele se interesse mais pelo conteúdo (BRASIL, 1997). Podemos notar que a matemática se relaciona com vários outros campos científicos, como a tecnologia e o pensamento computacional. Bem como a matemática, o pensamento computacional e a tecnologia são importantes para o ensino médio, corpo científico e toda sociedade. Com isso, e tendo em mente que um dos conteúdos matemáticos posto pelos PCNs a ser ensinado no ensino médio é a função afim, diante do que foi exposto, formulou-se a seguinte questão de pesquisa: Quais as potencialidades da Criptografia como ferramenta didática no ensino e aprendizagem da função afim?

Palavras-chave: Contextualização matemática; Criptografia; Função Afim.

INTRODUÇÃO

O tema Criptografia veio à tona ao conhecê-lo em uma oficina da XIII SEMAT – Semana de Matemática da Universidade Federal Rural de Pernambuco (UFRPE), onde se constatou que além deste tema está presente na atualidade (redes sociais, transações bancárias, compra online, entre outros), apoia-se na Matemática para assegurar o sigilo necessário na comunicação.

Diversos são os motivos pelos quais se tem o interesse de ocultar uma mensagem. Ela pode ser utilizada em sigilo de banco de dados, censos, investigações governamentais, dados hospitalares, informações de crédito pessoal, comandos militares, entre outros.

Assim, neste estudo pretende-se discutir a potencialidade da criptografia como ferramenta de estudo da função afim, pois a importância de buscarem-se métodos dinâmicos e temas atuais no processo de aprendizagem da matemática, também está previsto nas Orientações Curriculares para o Ensino Médio (PCNEM) (2006) e na Base Nacional Comum Curricular (BNCC) (BRASIL, 2015), onde as orientações dadas aos professores remetem às estratégias de ensino respaldadas na resolução de problemas e sugerem que deve partir dos conhecimentos prévios dos alunos e ajudá-los a ampliar e dar sentido matemático a tais conhecimentos.

Sabendo que a sociedade está integrada numa rede de informações crescentemente globalizada e voltando-se para a matemática, mais especificamente para a função da matemática, nota-se que o seu estudo necessita ser mais do que memorizar resultados oriundos dessa ciência, fazendo-se necessário a contextualização e interdisciplinaridade, ou seja, permitir conexões entre diversos conceitos matemáticos e aplicações dentro e fora da matemática.

Nesse sentido, dentro deste contexto a Criptografia é um tema com potencial didático para contextualização de conteúdos matemáticos, apresentando material útil para a compreensão de importantes conceitos matemáticos, pois não existe um método pronto para se decifrar uma mensagem e assim, realizar atividades envolvendo problemas criptográficos abrem um leque de possibilidades de resolução, além de despertar a curiosidade e condutas de investigador nos estudantes.

Nessa direção Olgin e Groenwald (2011) concluem que:

A criptografia é um exemplo de tema que pode ser abordado no Currículo do Ensino Médio, pois permite desenvolver atividades didáticas utilizando padrões e regras de codificação e decodificação, trabalhar os conteúdos matemáticos, já desenvolvidos em sala de aula pelos professores, dentro de um contexto que envolva segurança de dados, possibilita recontextualizar um conteúdo dentro de outro tema, produzindo novos significados e relações enriquecedoras.

Um dos conceitos matemáticos que pode ser trabalhado juntamente com a Criptografia é o de funções, por isso essa foi nossa opção de trabalho, mais especificamente com a função afim, visto também que, no PCNEM (2006) fala que o ensino isolado deste tema não permite a exploração do caráter integrador que ele possui.

METODOLOGIA

Para tentar alcançar o objetivo da pesquisa opta-se, por desenvolver uma intervenção de caráter qualitativo, visto que para tentar encontrar respostas ao objetivo da pesquisa será preciso compreender e analisar o processo discutido e vivenciado pelos estudantes acerca das investigações que pretendesse desenvolver com eles durante a resolução das atividades propostas.

Em um primeiro estágio do projeto foi desenvolvido um estudo exploratório acerca do tema criptografia, desde a história até algumas aplicações no cotidiano e a relação com a função afim, pois entendemos que é possível trabalhar o conteúdo de função afim de uma maneira diferente.

O uso da criptografia durante as aulas é interessante, pois poderá despertar o interesse dos estudantes e, além disso, poderá contribuir para a fuga de métodos tão tradicionais, como ela é aplicada em diversos ramos do cotidiano, aprofundar um mínimo possível no tema e trazer

essas descobertas para o ambiente escolar, já motiva esses estudantes a voltarem nas aulas de matemática.

Inicialmente é interessante tratar com os estudantes, os termos relacionados como chave (senha ou código) utilizada para cifrar ou decifrar uma mensagem, seguido de uma atividade construída com a intenção de relacionar criptografia e função afim a partir de exemplos.

Na segunda etapa foi feita 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.

DISCUSSÃO E RESULTADOS

A necessidade de manter informações em segredo é muito antiga, sendo assim esse tipo de escrita, nas palavras de Bezerra, Malagutti, Rodrigues (2010) teve como pioneiros reis, rainhas e generais que buscavam durante as guerras uma alternativa para se comunicar com seus exércitos de forma que somente os envolvidos entendessem a mensagem.

Desta forma, surgiram inúmeros grupos com o objetivo de criar modos de se ocultar uma mensagem, bem como grupos de decifradores, para tentar as mensagens que foram escondidas.

A primeira forma de se ocultar uma mensagem foi a estemografia segundo Bezerra, Malagutti, Rodrigues (2010), mas não era uma forma viável, porque demandava muito tempo e não era segura, com isso desenvolveu-se a criptografia.

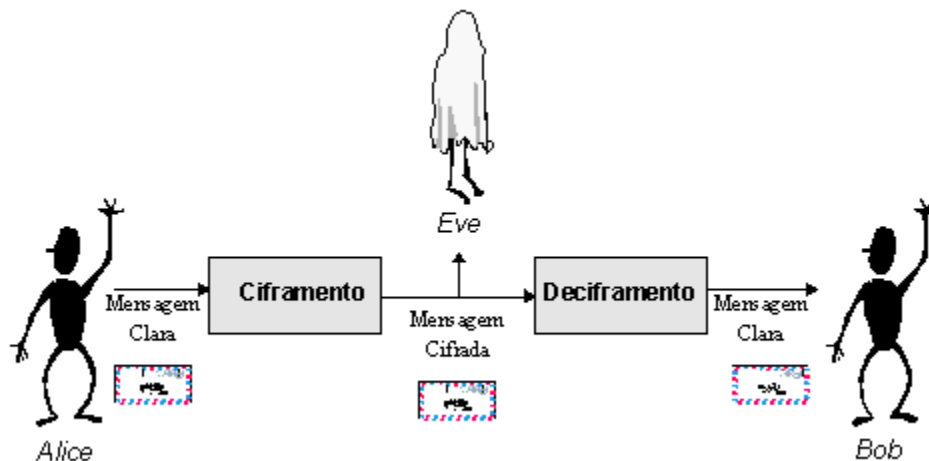
A criptografia essencialmente muda textos originais, para uma informação transformada, chamada texto cifrado, texto código ou somente cifra, que normalmente se parece com um texto aleatório ilegível. “A criptografia é conhecida como a arte ou ciência de escrever em cifra ou em código, de forma a permitir que somente o destinatário a compreende.” (SINGH, 2003).

As palavras mais comuns utilizadas na criptografia são cifrar e decifrar, onde, 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 mesmo que esta consiga visualizar os dados criptografados e decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, descomplicada.

A vantagem de se usar a criptografia é que mesmo um inimigo ou alguém que não deveria conseguir ter acesso à mensagem, é provável que o interceptador não consiga entendê-la, por que para isso ele precisaria de informações confidenciais normalmente chamadas de chaves ou senhas.

O conteúdo matemático de funções pode ser utilizado como chaves cifradoras e decifradores, onde o aluno do Ensino Médio aplica os conceitos matemáticos em situações práticas de criptografia, pois a função afim possui a característica de ser irredutível, o que garante que o processo de codificação da mensagem seja reversível e assim suas informações podem ser reveladas aos receptores (TAMAROZZI, 2000).

O esquema a seguir representa este processo:



Um exemplo de abordagem desse tema no meio acadêmico encontra-se na apostila de “Criptografia” do Programa de Iniciação Científica da Olimpíada Brasileira de Matemática das Escolas Públicas (PIC-OBMEP) (COUTINHO, 2015).

A seguir apresenta-se um exemplo de atividade didática que pode ser utilizada pelos professores do Ensino Médio apresentando o tema Criptografia como um recurso didático no ensino da matemática.

Proposta Pedagógica

A partir das discussões feitas acima apresentamos uma esquematização de atividade que podemos trabalhar na turma do ensino médio. Essa atividade é apenas uma sugestão, pois a relação da matemática com a criptografia envolvendo a função afim acontece de várias formas e o professor pode trabalhar isso da maneira que melhor se adapta a realidade da sua escola e alunos.

A presente proposta pedagógica tem como objetivo apresentar os aspectos relevantes da Criptografia por meio de vídeos, slides explicativos, apresentação oral e atividades. Além disso, pretende-se mostrar a relação da Criptografia com o conteúdo matemático Função Afim.

Para iniciar a proposta é necessário fazer um questionamento aos participantes sobre o que já ouviram falar sobre Criptografia, logo após apresentar um vídeo contendo a definição de

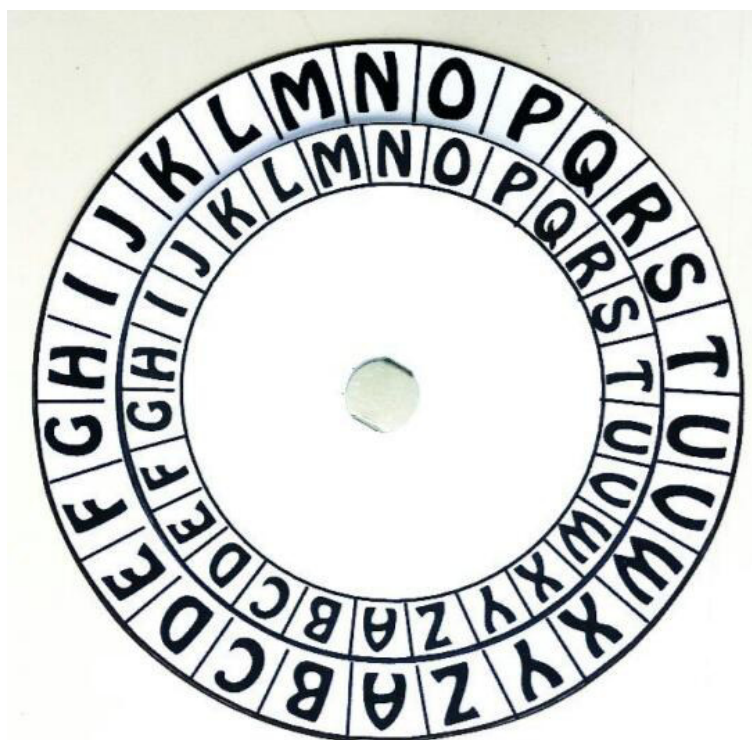
Criptografia, complementando a explicação dos primeiros registros de utilização de mecanismos capazes de assegurar o sigilo na comunicação.

Dentre esses mecanismos, pode-se mostrar aos alunos alguns: Esteganografia (em slide e em exemplo concreto), Citale Espartano (em slide e em exemplo concreto), Cifra de César (em slide, material concreto e atividade).

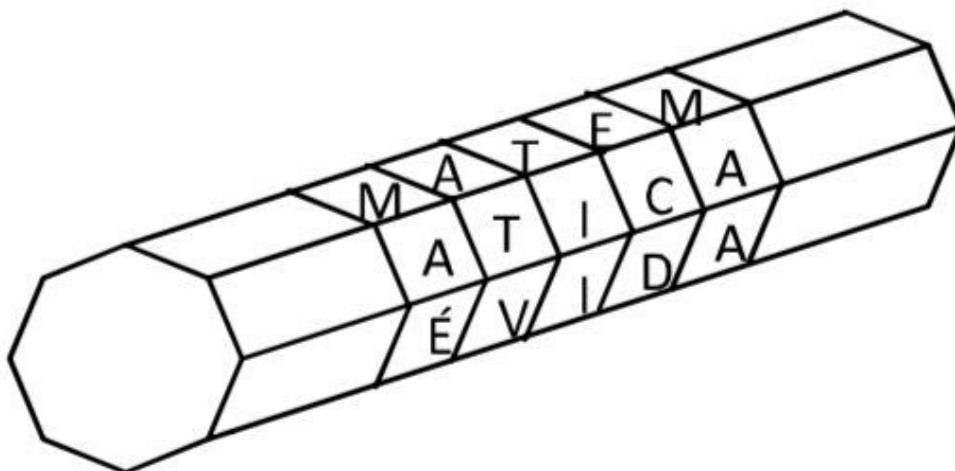
Também é necessário explicar de forma breve que além de existirem métodos para cifragem de mensagens, existem também métodos que são utilizados para fazer o processo inverso, isto é, decifrar mensagens.

Atividade 1 – Propor aos alunos que se dividam em grupos, onde cada grupo deve codificar uma frase de acordo com a Cifra fornecida a eles e envie para outro grupo decodificar.

Com essa atividade espera-se que nessa atividade o aluno encontre o valor de cada letra de acordo com o padrão utilizado pela Cifra fornecida, onde ele substituirá a letra do alfabeto normal pela sua posição, assim espera-se que o aluno encontre a mensagem cifrada.



Atividade 2 – Expor para os alunos que uma das primeiras formas de codificar foi o Citale Espartano (SINGH, 2003), que era um aparelho criptográfico militar, que consistia em uma bastão de madeira, onde se enrolava uma tira de couro e se escrevia a mensagem em todo o comprimento do bastão.



Atividade 3 – Propor que os alunos descubram uma mensagem utilizando uma Cifra de substituição monoalfabética, a Cifra do Chiqueiro, utilizada pelos maçons livres para guardar seus segredos (SINGH, 2003).



Esta atividade tem por objetivo proporcionar que o aluno se familiarize com o raciocínio a cerca da codificação de uma mensagem.

Atividade 4 – Sugerir que os alunos decodifiquem uma mensagem utilizando uma chave no formato de uma função afim.

Ao realizar a atividade o aluno começa a compreender onde está a relação entre a função afim em parceria com a Criptografia.

Atividade 5 – O professor fornece uma sequencia original de números e outra sequência codificada, para que assim os alunos tentem encontrar a chave e a mensagem que foi codificada.

A proposta é feita com o intuito de que o aluno construa novos conhecimentos através da descoberta.

Atividade 6 – Apresentar um problema em formato de Criptograma, onde cada letra indica um algarismo, letras iguais representam algarismos diferentes, e sabendo que cada letra tem um valor único variando de zero a nove, como no exemplo:

Assim nessa atividade o aluno será desafiado a resolver a atividade por tentativa e erro ou sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Atividade 7 – Cada grupo deve cifrar uma mensagem utilizando a função afim dada como chave.

Como nesta atividade será necessário cifrar uma mensagem utilizando o raciocínio lógico, além dos demais mecanismos apresentados, permite ao aluno se desenvolver de forma significativa.

Momentos	Atividade
1º momento – Atividade introdutória	O objetivo dessa atividade é introduzir o tema proposto e revisar o conteúdo de função afim, já trabalhado no ensino fundamental.
2º momento – Atividade didática envolvendo código com a função afim	O objetivo dessa atividade é revisar e reforçar o cálculo da imagem da função afim.

CONCLUSÕES

Espera-se com essa proposta, difundir a Criptografia que é um tema abrangente e atual, e sua história que é bem rica e interessante, possibilitando aos alunos, futuros profissionais significado à aprendizagem, pois se entende que o tema Criptografia apresenta material útil para exercícios de fixação de conteúdos, apresentando atividades e jogos de codificação (TAMAROZZI, 2000) que pode ser utilizados pelos professores 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 levado 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 da função afim de forma contextualizada.

REFERÊNCIAS

BRASIL. Base Nacional Comum Curricular. Brasília-DF: Ministério da Educação, 2015. Disponível em: <<http://basenacionalcomum.mec.gov.br/#/site/inicio>>. Acesso em: 7 de junho de 2018.

BRASIL. Ministério da Educação, Secretaria de Educação Básica. Orientações Curriculares Para o Ensino Médio: Ciências da Natureza, Matemática e suas tecnologias. Volume 2. Brasília: 2006.

BRASIL. Secretaria de Educação Fundamental. Parâmetros curriculares nacionais: introdução aos Parâmetros Curriculares nacionais – Brasília: MEC/SEF, 1997.

BEZERRA, Débora de Jesus; MALAGUTTI, Pedro Luiz e RODRIGUES, Vânia Cristina da Silva. Aprendendo Criptologia de forma divertida. V Biental da SBM. UFPB: 2010.

COUTINHO, Severino. Criptografia. Rio de Janeiro. IMPA: 2015.

DAMIANI, Magda Floriani. Sobre pesquisas do tipo intervenção. Campinas. UNICAMP: 2012.

GIL, Antonio Carlos. Métodos e Técnicas de Pesquisa social. São Paulo. Atlas: 1989.

MINAYO, Maria Cecília de Souza. Pesquisa social: Teoria, método e criatividade. Petrópolis. Editora Vozes: 2002.

OLGIN, Clarissa de Assis e GROENWALD, Cláudia Lisete Oliveira. Criptografia e o currículo de matemática no ensino médio. Revista de Educação Matemática – vol 13, número 15, 2011.

SINGH, Simon. O livro dos códigos: A ciência do sigilo – do antigo Egito à criptografia quântica. Record, 2010.

TAMAROZZI, Antonio. Codificando e decifrando mensagens. Revista do Professor de Matemática. Vol 45. Três Lagoas: 2000.