UNIVERSIDADE FEDERAL DE SANTA MARIA
UNIVERSIDADE ABERTA DO BRASIL
CENTRO DE CIÊNCIAS NATURAIS E EXATAS
CURSO DE ESPECIALIZAÇÃO EM ENSINO DE MATEMÁTICA NO ENSINO MÉDIO

Lidiane da Silva Dias

ENSINO DE FUNÇÕES E CRIPTOGRAFIA RSA

Santa Maria, RS
2019

Lidiane da Silva Dias

ENSINO DE FUNÇÕES E CRIPTOGRAFIA RSA

Trabalho de conclusão apresentado ao curso de Especialização em Ensino de Matemática no Ensino Médio (EaD), da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção de título de **Especialista em Ensino de Matemática no Ensino Médio**.

Orientadora: Profª. Drª. Carmen Vieira Mathias

Santa Maria, RS
2019

Lidiane da Silva Dias

ENSINO DE FUNÇÕES E CRIPTOGRAFIA RSA

Trabalho apresentado ao curso de Especialização em Ensino de Matemática no Ensino Médio, da Universidade Federal de Santa Maria (UFSM,RS), modalidade EAD, como requisito parcial para a obtenção de título de **Especialista em Ensino de Matemática no Ensino Médio**.

Aprovada em 06 de julho de 2019:

Carmen Vieira Mathias, Drª (UFSM)
Presidente/orientadora

Liane Terezinha Wendling Roos, Drª (UFSM)

Ivanilda Basso Aseka, Drª (UFSM)

Santa Maria, RS
2019

Dedico esta, bem como todas as minhas demais conquistas, ao meu esposo, Daniel e à minha filha, Sophia, que é quem me motiva a ser melhor tanto profissionalmente quanto pessoalmente.

AGRADECIMENTOS

Agradeço aos alunos e à equipe da escola em que foi implementado o planejamento, pois foram quem tornaram possível a conclusão dessa monografia.

À professora orientadora, Carmen e também à coordenadora do curso, professora Fabiane, pela orientação, apoio e compreensão, que foram tão importantes no desenvolvimento dessa monografia.

Aos meus pais, meu esposo e minha filha pelo carinho e por sempre me apoiarem.

Aos meus sogros e principalmente à minha sogra que está sempre pronta para me ajudar.

Enfim, a todos que de alguma forma me ajudaram para que se desse a conclusão desse trabalho.

“Não há nada como o sonho
para criar o futuro”.
Vitor Hugo

RESUMO

ENSINO FUNÇÕES E CRIPTOGRAFIA RSA

AUTORA: LIDIANE DA SILVA DIAS
ORIENTADORA: CARMEN VIEIRA MATHIAS

Atualmente um dos maiores desafios para os professores de matemática é despertar o interesse nos alunos. E em meio a esse contexto, o objetivo desse trabalho é apresentar uma alternativa didática contextualizada na forma de um planejamento, onde está relacionado um tema atual, como a criptografia RSA com o conteúdo de funções. Esse planejamento foi aplicado em uma turma de 1º ano do Ensino Médio em uma Escola Estadual do município de Santa Maria, com duração de duas horas/aulas. O planejamento apresenta duas atividades que propõem a participação e interação dos alunos, as atividades serviram como meio para o desenvolvimento das habilidades que levaram os alunos a atingir os objetivos, despertando motivação e colaborando para o ensino e aprendizagem do conteúdo.

Palavras-chave: Criptografia RSA. Funções. Planejamento.

ABSTRACT

TEACHING FUNCTIONS AND RIP CRYPTOGRAPHY

AUTHOR: LIDIANE DA SILVA DIAS
ADVISOR: CARMEN VIEIRA MATHIAS

Currently one of the greatest challenges for math teachers is to arouse interest in students. And in the midst of this context, the objective of this work is to present a didactic alternative contextualized in the form of a planning, where a current theme, such as RSA encryption with the content of functions, is related. This planning was applied in a 1st year high school class in a State School in the municipality of Santa Maria, with a duration of two hours / classes. The planning presents two activities that propose the participation and interaction of the students, the activities served as a medium for the development of the abilities that led the students to reach the objectives, arousing motivation and collaborating for the teaching and learning of the content.

Keywords: RSA Encryption. Functions. Planning.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Ensinar sempre foi uma nobre e árdua tarefa designada aqueles que se dispõe a compartilhar os saberes com seus aprendizes e dessa forma possibilitar a evolução através dos conteúdos ensinados. Como o ser humano é um ser social e constrói seu conhecimento do resultado da interação entre o sujeito e a realidade que o cerca, acredita-se que o educador precisa ter competência técnica, metodológica e saber criar um ambiente favorável ao aprendizado.

Nesse enfoque, planejar uma aula que atenda às necessidades de aprendizagem dos alunos de forma contextualizada é indispensável. O planejamento de aula é uma atividade inerente ao trabalho do professor e é uma função muito importante para o fazer docente, que exige dele um trabalho de reflexão sobre o ensino e a aprendizagem.

O professor tem um papel muito importante no aprendizado do aluno tornando, assim, necessário a reflexão sobre como ensinar, como avaliar e como organizar as situações de ensino e aprendizagem da matemática. Ao analisar o ensino e a aprendizagem de matemática, Chevallard, Bosch e Gascón (2001, p. 45) afirmam que "a presença da matemática na escola é uma consequência de sua presença na sociedade e, portanto, as necessidades matemáticas que surgem na escola deveriam estar subordinadas às necessidades da vida em sociedade".

Além disso, Pais (2002) aborda a importância de contextualizar os saberes ensinados na escola a fim de estruturar uma educação matemática mais significativa para os alunos.

> A contextualização do saber é uma das mais importantes noções pedagógicas que deve ocupar um lugar de maior destaque na análise da didática contemporânea. Trata-se de um conceito didático fundamental para a expansão do significado da educação escolar. O valor educacional de uma disciplina expande na medida em que o aluno compreende os vínculos do conteúdo estudado com um contexto compreensível por ele. (PAIS, 2002, p. 27).

Assim, acredita-se que uma das diversas formas de contextualizar o conteúdo da disciplina de matemática seria vincular conhecimentos de um tema atual, como a criptografia, com alguns conteúdos da disciplina, tornando, assim, a aprendizagem de tais conceitos mais significativos. As técnicas para criptografar mensagens, palavras, frases ou textos através de permutações, funções ou matrizes, além de estimular a aprendizagem, pode ser um meio de concretizar esses saberes.

Para Filho e Malagutti, a criptografia RSA[1] é um sistema que integra duas chaves:

[1] As letras RSA referem às iniciais dos nomes dos inventores do código

> A ideia do sistema é a seguinte: uma das chaves serve para cifrar mensagens e pode ser divulgada livremente – todos têm acesso a ela – por isso é conhecida como *chave pública*. Por outro lado, para decifrar a mensagem cifrada, há a necessidade de uma chave secreta, conhecida apenas pela pessoa para a qual a mensagem foi enviada, por isto essa chave é conhecida como *chave secreta.* (FILHO; MALAGUTTI, 2013, p. 73).

Diante do exposto, procura-se nesse trabalho mostrar que é possível aliar o conhecimento de criptografia RSA com o conteúdo de funções, abordando uma alternativa didática na forma de experimento. Acredita-se que ao levar esse assunto para as aulas é possível apresentar novas aplicações para o estudo de funções, visto que criptografia é um tema que pode despertar curiosidade nos alunos. Dessa forma, o objetivo desse trabalho é introduzir o conceito de criptografia visando a construção e aquisição do conhecimento do conteúdo de funções.

Optou-se por esse tema, pois acredita-se que propor e oferecer temas de atualidades como ferramentas para fortalecer o ensino da matemática, principalmente no Ensino Médio, poderá contribuir para o enfrentamento de desafios postos no cotidiano dos alunos conectando-os a realidade de nossa sociedade tecnológica e globalizada.

A implementação do planejamento proposto neste trabalho foi realizada em uma Escola Estadual de Ensino Médio, localizada na região urbana de Santa Maria – RS. A escola é ampla, tem sala de informática e biblioteca. A turma em que foi aplicado o planejamento era composta por 18 alunos todos entre 15 e 16 anos.

Esse trabalho é composto por 3 capítulos, o primeiro aborda o assunto de criptografia RSA, o segundo apresenta o planejamento que foi elaborado e o último uma análise da atividade desenvolvida com a turma. Por fim, são apresentadas as considerações finais e a resposta ao objetivo do trabalho.

2 CRIPTOGRAFIA RSA E FUNÇÕES

As possibilidades tecnológicas e as redes de computadores surgiram como uma alternativa da era moderna, auxiliando e muitas vezes facilitando a comunicação. No entanto, o ritmo acelerado das inovações tecnológicas e da abrangência de redes, como a internet, foram exigindo com que a educação também acelerasse o passo para tornar o ensino mais criativo e estimulante.

A internet está presente em nosso cotidiano e é através dela que muitas vezes mantemos contato com a família, amigos, nos relacionamos no meio corporativo, encontramos pessoas, empresas, segmentos e serviços, acompanhamos notícias, participamos de cursos e nos capacitamos, gerenciamos a vida financeira, compramos, investimos, emitimos documentos, ou seja, tudo hoje é facilitado e agilizado por meio do uso da internet.

Com o avanço cada vez maior das redes de computadores e com o crescimento da necessidade de transferência de dados com segurança, começaram a ser desenvolvidos algoritmos criptográficos para assegurar a integridade dos dados, assim assegurando uma comunicação segura entre as duas partes. Segundo Malagutti (2015), com o advento da comunicação eletrônica, muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da internet.

Além disso, conforme o autor, "A ciência que estuda sistemas de envio e recepção de mensagens secretas chama-se CRIPTOGRAFIA" (MALAGUTTI, 2015, p. 2), deste modo, a criptografia oculta o significado de uma mensagem, transformando um texto normal em texto secreto. Para transformar uma mensagem em mensagem secreta é preciso codificar a mensagem e para fazer o processo inverso é preciso decodificar a mensagem.

Conforme Singh (2015, p. 51) "A criptografia tem sido aprimorada e estado presente desde antes de Cristo seu desenvolvimento é marcado por três grandes fases: artesanal, mecânica e digital". Ainda, de acordo com o autor:

> A criptografia Digital veio com o aperfeiçoamento dos computadores, fazendo cálculos extremamente grandes em pouco tempo, se tornaram uma ferramenta valiosa na criptografia, com códigos mais complicados de serem quebrados, pode-se observar a criptografia simétrica DES, AES, IDEA, Assimétrica, RSA, ElGamal, Curvas Elípticas, dentre outras. (SINGH, 2015, p. 60).

Assim sendo, a criptografia RSA é um exemplo de criptografia Digital e atualmente é um dos sistemas utilizado em rede. Segundo Coutinho (2011, p.13):

> Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute or Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no *Netscape*, o mais popular dos *softwares* de navegação da *Internet*. (COUTINHO, 2011, p.13).

O segredo da criptografia RSA está em esconder de maneira eficiente o processo para a inversão da função. Os sistemas de criptografia clássicos perderam sua eficácia devido à facilidade com que atualmente são decodificados, utilizando qualquer computador doméstico.

Na criptografia em rede, a mensagem é criptografada usando-se algoritmos gerando diversos códigos que executam a criptografia. O algoritmo RSA é seguro pois para um atacante saber a chave privada é praticamente impossível, é algo computacionalmente inviável.

> A eficácia desse sistema de chaves duplas está na "impossibilidade prática" de se obter a chave secreta a partir da chave pública. Isto porque o sistema utiliza números muito grandes, formados por muitos algarismos. Atualmente, não são conhecidos algoritmos capazes de decompor números muito grandes em fatores primos em um tempo razoável. Essa é uma impossibilidade técnica, ou seja, ainda não pode ser resolvida, mesmo com os avanços da Matemática e da Informática. (FILHO; MALAGUTTI, 2013, p.74).

Mas, como podemos empregar a criptografia RSA na aula de matemática? Bem, a criptografia RSA funciona, de modo geral, da seguinte forma: Uma pessoa pretende enviar uma mensagem à outra pessoa, de forma secreta. A primeira pessoa então, utilizando a criptografia RSA para codificá-la, troca as letras da mensagem por números e logo após utiliza a chave pública para criptografa-la, ou seja, utiliza uma função bijetora. A segunda pessoa que recebe a mensagem criptografada, deve conhecer a chave privada para decodificá-la, isto é, a segunda pessoa deve saber a função inversa da função utilizada para criptografar a mensagem.

Como, na criptografia RSA, qualquer função satisfaz para codificar as mensagens, desse modo é possível utilizar a criptografia RSA aliado ao conteúdo de funções, abordando o tema função inversa na disciplina de matemática. Porém, sendo ela utilizada em rede, se for uma função fácil de obter a inversa, será fácil a "quebra de código". Logo, para que esse sistema seja eficaz, a maneira é obter duas funções, de modo que esse processo seja seguro, o bastante, para que não haja a "quebra de código".

3 O PLANO DE AULA: ANÁLISE A PRIORI

Neste capitulo está exposto o planejamento de aula que foi motivado pelo desejo de trabalhar com um tema atual e presente no cotidiano dos alunos. Relacionar os conteúdos com temas atuais do dia-a-dia facilita a articulação entre a teoria e a prática permitindo ao aluno perceber a utilidade da matemática no seu contexto.

> Aprender significativamente é dar sentido à linguagem que usamos, é estabelecer relações entre os vários elementos de um universo simbólico, é relacionar o conhecimento elaborado com os fatos do dia-a-dia, vividos pelo sujeito da aprendizagem ou por outros sujeitos. (MORETTO, 202, p. 17).

Para elaborar essa atividade foi realizada uma pesquisa no site[2] Recursos educacionais multimídia para a matemática do Ensino Médio criado por professores da UNICAMP, onde foi encontrado uma atividade semelhante, denominada, Mensagens Secretas com Matrizes. Porém foi realizada a adaptação do material, de forma a trabalhar com o conteúdo de funções e realizar a aplicação do planejamento em uma turma de 1º ano do Ensino Médio.

3.1 Estrutura

Nível de ensino: Ensino Médio

Componente curricular: Matemática

Tema: Função

O que o aluno poderá aprender com esta aula?

- Conceito de criptografia;
- Fixar o conteúdo como função afim, imagem e função inversa

Duração das atividades

- 2 horas/aula

Conhecimentos prévios

- Criptografia, função afim, imagem e função inversa

Estratégias e recursos:

[2] https://m3.ime.unicamp.br/

Nesta atividade serão trabalhados tópicos relacionados ao conteúdo de funções, aliados ao tema criptografia RSA. Inicialmente, o professor deve explicar o processo da criptografia e fornecer uma mensagem codificada, solicitando aos alunos que tentem decifrá-la. Depois, dividindo a classe em grupos, cada grupo deve criar sua própria mensagem criptografada e trocá-la com os demais. O desafio é tentar decifrar o que o outro grupo quis dizer, conhecendo a função chave que foi utilizada.

3.2 Desenvolvimento da Aula

Atividade 1- mensagem do professor

Objetivo: Familiarizar os alunos com a ideia de codificação e decodificação.

Usando a associação das letras do nosso alfabeto aos números, conforme a Tabela 1, e a partir da mensagem codificada 35 7 23 29 33 7 -3 1 27 -1 35 -3 -1 3 27 7 35, o aluno deverá empregar a função $f(x) = 2x - 3$ para decodificar o que está criptografado.

Tabela 2 - Associação de letras aos números

.	**,**	**?**	**espaço**	**A**	**B**	**C**	**D**	**E**	**F**
-3	-2	-1	0	1	2	3	4	5	6
G	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
7	8	9	10	11	12	13	14	15	16
Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
17	18	19	20	21	22	23	24	25	26

Fonte: O autor

Resposta esperada:

Primeiramente é esperado que o aluno determine a função inversa de $f(x) = 2x - 3$:

$$y = 2x - 3$$

$$x = 2y - 3$$

$$x + 3 = 2y$$

$$\frac{x + 3}{2} = y$$

$$y = \frac{x + 3}{2}$$

Ou seja,

$$f^{-1}(x) = \frac{x+3}{2}$$

Então, o aluno deve substituir cada valor dado na mensagem codificada na função inversa. Ele deverá proceder os cálculos da seguinte maneira:

Para $x = 35$

$$f^{-1}(35) = \frac{35+3}{2}$$

$$f^{-1}(35) = \frac{38}{2}$$

$$f^{-1}(35) = 19$$

Analisando a tabela 1, é possível verificar que a letra S equivale ao número 19. Logo, 35 corresponde a letra S.

Determinando os valores numéricos da função inversa $f^{-1}(x) = \frac{x+3}{2}$ para os valores que constam na mensagem codificada, conforme realizado para $x = 35$ e verificando a associação na tabela 1, obtém-se a decodificação apresentada na tabela 2.

Tabela 3 - Decodificação da mensagem

x	$f^{-1}(x)$	Letra associada
35	19	S
7	5	E
23	13	M
29	16	P
33	18	R
7	5	E
-3	0	ESPAÇO
1	2	B
27	15	O
-1	1	A
35	19	S
-3	0	ESPAÇO
-1	1	A
3	3	C
27	15	O
7	5	E
35	19	S

Fonte: O autor

Logo, após o aluno ter concluído os cálculos ele encontrará a mensagem secreta que é: SEMPRE BOAS AÇÕES.

Atividade2 – Troca de mensagens

Objetivo: Explorar a participação e interação dos alunos.

Nessa atividade é esperado que cada grupo crie uma mensagem pequena e utilizem uma função para codificar a mensagem criada e fazer a troca de mensagens com outro grupo. Ao utilizarem uma função que não seja necessariamente a função da etapa anterior, eles devem perceber que essa função precisará ser uma função invertível.

4 O PLANO DE AULA: ANÁLISE A POSTERIORI

A implementação do planejamento ocorreu em um encontro de duas horas/aulas e se deu em uma turma de 1º ano do Ensino Médio em uma escola Estadual do município de Santa Maria. Antes da aplicação do planejamento houve uma conversa com a professora titular da turma, a qual informou que estava trabalhando o conteúdo de funções, porém não havia trabalhado o conteúdo de função inversa e o mesmo não seria trabalhado com a turma. Mesmo de posse dessas informações, a aplicação do planejamento foi realizada na turma.

4.1. Principais momentos

No primeiro momento, ao entrarmos na sala de aula a professora apresentou a pesquisadora para a turma, explicou o motivo de estar presente no momento e solicitou a colaboração de todos. A turma foi bastante receptiva e houve a participação de todos os alunos durante a aplicação do planejamento.

Ao iniciar a aula foi entregue a todos os alunos uma folha (Apêndice A) que continha todo o desenvolvimento da atividade. Também foi questionado aos alunos se sabiam o que era criptografia. Alguns alunos responderam que sim, então foi explicado um pouco do assunto e logo em seguida foi solicitado a um aluno para fazer a leitura do material dirigido aos alunos.

Na Atividade 1 denominada Mensagem do professor, são apresentadas uma mensagem codificada e uma função, denominada chave pública. A atividade solicita que os alunos decifrem a mensagem secreta. Porém, antes que os alunos realizassem a atividade, foi explicado por meio da palavra LUA, como era feita a codificação de uma mensagem.

Para isso, primeiramente verifica se na Tabela 1 o número que corresponde cada letra da palavra e depois substitui o número na função $f(x) = 2x - 3$. Conforme a Tabela 1 pode se observar que a letra L corresponde ao número 12, substituindo na função, temos:

$$f(12) = 2 \cdot 12 - 3$$
$$f(12) = 24 - 3$$
$$f(12) = 21$$

Logo, a letra L equivale ao número 21. Procedendo dessa maneira para as demais letras da palavra LUA é possível constatar que as letras U e A equivalem aos números 39 e -1, respectivamente, ou seja, utilizando esse processo para codificar a palavra LUA teremos a mensagem codificada 21 39 -1.

Após os alunos entenderem o processo para codificar uma mensagem, foi explicado, então, o processo inverso, ou seja, a decodificação da mensagem 21 39 -1. Para decodificar a mensagem, considerando que os alunos não haviam aprendido o conteúdo de função inversa, foi solicitado que igualassem a função à cada número dado da mensagem codificada, encontrando o valor de x, da seguinte forma:

Para o número 21, temos:

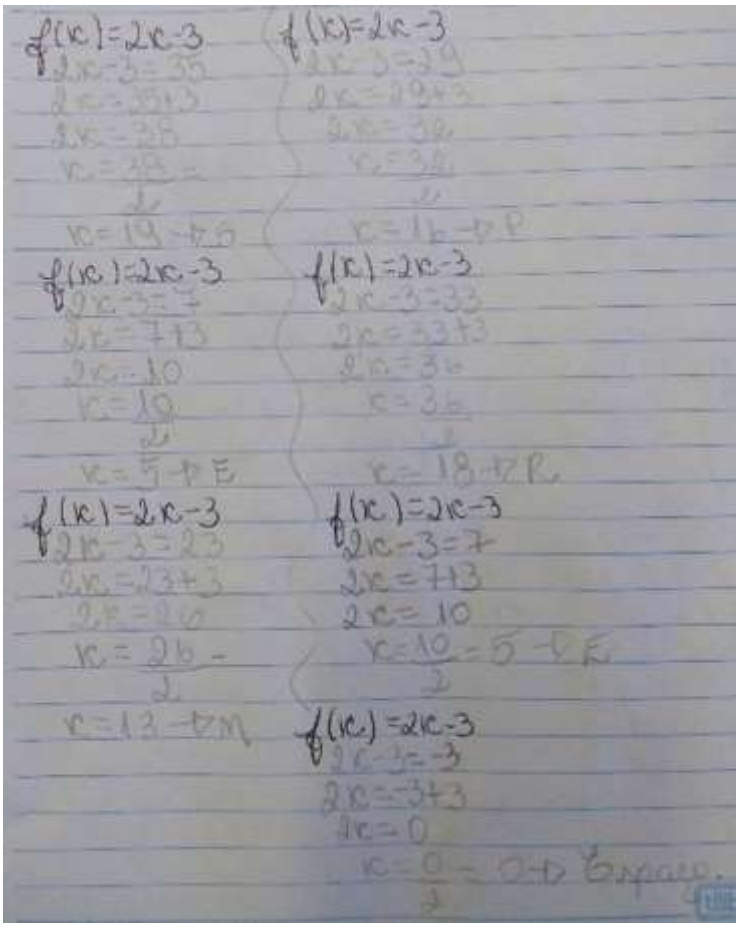
$$2x - 3 = 21$$
$$2x = 21 + 3$$
$$2x = 24$$
$$x = \frac{24}{2}$$
$$x = 12$$

Logo, ao encontrar o número 12 como resposta e verificando na Tabela 1 é possível constatar que o número 12 equivale à letra L, aplicando esse processo para os números 39 e -1 iremos encontrar como resposta as letras U e A, respectivamente.

Na Atividade 1 é dada a mensagem codificada 35 7 23 29 33 7 -3 1 27 -1 35 -3 -1 3 27 7 35, para encontrar a mensagem é preciso aplicar o processo para decodifica-la. A figura 1 apresenta parte da resolução da Atividade 1, de uma aluna que elaborou a atividade com facilidade, mostrando clareza no desenvolvimento dos cálculos.

No primeiro calculo a aluna igualou a função ao número 35 e encontrou o número 19 como resposta e depois ela verificou na Tabela 1, que o número 19 equivale à letra S. Na figura é apresentado os cálculos para os números 35, 7, 23, 29, 33, 7, e -3.

Figura 4 - Resolução da atividade 1

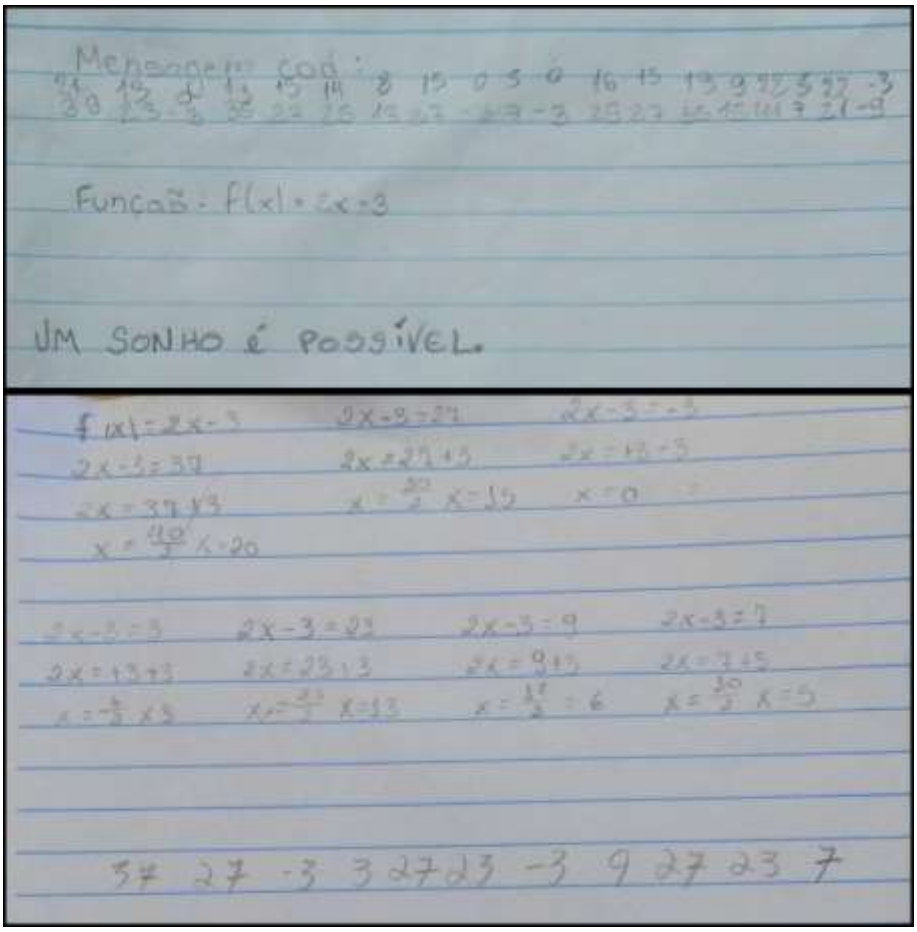


Fonte: Dados da pesquisa

Antes de iniciar a Atividade 2 denominada Troca de mensagens foi solicitado aos alunos que formassem quatro grupos. E eles se organizaram e formaram dois grupos com quatro integrantes e dois grupos com cinco integrantes. Na sequência escolheram o grupo para qual queriam mandar a mensagem secreta. Foi sugerido aos alunos a utilização de outra função, no entanto dois grupos optaram pela mesma, assim como ilustra a figura 2.

O Grupo 1 apresentou a seguinte mensagem: Um sonho é possível, eles utilizaram a função $f(x) = 2x - 3$ para codificar e obtiveram a mensagem 39 23 -3 35 27 -3 7 -3 29 27 35 15 41 7 21 -9. O Grupo 2 apresentou apenas os cálculos da mensagem codificada e a mensagem 37 27 -3 3 27 23 -3 9 27 23 7.

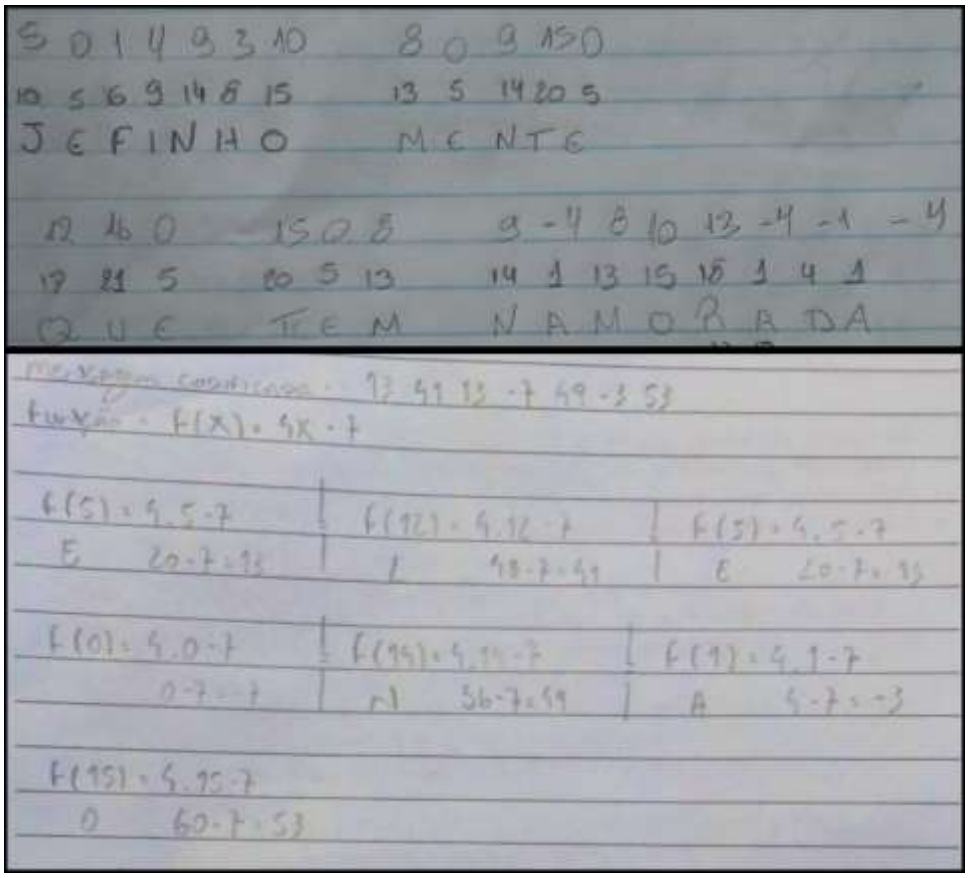
Figura 5 - Resolução da atividade 2 (Grupo 1 e Grupo 2)



Fonte: Dados da pesquisa

A figura 3 ilustra a resolução dos outros dois grupos que escolheram outras funções. O Grupo 3 não apresentou a função utilizada para codificar a mensagem, porém apresentou a mensagem: Jefinho mente que tem namorada e a mensagem codificada 10 5 6 9 14 8 15 13 5 14 20 5 17 21 5 20 5 13 14 1 13 15 18 1 4 1. O Grupo 4 apresentou a mensagem codificada: 13 41 13 -7 49 -1 53 e a função $f(x) = 4x - 7$ utilizada para codificar a mensagem.

Figura 6 - Resolução da atividade 2 (Grupo 3 e Grupo 4)



Fonte: Dados da pesquisa

Os alunos acharam interessante o tema e a atividade proposta, não encontraram maiores dificuldades, foram bastante participativos e interativos, resultando na construção e apreensão dos conhecimentos numa perspectiva contextualizada.

CONSIDERAÇÕES FINAIS

Sabe-se que a aprendizagem é um processo de construção de conhecimento e que o professor assume um papel de mediador, elaborando estratégias de ensino, de maneira que o aluno possa desenvolver suas percepções e convicções a partir da articulação entre os conhecimentos prévios dos alunos e o conteúdo da disciplina. Nesse sentido, buscou-se realizar um planejamento contextualizado organizando atividades com temas atuais, de forma a construir o conhecimento diante das situações reais da vida.

Segundo Dante (1994, p. 13 – 14):

> Uma aula de matemática onde os alunos, incentivados e orientados pelo professor, trabalhem de modo ativo – individualmente ou em pequenos grupos – na aventura de buscar a solução de um problema que os desafia é mais dinâmica e motivadora do que a que segue o clássico esquema de explicar e repetir. [...].

Além disso, sabe-se que a criptografia é um tema abrangente e atual e a matemática está diretamente associada a esse tema, logo estas características serviram de motivação para realização de um planejamento atrativo e dinâmico.

Os resultados obtidos na implementação do planejamento na turma revelam que a contextualização do tema criptografia RSA contribuiu no processo de ensino e aprendizagem dos alunos, com o conteúdo de função, despertando motivação e interesse pela atividade. Sendo assim, o planejamento se mostrou um material que desperta no aluno o desejo de aprender, podendo então usar o conhecimento de criptografia com as aplicações da matemática em sala de aula.

Durante o desenvolvimento e a aplicação desse planejamento, pode-se perceber que ser professor e educador vai muito além da sala de aula, que ensinar exige dedicação, preparação, embasamentos teóricos e muito mais. Diariamente há a aplicação da matemática em diversos ramos, basta analisar e se envolver para que possa obter um planejamento bastante significativo para a aprendizagem dos alunos.

REFERÊNCIAS

CHEVALLARD, Yves; BOSCH, Marianna; GASCÓN, Josep. **Estudar as matemáticas:** o elo perdido entre o ensino e a aprendizagem. Porto Alegre: Artmed, 2001.

COUTINHO, S. C. **Criptografia.** Rio de Janeiro: IMPA, 2008. v.7. (Programa de Iniciação Cientifica – OBMEP, v.7).

DANTE, Luiz Roberto. **Didática da resolução de problemas de matemática:** 1ª a 5ª séries, para estudantes do curso de magistério e professores do 1º grau. 4. ed. São Paulo: Ática, 1994.

FILHO, Daniel Cordeiro de Morais; MALAGUTTI, Pedro Luiz Aparecido. **Matemática discreta:** módulo II. Cuiabá, MT: Central de Texto, 2013. – (Matem@tica na pr@tica. Curso de especialização em ensino de matemática para o ensino médio).

MALAGUTTI, Pedro. **Atividades de Contagem a partir da Criptografia.** Rio de Janerio, IMPA, 2015.

MORETTO, Vasco Pedro. **Prova:** um momento privilegiado de estudo – não um acerto de contas. 3. ed. Petrópolis, RJ: Vozes, 2002.

PAIS, Luiz Carlos. **Didática da Matemática:** uma análise da influência francesa. Belo Horizonte: Autêntica, 2002.

SINGH, Simon. **O livro dos códigos.** Rio de Janeiro: Record, 2005.

ANEXOS

ANEXO B - Relação de frequência das aulas realizadas

ESCOLA ESTADUAL DE ENSINO MÉDIO CILON ROSA

Rua Appel, 805 – Centro - 97015-130

(55)3222 – 4311 – Santa Maria –RS

Relação de horários das aulas voluntárias da Profª Lidiane Dias

Data	Horário
07/06/2018	13:55 – 15:25

Giovanna Stefaniello
VICE-DIRETORA
ID: 3758664

E. E. DE ENSINO MED.
CILON ROSA
SANTA MARIA - RS
Dec. Reconh. N.º 2[illegible]
D.O. 25/08/[illegible]
Port. Desig. N.º 8[illegible]
D.O. 28/06/[illegible]

APÊNDICES

APÊNDICE B – Material dirigido aos alunos

EXPERIMENTO:

Mensagens secretas com funções

Introdução:

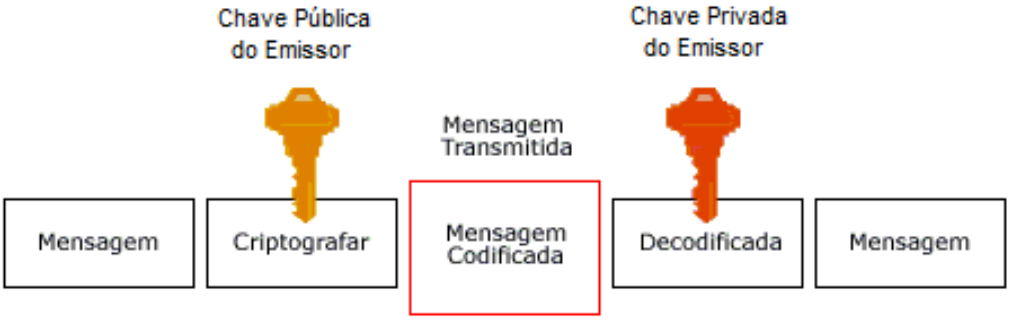
Nesse experimento, aprenderemos uma das diversas maneiras de criptografar mensagens. A criptografia tem sua participação no curso da história da humanidade e hoje está presente no nosso cotidiano, são senhas, compras pela internet, cartões, caixas eletrônicos, e tudo isso precisa ser mantido em segredo, e nós nem sabemos como isso acontece, simplesmente acreditamos que é confiável.

A criptografia é o estudo que desenvolve métodos para ocultar o conteúdo de uma mensagem. Sua evolução caminhou em paralelo com as descobertas dos meios de comunicação e as necessidades das pessoas manterem em segredo suas conversas e dados, cada vez mais suscetíveis em cair em mãos erradas.

Utilizaremos o método RSA (Rivest-Shamir-Adleman) que é um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para transmissão segura de dados. Neste sistema de criptografia, a chave de codificação é pública e é diferente da chave de decodificação que é secreta.

Como funciona esse método? A ideia é transformar as letras da mensagem em números. Para enviar a mensagem secreta, usaremos uma função, chave pública, que codifica os números associados à mensagem secreta, transformando-a na mensagem codificada.

Quando a outra pessoa recebe a mensagem codificada, é necessário que ela conheça a outra chave, que é a chave secreta, que nada mais é do que a função inversa da primeira função para decodificar a mensagem.



PROCEDIMENTO:

Tabela 1 – Associação das letras aos números

.	,	?	espaço	A	B	C	D	E	F
-3	-2	-1	0	1	2	3	4	5	6
G	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
7	8	9	10	11	12	13	14	15	16
Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
17	18	19	20	21	22	23	24	25	26

Etapa 1 - Mensagem do professor

Usando a associação das letras do nosso alfabeto aos números, conforme a Tabela 1, seu professor apresentará uma mensagem criptografada e explicará como a construiu. O desafio é conseguir decifrar o que está criptografado.

Chave pública: $f(x) = 2x - 3$
Mensagem codificada: 35 7 23 29 33 7 -3 1 27 -1 35 -3 -1 3 27 7 35

Etapa 2 - Troca de mensagens

1. Agora que vocês já sabem como criptografar uma mensagem, invente e criptografe uma com no máximo 20 caracteres.
2. Troque a sua mensagem com a de outro grupo, fornecendo a mensagem criptografada e a função chave que usou na multiplicação.
3. Tente decifrar a mensagem do outro grupo – e não fiquem bravos se ele estiver caçoando de vocês!

Observação: Se a função escolhida não admitir a função inversa, pode ocorrer de a mensagem não ser decifrável, pois sem a condição da função ser invertível não podemos garantir que pontos que representam letras distintas possam ser levados a letras distintas. Para que uma função f admita a inversa f^{-1} é necessário que ela seja bijetora. Se f não for bijetora, ela não possuirá inversa.

REFERENCIA:
https://m3.ime.unicamp.br/recursos/1020