UNIVERSIDADE FEDERAL DE SÃO CARLOS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

JAQUELINE DE MORAES RODRIGUES

CRIPTOGRAFIA E CONTEÚDOS DE MATEMÁTICA NO ENSINO FUNDAMENTAL

SÃO CARLOS
2013

UNIVERSIDADE FEDERAL DE SÃO CARLOS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

JAQUELINE DE MORAES RODRIGUES

CRIPTOGRAFIA E CONTEÚDOS DE MATEMÁTICA NO ENSINO FUNDAMENTAL

Dissertação de mestrado profissional apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de São Carlos, como parte dos requisitos para obtenção do título de Mestre.

Orientação:
Prof. Dr. Pedro Luiz Aparecido Malagutti

São Carlos
2013

Ficha catalográfica elaborada pelo DePT da

Biblioteca Comunitária da UFSCar

Rodrigues, Jaqueline de Moraes

"Criptografia e Conteúdos de Matemática no Ensino Fundamental" / Jaqueline de Moraes Rodrigues. – São Carlos: UFSCar, 2013.

Páginas: 33

Dissertação de mestrado - Universidade Federal de São Carlos, 2013.

Palavras-chave: Funções, Criptografia, Codificar e Decodificar.

Banca Examinadora

Prof. Dr. Pedro Luiz Aparecido Malagutti
DM - UFSCar

Prof. Dr. Wagner Vieira Leite Nunes
ICMC- USP

Prof. Dr. Paulo Antonio Silvani Caetano
DM - UFSCar

Em especial à minha mãe, a quem devo tudo que sou hoje, a todos os meus amigos e a todos alunos e professores do PROFMAT.

AGRADECIMENTOS

Agradeço em primeiro lugar à Deus, pela vida e por mais essa oportunidade de aprendizado e crescimento que me foi concedida.

Dedico este trabalho à minha mãe, por estar ao meu lado sempre, me incentivando e acreditando em minha capacidade. Agradeço a ela pelos momentos que me motivava a continuar e não desistir, que por tantas vezes teve a sabedoria de me chamar a atenção com seu jeito firme me trazendo de volta a razão para que eu não descuidasse dos meus estudos.

Agradeço às minhas companheiras de jornada na escola João Urias da Silva onde lecionei nesse período, por compreender as ausências na escola e por estarem ao meu lado nos momentos que mais precisei.

Agradeço a todos os alunos da turma por terem contribuído para a conclusão do mesmo.

Agradeço a todos os professores do PROFMAT, pelos ensinamentos que levarei sempre comigo.

RESUMO

O objetivo central dessa dissertação é expor os resultados de uma experiência didática do uso de Criptografia para o estudo de funções nas aulas de Matemática no Ensino Fundamental, cujo resultado foi a verificação de melhoras no entendimento do conceito supracitado. A vivência em sala de aula mostra que os alunos têm grandes dificuldades em trabalhar o conceito de funções. São apresentadas diversas atividades com base na Criptografia para superar as dificuldades mais frequentes que os alunos trazem na aprendizagem de funções e conceitos correlatos.

Palavras–chave: Funções, Criptografia, Codificar e Decodificar.

ASTRACT

The central aim of this dissertation is to present the results of a teaching experience of using encryption for the study of functions in mathematics classes in elementary school, the result was checking improvements in conceptual understanding above. The experience in the classroom shows that students have great difficulty working the concept of functions. Various activities are presented based on cryptography to overcome the difficulties that students frequently bring in learning functions and related concepts.

Keywords: Functions, Cryptography, Coding and Decoding.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Há algum tempo venho observando a dificuldade que os alunos do 9° ano do Ensino Fundamental têm em iniciar o estudo de funções. Muitos ainda confundem função com equação e tentam resolvê-la igualando-a a zero.

Pude perceber que os alunos apresentam uma grande dificuldade em resolver situações em que é usado o conceito dinâmico de função, o qual envolve a descoberta do domínio e a aplicação da função como uma lei para se chegar à imagem.

Outro fato que me chamou a atenção foi que a maior dificuldade dos alunos em um exercício de construção de gráfico está em atribuir valores para x, aplicar a função, e não na construção do gráfico em si, ou seja, a dificuldade está logo no início, na decisão de quem é a variável independente e não nos cálculos, nem na representação geométrica.

Com base em minhas observações, procurei desenvolver atividades que instigassem os alunos e facilitasse esse primeiro contato com as funções.

Pensando nisso, resolvi usar a criptografia com funções, em que o aluno aplicaria funções para codificar mensagens, trabalhando também com funções inversas de forma implícita na decodificação de mensagens, uma vez que esse conceito só será formalizado no Ensino Médio.

Nesta perspectiva, acredito que um trabalho semelhante ao que ora se apresenta pode contribuir significativamente para a melhoria das aulas de matemática e no aprendizado dos alunos.

O objetivo deste trabalho é facilitar o entendimento do aluno sobre a aplicação de funções dado o seu domínio, por meio da codificação e decodificação de mensagens. Isto pode ser realizado de forma divertida, despertando a curiosidade e levando a aluno a investigação da função usada na hora de codificar e decodificar as mensagens. Assim sendo, colocamos a seguinte pergunta investigativa.

A Criptografia pode levar o aluno a atribuir significado ao conceito de função na etapa final do Ensino Fundamental?

Devem-se ressaltar dois pontos importantes:

1) A Criptografia deve ser usada apenas como um auxílio para o entendimento do aluno sobre função e suas aplicações, não devendo ser utilizada para a introdução do referido assunto, uma vez que nesse caso poderia dificultar ao invés de ajudar.

2) Faz-se necessário que os alunos tenham um conhecimento prévio sobre funções, sendo indicado que se façam algumas aulas anteriores à atividade para a formalização do referido conceito para que os alunos tenham uma base teórica.

Este trabalho está organizado da seguinte forma: o Capítulo 1 traz um relato da escola, a comunidade em que está inserida, retrata a realidade dos alunos envolvidos no projeto e uma breve história de minha trajetória profissional e os objetivos que me levaram a escolher o assunto e a forma a ser trabalhada.

No Capítulo 2, será apresentado o referencial teórico em que a pesquisa foi embasada, que foi a Engenharia Didática e também será apresentada uma descrição passo a passo do trabalho realizado.

No Capítulo 3, encontra-se a descrição da aplicação das atividades, o que aconteceu durante sua realização e as dificuldades encontradas pelos alunos junto com os resultados e soluções.

No Capítulo 4 são apresentadas as conclusões gerais, bem como sugestões para projetos futuros que relacionam Criptografia com o estudo de funções.

1. BREVE DESCRIÇÃO DA ESCOLA, DOS ALUNOS E DAS ATIVIDADES.

A escola Estadual Capitão João Urias da Silva está localizada no Bairro São Roque da Fartura, distrito de Águas da Prata, cujo acesso se dá pela estrada que liga Águas da Prata a Poços de Caldas, pouco antes da divisa de São Paulo com Minas, é uma região que ficou próxima de lugares marcados por conflitos entre paulistas e mineiros, em 1932. Situado na Serra da Mantiqueira, o bairro se originou através do desmembramento da Fazenda Sobradinho. Um dos herdeiros desse desmembramento foi o Capitão João Urias da Silva, fundador da escola, que juntamente com Felipe Urtado Serrato doaram pedaços de terra para a construção da igreja e do cruzeiro que marcam o início do povoado e da escola. Por essa razão a escola, fundada em 1°de abril de 1977, recebe o seu nome.

É uma escola pequena que compartilha o prédio com a escola municipal EMEB Felipe Urtado Serrato (1° ao 5° ano). A escola Capitão João Urias da Silva, possui quatro salas de aula que funcionam apenas no período da manhã, com os anos finais do ensino fundamental, sendo uma sala para cada ano, com um total de 110 alunos. Possui ainda, uma sala para secretaria e diretoria juntas e uma biblioteca que fica junto com a sala de informática, instalada no ano de 2012. Não há sala de professores.

A escola conta com 21 funcionários entre professores, cozinheiras, inspetores, etc. Por ser uma escola pequena, não possui coordenadores nem diretor, apenas uma vice – diretora.

Apesar de seu tamanho e de estar localizada em uma região de difícil acesso, as salas são todas equipadas com lousa digital e *data show* desde 2012, o que trouxe um grande benefício para os alunos, pois assim eles têm acesso a internet e programas como Geogebra, Cabri Géomètre, etc. Isso foi uma grande conquista para eles, uma vez que 90% dos nossos alunos provêem da zona rural que circunda o bairro e muitos não tem computador nem internet em casa.

Figura 1. Entrada da Escola Estadual Cap. João Urias da Silva.

Comecei a lecionar nessa escola no ano de 2011 como professora efetiva do Estado de São Paulo, porém já lecionava como professora eventual do estado desde 2006.

Me graduei em Licenciatura Plena em Matemática no ano de 2005, pela Faculdade de Filosofia Ciências e Letras de São José do Rio Pardo, cidade onde nasci e morei até o primeiro semestre de 2007. No segundo semestre de 2007, mudei-me para São João da Boa Vista. Em 2008, para ampliar meus conhecimentos, comecei a fazer Especialização em Matemática na Unicamp, voltada para professores que estão em sala de aula. Em 2010 fui aprovada no concurso do Estado de São Paulo, quando escolhi a escola Capitão João Urias da Silva para começar a lecionar no ano seguinte.

Em fevereiro de 2011, prestei a prova do PROFMAT e fui aprovada.

1.1 Objetivos

Trabalhando resolução de sistemas através de gráficos com os alunos do 8° ano e funções com os alunos do 9° ano, pude perceber que a maior

dificuldade dos alunos não era a construção dos gráficos em si, mas sim em como atribuir valores para x e aplicar a função. Sempre surgiam as mesmas perguntas: “Professora como eu começo?” ou “Como eu escolho?” ou ainda, “Como eu resolvo?”. Na maioria das vezes os alunos ainda trazem a idéia de equação fixa em suas mentes e acabam igualando a função a zero e achando a solução.

Foi no segundo semestre de 2012, durante as aulas de Matemática e Atualidades que escolhi o Criptografia para fazer minhas apresentações. Durante minhas pesquisas achei vários trabalhos que utilizavam a Criptografia com funções, voltados para o Ensino Médio, foi então que percebi que seria viável usar o assunto com os meus alunos do Ensino Fundamental para introduzir o assunto de funções e suas aplicações.

Assim o objetivo geral foi investigar o tema Criptografia e suas aplicações para o desenvolvimento de atividades didáticas aplicáveis no currículo de Matemática do Ensino Fundamental. Esse objetivo geral levou aos seguintes objetivos específicos: pesquisar e desenvolver atividades didáticas com o tema Criptografia que permitam ao aluno, do Ensino Fundamental, aplicar os conteúdos e estabelecer estratégias mentais na resolução de situações problemas e implementar um experimento com alunos do 9º ano do Ensino Fundamental com atividades que relacionam o tema de Criptografia e os conteúdos de Matemática deste ano.

2. METODOLOGIA DE PESQUISA: ENGENHARIA DIDÁTICA

O presente trabalho tem como referencial a Engenharia Didática que é uma metodologia de pesquisa para educadores e profissionais do ensino, inspirada na atividade do engenheiro e fundamentada em experiências em sala de aula.

> Engenharia Didática é um termo que foi criado na França (década de 80) e que é inspirado na atividade do engenheiro. Segundo Michèle Artigue, uma pesquisadora francesa estudiosa do tema, a relação entre as atividades de um educador e um engenheiro é estabelecida quando:
>
> I) o sólido conhecimento que é exigido nas produções do engenheiro e que também se faz necessário para o pesquisador;
>
> II) os problemas de caráter prático a serem enfrentados e que não são facilmente resolvidos com teoria prévia. Não havendo uma teoria na qual buscar solução, é necessário criar uma nova teoria, reinventar ou ampliar alguma já existente. O mesmo acontece no trabalho do pesquisador, que busca soluções e/ou aprimoramentos para dificuldades que percebe em seu trabalho, por exemplo, como professor, que procura meios que possibilitem ajudar o aluno a superar suas dificuldades na construção do conhecimento.
>
> O termo tem dois sentidos: é uma metodologia de pesquisa fundamentada em experiências de sala de aula e também pode ser entendido como a proposta de ensino que é desenvolvida a partir dos resultados da pesquisa realizada. Na junção do conhecimento teórico com o prático, constroem-se novos produtos didáticos. Este é o referencial da Engenharia Didática. A valorização da prática do professor aparece como conscientização que teorias que não são desenvolvidas em sala de aula são insuficientes para as transformações buscadas nos sistemas de ensino mais tradicionais.
>
> Segundo Artigue (1996), uma Engenharia Didática compreende as fases:
>
> 1) análises prévias;
>
> 2) concepção e análise a priori de experiências didático-pedagógicas a serem desenvolvidas na sala de aula de Matemática;
>
> 3) implementação da experiência;

4) análise a posteriori e validação da experiência. (CEMIN, 2008, p. 14 – 15)

Esse trabalho foi desenvolvido em duas etapas. A primeira desenvolvida através de um estudo exploratório em torno dos conceitos de Criptografia e do desenvolvimento de atividades didáticas para o Currículo de Matemática do Ensino Fundamental. O estudo exploratório, segundo Trivinos (1987), permite aos investigadores envolvidos aumentar sua experiência em torno do problema, aprofundando seus estudos nos limites de uma realidade específica, buscando antecedentes e maiores conhecimentos para, em seguida, planejar uma pesquisa de tipo experimental.

Nessa primeira etapa foram feitas análises prévias das principais dificuldades dos alunos no assunto escolhido, no caso, Funções, e do nível de conhecimento que eles possuíam sobre o mesmo. Com base nas análises foram desenvolvidas atividades a serem aplicadas em sala de aula, bem como uma prévia sobre as possíveis soluções e dificuldades que seriam apresentadas pelos alunos durante o experimento.

A segunda etapa foi o desenvolvimento do experimento com 12 alunos do 9º ano, do Ensino Fundamental, da escola estadual Capitão João Urias da Silva, do município de Águas da Prata, estado de São Paulo. As atividades foram desenvolvidas em 4 aulas, distribuídas em dois dias letivos. Os conteúdos das atividades didáticas aplicadas, desenvolvidas no experimento, foram: criptografia, função do primeiro grau e suas aplicações.

Os dados foram coletados através da observação e da análise dos registros dos alunos investigados. Para a realização das atividades propostas os alunos reuniram-se em seis duplas, denominadas duplas: A, B, C, D, E e F.

3. APLICAÇÃO, RESULTADOS E DISCUSSÕES

3.1 Atividades Didáticas com o tema Criptografia

A ideia de aplicação consiste em: pegar uma informação (mensagem) convertê-la em números (codificar) através de uma função bijetora e, pela aplicação de sua inversa, transformar (decodificar) esses números novamente na informação original. Veja o esquema abaixo:

$$\langle mensagem\ original \rangle \xrightarrow{f} \langle mensagem\ codificada \rangle \xrightarrow{f^{-1}} \langle mensagem\ original \rangle$$

O primeiro passo é associar cada letra do alfabeto a um número como, por exemplo, os da tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	X	Z
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

O número 99 representa o espaço em branco entre duas palavras. Assim a palavra PROFMAT pode ser codificada como 26282516231130.

Deve-se ressaltar que há várias possibilidades para se formar a relação entre letras e números, porém o mais indicado é que todas as letras sejam representadas por dois dígitos para se evitar duplo sentido, pois se começássemos essa relação a partir do número 1, com A = 1, B = 2, e assim por diante, o número 11 poderia significar AA ou ainda K que é a 11ª letra do alfabeto.

Nessa atividade usaremos a função afim $f(x) = ax + b$, ou seja, $f : \{11,12,13,...,35,36\} \to \mathbb{R}$, definida por $f(x) = ax + b$ com $a, b \in \mathbb{R}$ e $a \neq 0$. Esta função é sempre bijetora sobre sua imagem e por isso admite inversa sobre sua imagem.

Vejamos o seguinte exemplo:

Imagine que dois alunos, digamos João e Pedro troquem mensagens por meio de códigos, em que João detém a posse da função f que codifica a mensagem e Pedro detém a posse da função inversa f^{-1} que decodifica os códigos recebidos.

Suponhamos que João queira enviar a mensagem: “amanhã tem prova” a Pedro. De posse de $f(x)=3x+2$, João irá codificar a mensagem da seguinte maneira:

De acordo com a tabela construída, João irá fazer uma pré-codificação da mensagem obtendo a seguinte sequência:

11 23 11 24 18 11 99 30 15 23 99 26 28 25 32 11

Para diminuir a quantidade de cálculos João resolveu separar a sequência em blocos de três ou quatro dígitos obtendo:

1123-1124-181-199-301-523-992-628-253-211

O tamanho dos blocos não influencia na codificação nem na decodificação da mensagem, os blocos podem ser grandes ou pequenos e não precisão ser todos do mesmo tamanho, isso ajuda a evitar a análise de frequência das letras, portanto dificulta a criptoanálise. Porém, os blocos não devem começar com o digito zero, para que na hora da decodificação não ocorram erros ao juntar os blocos novamente, por exemplo, imagine um bloco 025 que após codificado vire 312, quando a outra pessoa que receber a mensagem codificada, for decodificá-la, esse mesmo bloco 312 se tornará o bloco 25 o que juntamente com os outros blocos não formaria a mesma mensagem pois estaria faltando o digito 0. Portanto, os blocos podem ser de qualquer tamanho, mas não devem começar com o dígito zero.

Em seguida João aplicou a função em cada um dos blocos:

$$f(1123) = 3 \cdot 1123 + 2 = 3371$$
$$f(1124) = 3 \cdot 1124 + 2 = 3374$$
$$f(181) = 3 \cdot 181 + 2 = 545$$
$$f(199) = 3 \cdot 199 + 2 = 599$$
$$f(301) = 3 \cdot 301 + 2 = 905$$
$$f(523) = 3 \cdot 523 + 2 = 1571$$
$$f(992) = 3 \cdot 992 + 2 = 2978$$
$$f(628) = 3 \cdot 628 + 2 = 1886$$
$$f(253) = 3 \cdot 253 + 2 = 761$$
$$f(211) = 3 \cdot 211 + 2 = 635$$

Assim a mensagem codificada será:

3371 – 3374 – 545 – 599 – 905 – 1571 – 2978 – 1886 – 761 – 635

Ao receber o código, Pedro, de posse de $f^{-1}(x) = \frac{x-2}{3}$ decodificará da seguinte maneira:

$$f^{-1}(3371) = \frac{3371-2}{3} = \frac{3369}{3} = 1123$$
$$f^{-1}(3374) = \frac{3374-2}{3} = \frac{3372}{3} = 1124$$
$$f^{-1}(545) = \frac{545-2}{3} = \frac{543}{3} = 181$$
$$f^{-1}(599) = \frac{599-2}{3} = \frac{597}{3} = 199$$
$$f^{-1}(905) = \frac{905-2}{3} = \frac{903}{3} = 301$$
$$f^{-1}(1571) = \frac{1571-2}{3} = \frac{1569}{3} = 523$$
$$f^{-1}(2978) = \frac{2978-2}{3} = \frac{2976}{3} = 992$$
$$f^{-1}(1886) = \frac{1886-2}{3} = \frac{1884}{3} = 628$$
$$f^{-1}(761) = \frac{761-2}{3} = \frac{759}{3} = 253$$
$$f^{-1}(635) = \frac{635-2}{3} = \frac{633}{3} = 211$$

Assim, Pedro obtém a sequência 1123-1124-181-199-301-523-992-628-253-211 que equivale à:

11	***23***	***11***	***24***	***18***	***11***	***99***	***30***	***15***	***23***	***99***	***26***	***28***	***25***	***32***	***11***
A	***M***	***A***	***N***	***H***	***Ã***		***T***	***E***	***M***		***P***	***R***	***O***	***V***	***A***

3.2 Aplicação e Resultados

Primeiramente foi explicado aos alunos que existem dois tipos de criptografia:

- a ***criptografia simétrica*** (ou de ***chave secreta***) em que utilizamos uma mesma chave tanto para cifrar como para decifrar (ou pelo menos a chave de decifração pode ser obtida trivialmente a partir da chave de cifração), ou seja, a mesma chave utilizada para “fechar o cadeado” é utilizada para “abrir o cadeado”.
- a ***criptografia assimétrica*** (ou de ***chave pública***) em que utilizamos chaves distintas, uma para cifrar e outra para decifrar e, além disso, a chave de decifração não pode ser obtida facilmente a partir do conhecimento da chave de cifração apenas. Aqui, uma chave é utilizada para “fechar” e outra chave, diferente, mas relacionada à primeira, tem que ser utilizada para “abrir”. Por isso, nos algoritmos assimétricos, as chaves são sempre geradas aos pares: uma para cifrar e a sua correspondente para decifrar.

Após essa introdução foram apresentadas atividades com o uso de códigos para que o estudante conhecesse os conceitos básicos da Criptografia.

Atividade 1 - Nessa atividade cada dupla deveria escrever uma frase e cifrá-la. Essa frase cifrada seria entregue para outra dupla que deveria decifrá-la. Para tal atividade os alunos deveriam usar o método da Cifra do Chiqueiro.

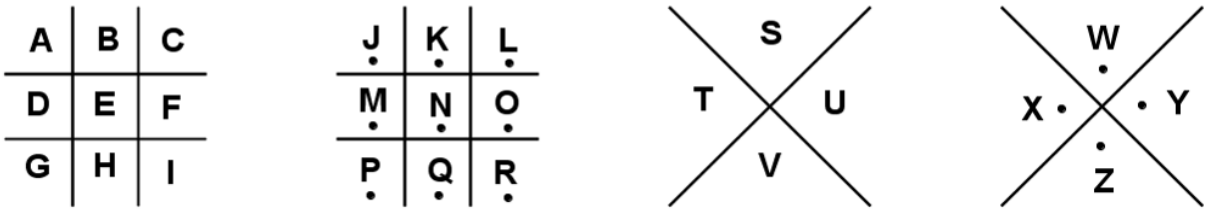

Figura 2. Quadro de método de substituição da Cifra do Chiqueiro.

Análise a priori das possíveis soluções dos alunos

Nessa atividade espera-se que os alunos consigam cifrar a mensagem encontrando o valor de cada letra de acordo com o padrão utilizado pela Cifra do Chiqueiro, em seguida, após a troca de mensagens pelas duplas, espera-se que eles sejam capazes de decifrar uma mensagem desconhecida, recebida de outra dupla, utilizando o processo inverso usado para cifrar a primeira mensagem.

Soluções dos alunos

Os alunos não encontraram dificuldades para realizar a atividade utilizando a Cifra do Chiqueiro. O grupo A usou a tabela e decodificou sua mensagem como mostra a figura a seguir.

Dupla A – mensagem escolhida e cifra.

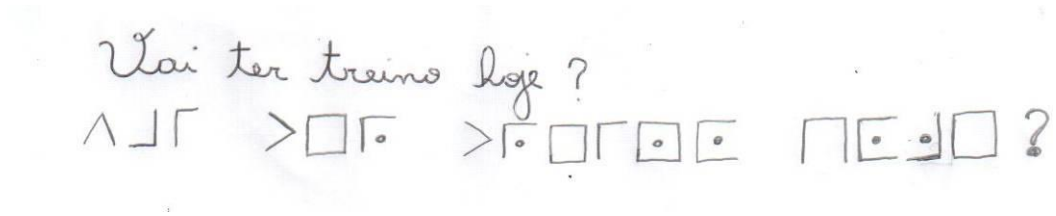

Figura 3.

A mensagem cifrada pela dupla A foi entregue a dupla D, para que estes a decifrassem. A escolha das duplas para a troca de mensagem foi feita de forma aleatória através de sorteio. A dupla D, por sua vez, também não apresentou dificuldades para decifrar a mensagem.

Dupla D – mensagem recebida e decifrada

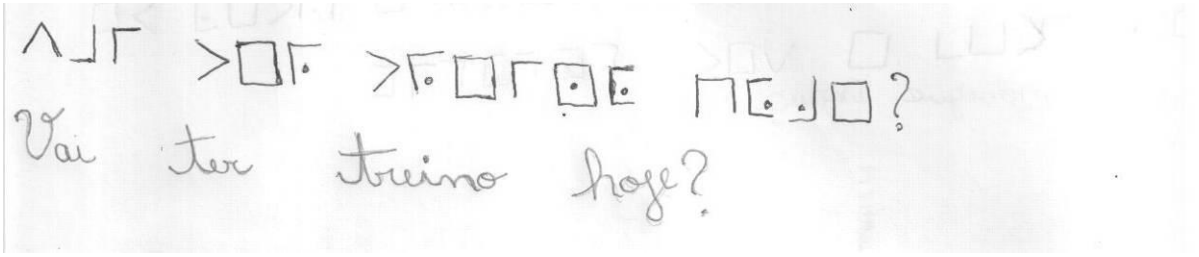

Figura 4.

Em seguida foi desenvolvida uma atividade com criptogramas, na qual o aluno deveria usar estratégias de resoluções de problemas com conceitos de Aritmética, já estudados anteriormente, conforme a atividade seguinte.

Atividade 2 – Criptograma: Qual é o número? Na adição apresentada a seguir, letras iguais representam o mesmo algarismo e letras diferentes representam algarismos diferentes. Encontre o número ABCDE.

$$\begin{array}{r} ABCDE \\ BCDE \\ +\ CDE \\ DE \\ E \\ \hline AAAAA \end{array}$$

Análise a priori das possíveis soluções dos alunos

Nessa atividade esperava-se que o aluno tentasse resolver a atividade por tentativa e erro onde se atribui para cada letra valores aleatórios. Em um

segundo momento, espera-se que o aluno sistematize as informações relevantes, formulando hipóteses e elaborando estratégias para a resolução.

Informação relevante: letras iguais representam algarismos iguais, letras diferentes representam algarismos diferentes.

Solução dos alunos

Nessa atividade os alunos apresentaram certa dificuldade para organizar as informação e começar a resolver o problema. Após a entrega da atividade e leitura da mesma, os alunos procuraram juntos um caminho para a resolução da questão. Depois de alguns minutos, observando a dificuldade dos alunos e encaminhando seus questionamentos – para que eles percebessem pontos relevantes para a resolução do problema - foi necessário o acréscimo de uma primeira informação:

1ª) A vale 5.

Após essa informação, depois de mais um tempo de tentativas, três duplas conseguiram resolver o problema. Foi então, necessário mais uma informação para que os demais alunos conseguissem resolver o problema:

2ª) E é diferente de 1.

Após a segunda informação o restante dos alunos conseguiu resolver a questão.

Dupla B -

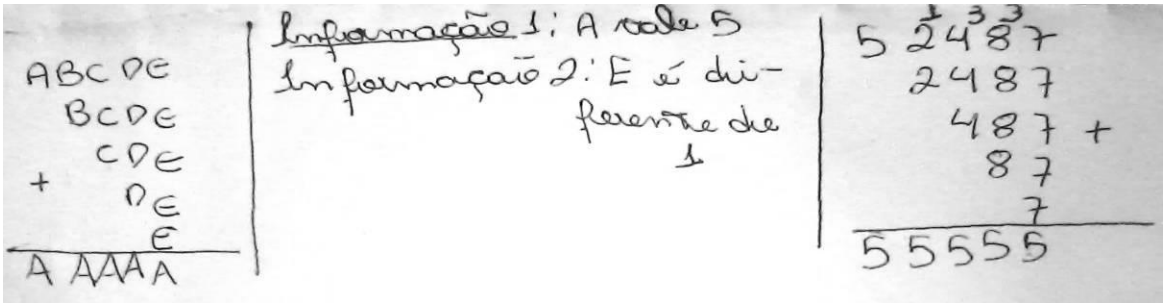

Figura 5.

Depois dessas duas atividades iniciais foram realizadas atividades interligando os conteúdos de Matemática, no nosso caso, funções, com a Criptografia.

Inicialmente foi distribuída para os alunos a tabela já apresentada que relaciona cada letra do alfabeto a um número do intervalo [11;36], foi explicado que era necessário usar esse intervalo para não haver duplicidades, pois, como já foi citado anteriormente, se começássemos a correspondência a partir do 1, teríamos por exemplo o número 11 que poderia ser AA ou K (pois a letra k é a décima primeira letra do alfabeto), a fim de evitar esse tipo de problema escolhemos o intervalo [11;36]. Lembrando que para o espaço entre as palavras adotamos o número 99, e que, na separação, os blocos não podem começar com zero.

Para uma primeira atividade com Funções e Criptografia os alunos escolheram o nome da escola e escolheram também a função que seria usada para criptografar. Após a escolha, em conjunto e inicialmente com a intervenção da professora, começaram a resolver a atividade.

Atividade 3 – Utilize a função $f(x)=2x+5$ para codificar o nome da escola “Capitão João Urias da Silva”.

Análise a priori das possíveis soluções dos alunos

Esperava-se nessa primeira atividade com funções, que os alunos não tivessem dificuldades para aplicar a função na codificação e, ainda, que usando os conceitos de operação inversa já estudada anteriormente, eles conseguissem chegar à função decodificadora da mensagem.

Solução dos alunos

Os alunos não apresentaram dificuldade para realizar a pré-codificação do nome da escola, obtendo a seguinte sequência:

131126193011259920251125993128191129991411992919223211

Depois, a sequência foi separada em dez blocos de cinco dígitos cada e um bloco restante com quatro dígitos, foi ressaltado para alunos que o bloco não poderia começar com o dígito zero, pois isso causaria problemas na hora de decodificar a mensagem.

Após codificar os dois primeiros blocos com a função dada, os alunos conseguiram continuar a codificar o resto da mensagem sem grandes dificuldades.

Dupla C –

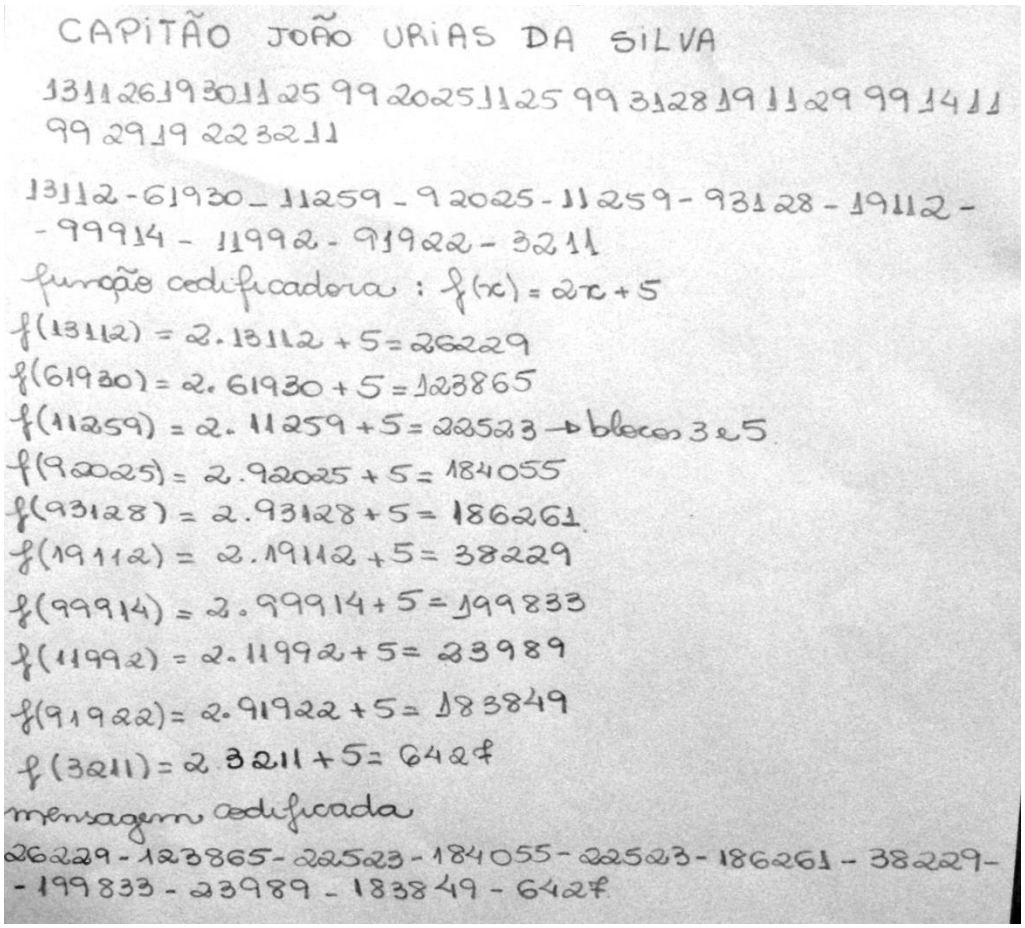

Figura 6.

Após a codificação da mensagem, comecei a instigar os alunos a pensarem em como decodificá-la, surgiram observações do tipo:

- para decodificar deveremos fazer as operações inversas, que no nosso caso, são a subtração e a divisão.

- como a última operação a ser feita foi a adição, então devemos começar pela subtração.

Assim os alunos chegaram à função decodificadora, feito isso, formalizaram suas observações de forma algébrica.

$$y = 2x + 5 \Leftrightarrow y - 5 = 2x + 5 - 5 \Leftrightarrow y - 5 = 2x \Leftrightarrow \frac{y-5}{2} = \frac{2x}{2} \Leftrightarrow \boxed{x = \frac{y-5}{2}}$$

Depois de formalizar a função decodificadora os alunos não tiveram dificuldades para decodificar a mensagem.

Dupla C –

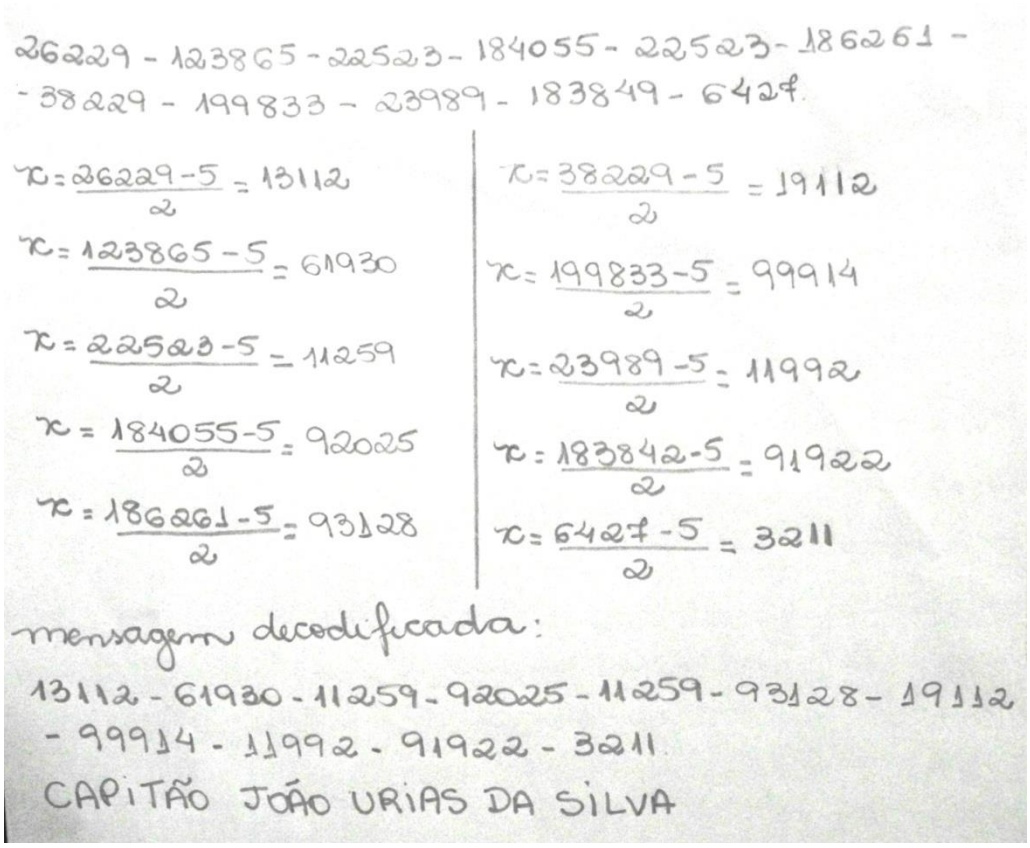

Figura 7.

Foi exposto aos alunos que a função decodificadora era a função inversa da função codificadora e dessa forma introduziu-se intuitivamente o conceito de função inversa, conceito esse, que os alunos construíram de forma investigativa nessa atividade, usando como ferramentas conceitos já estudados anteriormente com operações inversas.

Por ser uma sala do 9º ano do Ensino Fundamental, esse assunto não foi aprofundado, pois os conceitos de função injetora, bijetora e sobrejetora só são formalizados no 1°ano do Ensino Médio.

Atividade 4 – Escreva uma mensagem e uma função codificadora. Codifique a mensagem escolhida e envie para outra dupla decodificá-la.

Análise a priori das possíveis soluções dos alunos

Nessa atividade as duplas trocaram mensagens entre si. Cada dupla deveria elaborar uma mensagem e uma função codificadora, codificar a mensagem e enviá-la para outra dupla juntamente com a função codificadora.

A dupla que recebesse a mensagem deveria achar a função decodificadora através da função recebida junto com a mensagem e decodificá-la.

Solução dos alunos

De um modo geral os alunos não apresentaram dificuldades para desenvolver essa atividade.

Dupla E –

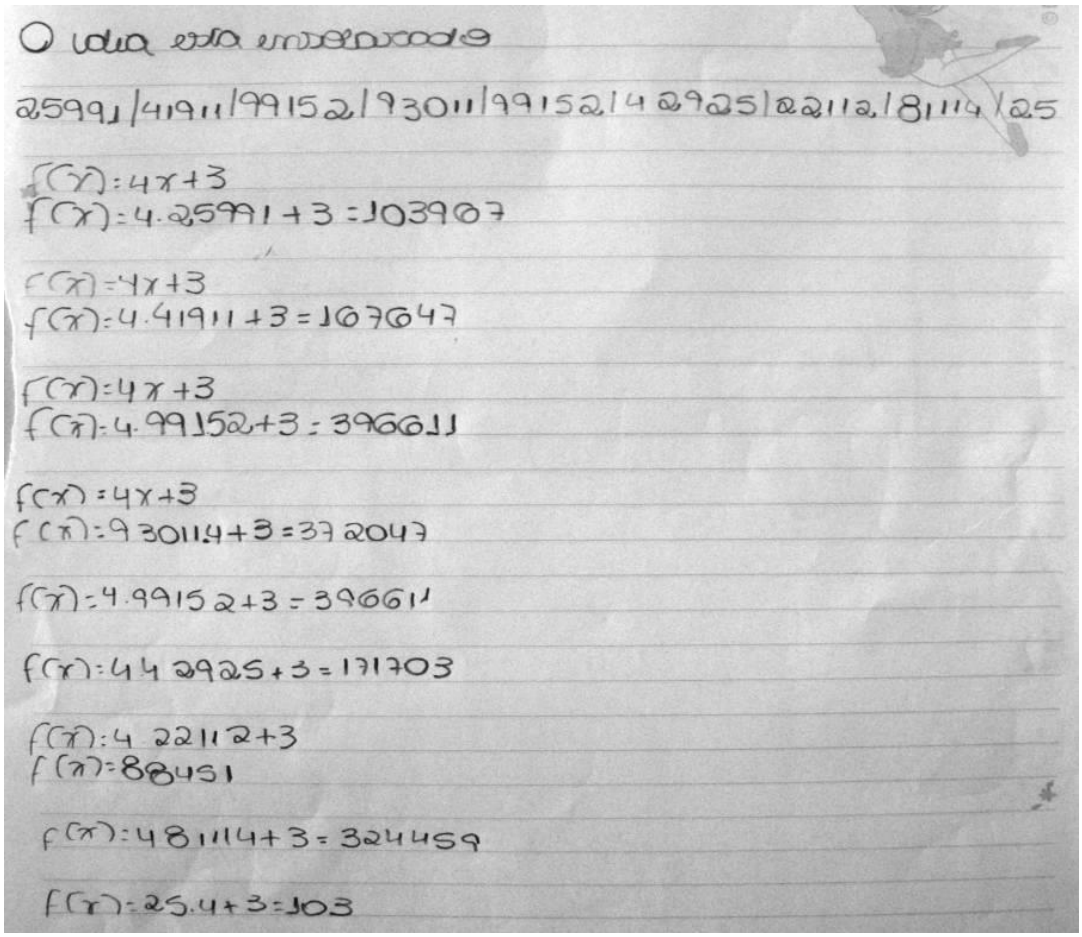

Figura 8.

A dupla E escolheu a mensagem “o dia está ensolarado” e a função codificadora $f(x)=4x+3$, codificou a mensagem e enviou para a dupla F.

A mensagem recebida pela dupla F foi:

103967 – 167647 – 396611 – 372047 – 396611 – 171703 – 88451- 324459 – 103.

Dupla F –

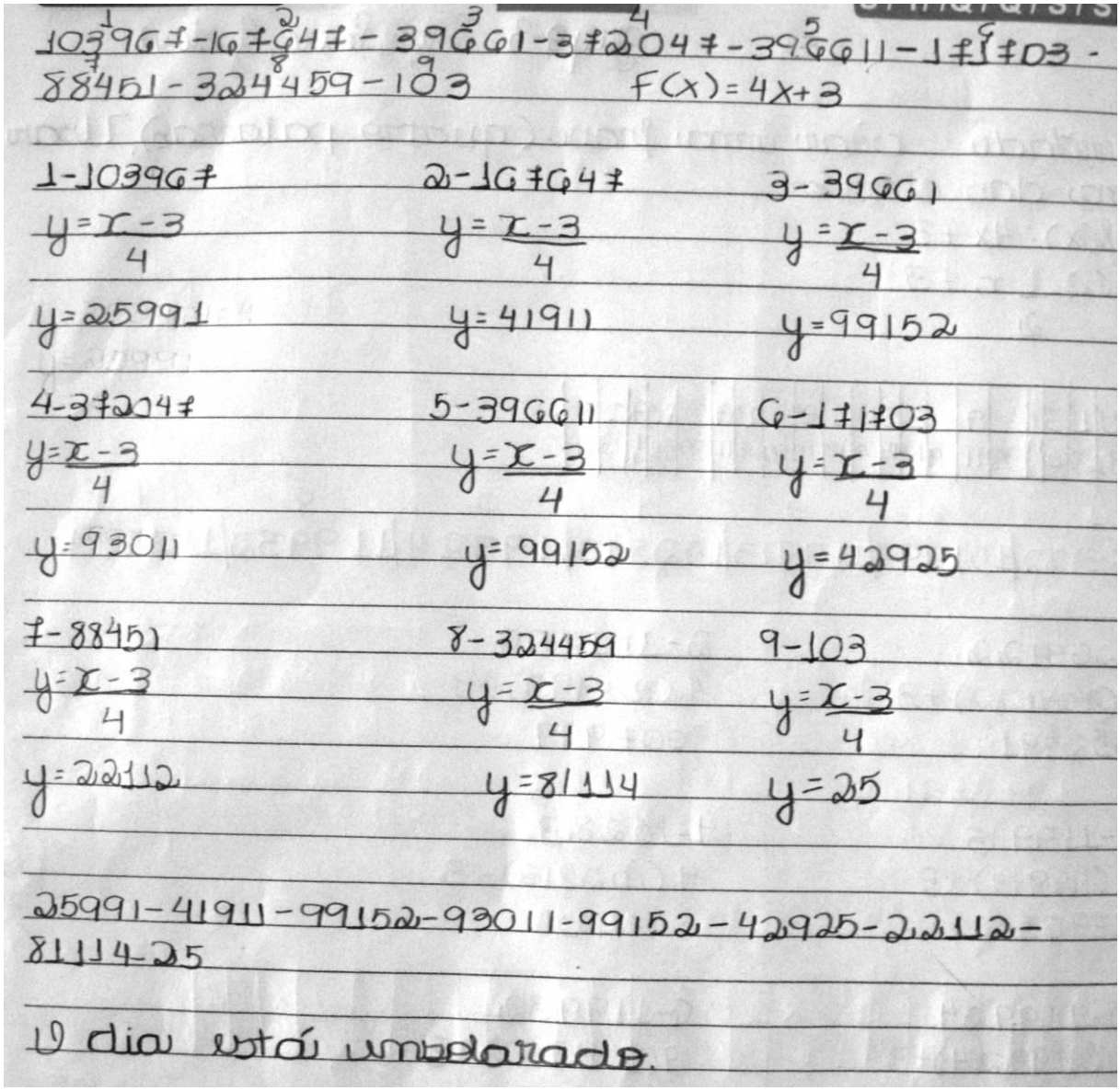

Figura 9.

Para finalizar e descontrair foi sugerida uma última atividade para a classe.

Atividade 5: Decodifique a mensagem a seguir sabendo que a função codificadora usada foi $f(x) = 5x + 3$:

1305643 – 556078 – 1214998 – 1307613 – 599628 – 1509618 – 599558 – 1561058.

Análise a priori das possíveis soluções dos alunos

Espera-se nessa última atividade, que os alunos não apresentem dificuldade para determinar a função decodificadora através da função codificadora dada e que decifrem a mensagem recebida.

Solução dos alunos

Dupla A –

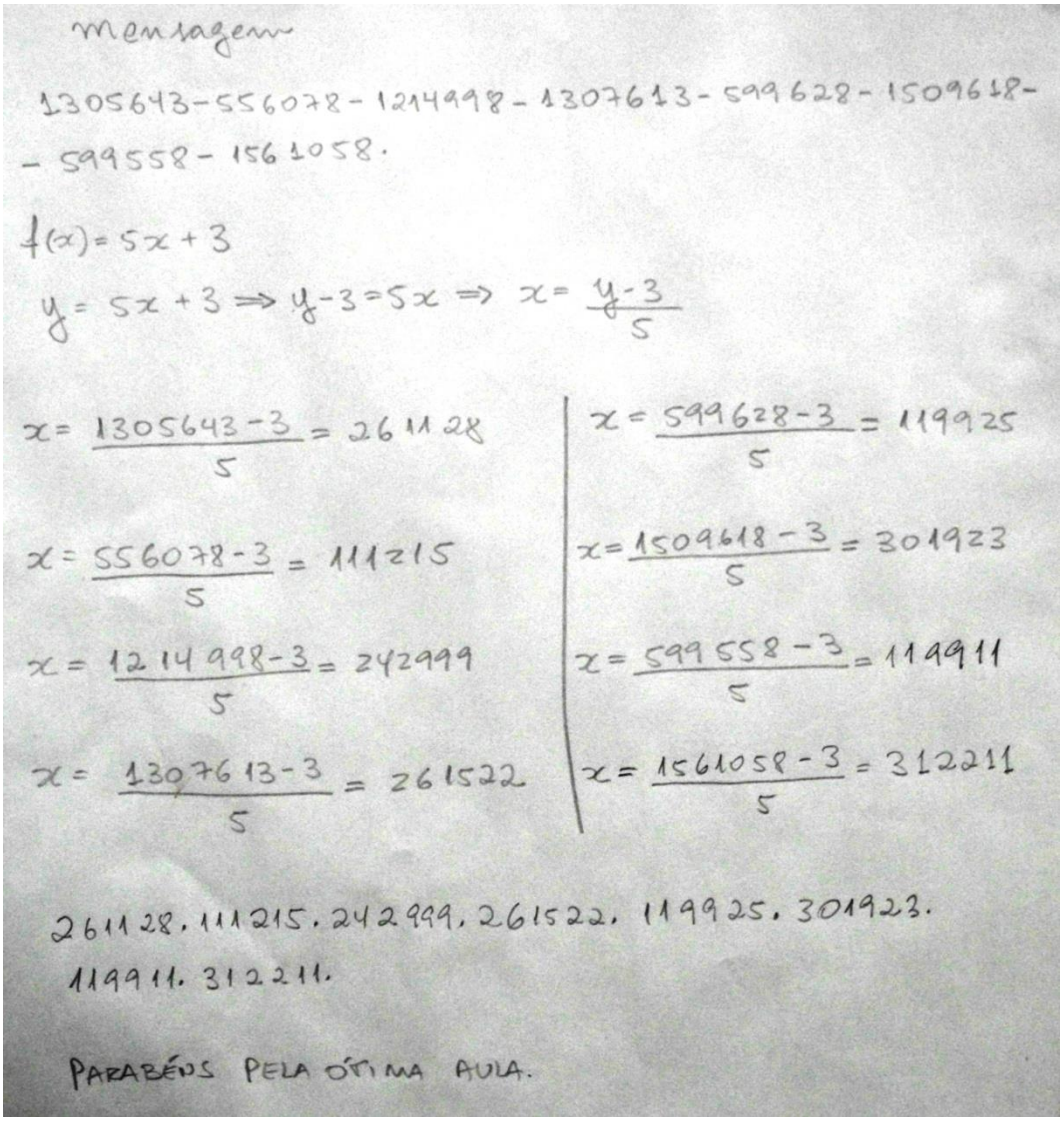

Figura 10.

CONCLUSÕES

Segundo Tamarozzi (2001) o tema Criptografia apresenta material útil para exercícios de fixação de conteúdo, apresentando atividades e jogos de codificação. Nesse trabalho pode-se observar que as atividades com codificação possibilitaram aos alunos trabalhar os conteúdos de Matemática utilizando como ferramenta a Criptografia, que também os ajuda a desenvolver a capacidade de concentração nas atividades, o trabalho em equipe, a capacidade organizar dados e desenvolver estratégias de resolução de problemas.

As atividades com Criptografia tornam a aula mais interessante e dessa forma chama a atenção do aluno instigando-o a investigar, questionar e procurar soluções. Porem deve se levar em conta duas variáveis:

1) Os alunos devem possuir um conhecimento sobre o conteúdo a ser trabalhado por meio da Criptografia.
2) É necessário saber o grau de conhecimento que o aluno traz consigo sobre o assunto trabalhado

É importante estar atento a essas duas variáveis para que as atividades propostas estejam de acordo com os conhecimentos do aluno, podendo auxiliá-lo a melhorar seus conhecimentos.

Deve se ressaltar que a Criptografia é um ótimo tema para desenvolver atividades que auxiliem a entender e trabalhar conteúdos já conhecidos, como uma ajuda para sanar dúvidas e fixar conteúdos, mas não deve ser usada para introduzir e definir um conteúdo novo, pois nesse ponto pode atrapalhar o aprendizado do aluno.

Dessa forma pode-se concluir que a Criptografia é capaz levar o aluno a atribuir significado ao conceito de função na etapa final do Ensino Fundamental. Além de possibilitar ao professor opções para desenvolver atividades diferenciadas e divertidas que auxiliem a fixação, revisão e aprofundamento do conceito de função e relações algébricas, a Criptografia também é uma ótima ferramenta para ajudar os alunos na construção empírica do conhecimento sobre funções inversas.

Referências Bibliográficas

-Cemin, Kelen Luzia. TCC- Ensino de Combinatória: Problemas de Divisão Teoria de Vergnaud e Metodologia da Engenharia Didática. Porto Alegre, 2008. Disponível em: <http://euler.mat.ufrgs.br/~comgradmat/tccs/monos_0802/TCC_Kelen.pdf>, acessado em 04/01/2013.

-Taramozzi, A. C. Codificando e decifrando mensagens. In **Revista do Professor de Matemática** nº 45, p. 41 - 43, Sociedade Brasileira de Matemática, 2001.

-Coutinho, S. Números Inteiros e criptografia RSA. Sociedade Brasileira de Matemática, 2000.

-Terada, R. Criptografia e a importância das suas aplicações. In **Revista do Professor de Matemática** nº 12, Sociedade Brasileira de Matemática, 1988. Disponível em <http://ensino.univates.br/~chaet/Materiais/RPM12_a01.pdf>, acessado pela última vez em 07/07/2013.

- Joel Guilherme. Criptografia, Chaves Públicas e Assinatura Digital para leigos. Disponível em: <http://www.sbis.org.br/**Criptografia**.doc>, acessado pela última vez em 07/07/2013.

-Olgin, Clarisse de A.; Groenwald, Claudia L. O. Criptografia e Conteúdos de Matemática do Ensino Médio. Rio Grande do Sul, 2011. Disponível em <http://www.projetos.unijui.edu.br/matematica/cnem/cnem/principal/cc/PDF/CC9.pdf> , acessado pela última vez em 07/07/2013.

- Olgin, Clarisse de A.; Groenwald, Claudia L. O. Criptografia e Conteúdos de Matemática do Ensino Médio. Recife, 2011. Disponível em <http://www.cimm.ucr.ac.cr/ocs/index.php/xiii_ciaem/xiii_ciaem/paper/viewFile/2092/707>, acessado pela última vez em 07/07/2013.