REVISTA REAMEC
Revista da Rede Amazônica de Educação em Ciências e Matemática

CRIPTOGRAFIA: UMA POSSIBILIDADE PARA O ENSINO DE FUNÇÃO INVERSA

CRYPTOGRAPHY: A POSSIBILITY FOR THE TEACHING OF REVERSE FUNCTION

Idemar Vizolli[1]
Euvaldo de Souza Carvalho[2]
Onésimo Rodrigues Pereira[3]

RESUMO

A Criptografia encontra grande aplicabilidade na proteção de informações sigilosas e pode se constituir como motivadora ao processo de ensino e aprendizagem de conceitos matemáticos. Assim, desafiamo-nos a compreender a estruturação da Criptografia, bem como utilizar a função inversa para codificar e decodificar mensagens. Trata-se de um estudo teórico, a partir da literatura que versa sobre Criptografia e Função Inversa. Para tanto, tratamos da criptografia e sua utilização, sobretudo a partir do advento das tecnologias de comunicação; apresentamos o sistema de criptografia de chave pública – Rivest, Shamir, Adleman (RSA); e o conceito de função inversa. A partir disso, elaboramos uma proposta de atividades didáticas com vistas ao processo de ensino e aprendizagem. Conclui-se que Criptografia se constitui como uma possibilidade metodológica promissora para o desenvolvimento de atividades didáticas, com vistas à compreensão do conceito de função inversa.

Palavras chave: Ensino, Criptografia, Função Inversa, Matemática.

ABSTRACT

Cryptography finds great applicability in the protection of sensitive information and can be a motivator to the teaching and learning process of mathematical concepts. So we challenge ourselves to understand the structure of encryption and use the inverse function to encode and decode messages. It is a theoretical study, from the literature that deals with Cryptography and Reverse Function. For this, we deal with cryptography and its use, especially since the advent of communication technologies; we present the public key cryptography system - Rivest, Shamir, Adleman (RSA); and the concept of inverse function. From this, we elaborate a proposal of didactic activities with a view to the process of teaching and learning. We conclude that Cryptography constitutes a promising methodological possibility for the development of didactic activities, with a view to understanding the concept of inverse function.

Keywords: Teaching, Cryptography, Reverse Function, Mathematics.

[1] Doutor em Educação. Professor na Universidade Federal do Tocantins. idemar@uft.edu.br.
[2] Mestre em Matemática. Professor na Rede Pública de Ensino no Estado do Tocantins. euvaldocarvalho@yahoo.com.br.
[3] Mestre em Matemática. Professor na Rede Pública de Ensino em Palmas, TO. onesimo-rodrigues@bol.com.br.

1 PREÂMBULO

De acordo com os Parâmetros Curriculares Nacionais (PCN), desde a antiguidade a matemática foi considerada uma ciência de difícil compreensão e reservada para poucos, haja vista que seu ensino e sua aprendizagem são cercados de obstáculos.

> O ensino de Matemática costuma provocar duas sensações contraditórias, tanto por parte de quem ensina, como por parte de quem aprende: de um lado, a constatação de que se trata de uma área de conhecimento importante; de outro, a insatisfação diante dos resultados negativos obtidos com muita frequência em relação à sua aprendizagem. (PCN, 1998, p. 15).

Isso denota que é necessário reformular objetivos, rever conteúdos e buscar metodologias para que os conteúdos trabalhados em sala de aula tenham sentido na vida dos estudantes e que, ao mesmo tempo, desperte neles o interesse pela aprendizagem matemática. Convém ressaltar que apresentar o contexto no qual os conceitos foram desenvolvidos, explicar a necessidade do que está sendo ensinado, mostrar aplicações dos conteúdos, não deve ser preocupação estranha aos professores. É notória a necessidade da construção de uma nova consciência em relação ao processo de ensino e aprendizagem de Matemática, especialmente porque o conhecimento não é algo pronto e acabado, pelo contrário, encontra-se em constante processo de construção e desenvolvimento.

A referir-se aos estudos de Freud, Campos (1996) afirma que se alguma atividade não atrai o indivíduo, ou que, ao executá-la, não se sente bem física ou mentalmente, certamente a recusará ou a rejeitará, porque ela não atende aos seus desejos.

Ao frequentar disciplinas no Mestrado Profissional em Matemática (PROFMAT), fomos instigados a desenvolver estudos na perspectiva de superação de problemas em que se insere o processo de ensino e aprendizagem de Matemática, ocasião em que nos deparamos com estudos sobre o sistema de criptografia de chave pública – Rivest, Shamir, Adleman (RSA) e vislumbramos uma possiblidade metodológica para trabalhar conceitos matemáticos em sala de aula.

Uma vez que a Criptografia constitui-se de código secreto e é muito utilizada na proteção de informações sigilosas, acreditamos que é possível utilizá-la como metodologia no processo de ensino e aprendizagem de conceitos matemáticos. Assim, estabelecemos como objetivos, compreender a estruturação da Criptografia e utilizar a função inversa para codificar e decodificar mensagens.

Trata-se de uma pesquisa bibliográfica, a qual, segundo Fonseca (2002), constitui-se a partir de estudos cujas informações foram analisadas e permitem conhecer o que já se produziu sobre o assunto. Ela "explica um problema a partir de referenciais teóricos publicados em documentos" (CERVO; BERVIAN, 1983, p. 55). Esse tipo de pesquisa, normalmente, é feita a partir de análises em fontes secundárias (livros, periódicos, teses, dissertações, dentre outras). Estruturamos este artigo de modo que o leitor conheça um pouco sobre criptografia, especialmente, porque vivemos o advento das tecnologias de comunicação e informação, bem como apresentamos o Rivest, Shamir, Adleman (RSA), um sistema de criptografia de chave pública. Além disso, o conceito de função inversa. Na continuidade, codificamos e decodificamos uma mensagem fazendo uso de uma função inversa.

2 CRIPTOGRAFIA E O SISTEMA RSA

Desde as civilizações mais antigas, até os dias atuais, a comunicação entre reinos ou países fez-se necessária. Entretanto, muitas são as informações sigilosas que garantem a segurança dos povos, como, por exemplo, a comunicação entre países aliados na criação de uma nova tecnologia, as transações bancárias via internet ou uma simples troca de mensagens entre usuários de um site ou aplicativo (COUTINHO, 2009). Posto isso, são grandes os riscos se as mensagens sigilosas forem interceptadas. Essa ameaça gerou a necessidade do desenvolvimento de métodos para camuflar as mensagens, denominados códigos. “Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo.” (SINGH; SIMON, 2004, p. 11). Os códigos mais simples consistem em substituir uma letra do alfabeto por outra, os quais, em conformidade com Coutinho (2009), já eram utilizados pelo ditador romano Júlio César para levar mensagens às suas tropas durante as guerras pela Europa.

Embora os principais códigos usados na proteção de informações sejam elaborados por matemáticos ou pesquisadores com conhecimento profundo na área, os sistemas criptográficos são amplamente utilizados no meio civil. Isso mostra o quanto a Criptografia está presente no nosso cotidiano, sempre abrindo espaço para cifradores e decifradores.

De acordo com Singh (2003), acredita-se que, com o desenvolvimento matemático sobre a Criptografia, a Terceira Guerra Mundial será dos matemáticos, uma vez que estes terão o controle sobre uma grande arma: a transmissão segura de informações.

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. (SINGH, 2003, p.13)

Uma vez que a criptografia é responsável pelo sigilo de dados importantes nas mais diversas áreas, não poderia ser algo de fácil decodificação. A palavra criptografia deriva do grego, *cryptos*, que significa secreto, oculto e *grafo* (grafia, escrita). A Criptografia estuda os métodos de codificação de mensagens para que somente o destinatário preestabelecido consiga ler seu conteúdo.

Para Coutinho (2009), o ato de criptografar vem acompanhado de duas receitas: uma para codificar e outra para decodificar. Codificar é o ato de camuflar uma mensagem de modo que somente o destinatário legítimo possa lê-la. Decodificar é o que o destinatário faz quando recebe uma mensagem e deseja ter acesso ao seu conteúdo. Nesse contexto, podemos utilizar outro termo: decifrar, que consiste em ter conhecimento das informações sem ser o destinatário legítimo.

Coutinho (2009) defende, também, que métodos criptográficos que consistem simplesmente em substituir uma letra do alfabeto por um símbolo qualquer são facilmente decifráveis, haja vista que as características da língua portuguesa, por exemplo, facilitam esse deciframento. Segundo o autor, na nossa língua, as vogais são mais frequentes que as consoantes; a vogal mais frequente é o "A"; monossílabo com uma única letra é uma vogal, dentre outras. Fatos como esse facilitam quebrar o código e decifrar as mensagens criptografadas. E isso torna-se ainda mais fácil se a mensagem for longa, devido à frequência das letras. Vale ressaltar que existem programas de computador que decifram mensagens desse tipo, em frações de segundo, tornando qualquer tipo de código que

envolva substituição de letras inseguro. Tomemos, por exemplo, a frequência aproximada das letras em português (em %) expressa na tabela 01, a seguir.

Tabela 01 – Frequência das letras do alfabeto português (língua portuguesa brasileira).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7	4,7	5,0	10,7	2,5
Q	R	S	T	U	V	W	X	Y	Z						
1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2	0,01	0,4						

Fonte: Coutinho (2015, p. 3)

Usando a frequência das letras em português, podemos decifrar a mensagem:

B qbmbxsb dsjquphsbgjb bjoeb fxpdb jnbhfot ef bhfouft tfdsfupt! Para tanto, precisamos verificar a frequência de cada letra (vide tabela 02, a seguir).

Tabela 02 – Frequência das letras da mensagem para codificação

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	11	0	3	2	7	1	3	0	4	0	0	1	1	3	3
Q	R	S	T	U	V	W	X	Y	Z						
2	0	4	4	3	0	0	2	0	0						

Fonte: Construção própria

Observe que a letra “b” é a mais frequente (11), seguida da letra “f” (7), depois “j”, “s” e “t” (4),... Provavelmente “b” seja a codificação da letra “a”, assim como a letra “f”, a da letra “e”. Fazendo essa substituição chegaremos à: A qAmAxsA dsjquphsAgjA AjoeA ExpdA jnAhEot eE AhEouEt tEdsEupt!

A letra “t” codifica “r”, “o” ou “s”. O mais provável é a terceira opção, já que muitas palavras na língua portuguesa terminam em “s”. Temos: A qAmAxsA dsjquphsAgjA AjoeA ExpdA jnAhEoS eE AhEouES SEdsEupS!

Se “s” codifica “r” temos: A qAmAxRA dsjquphRAgjA AjoeA ExpdA jnAhEoS eE AhEouES SEdREupS!

Agora, a palavra SEdREupS aparenta ser SECRETAS ou SECRETOS. Entretanto, como “p” não pode codificar “a” (porque “b” codifica “a”), então a palavra é SECRETOS. Assim, “d” codifica “c”, “u” codifica “t” e “p” codifica “o”. Com isso temos: A qAmAxRA CRjqTOhRAgjA AjoeA ExOCA jnAhEoS eE AhEoTES SECRETOS!

Aparentemente a palavra CRjqTOhRAgjA é, na verdade, CRIPTOGRAFIA. Assim sendo, “j” codifica “i”, “q” codifica “p”, “h” codifica “g”, “g” codifica “f” e “j” codifica “i”. O que nos permite chegar à: A PAmAxRA CRIPTOGRAFIA AIoeA ExOCA InAGEoS eE AGEoTES SECRETOS! Disso, podemos reconhecer a palavra

PAmAxRA, a qual deve ser a codificação de PALAVRA. Logo, "m" codifica "l", "x" codifica "v" e "o" codifica "n". Com isso, passamos a ter a seguinte mensagem: A PALAVRA CRIPTOGRAFIA AINeA EVOCA InAGENS eE AGENTES SECRETOS! Feitas essas substituições, fica fácil perceber que "e" codifica "d" e "n" codifica "m". Assim, a mensagem totalmente decifrada é: A PALAVRA CRIPTOGRAFIA AINDA EVOCA IMAGENS DE AGENTES SECRETOS!

O aumento de interceptações de mensagens nos meios de comunicação gerou a necessidade da proteção de informações de modo que apenas o destinatário legítimo saiba seu conteúdo. Assim, tronou-se imperativo inventar códigos que fossem difíceis de serem quebrados, mesmo com a ajuda de um computador, os chamados códigos de chave pública, nos quais, saber codificar não implica saber decodificar. Sabemos, por exemplo, que, ao efetuarmos transações que envolvem dinheiro (compras com cartão de crédito ou saques em terminais de autoatendimento), as informações referentes a essas transações circulam por linhas telefônicas ou rede e podem ser interceptadas. Entretanto, a situação não se encerra por aí! As informações não seguem desprotegidas, elas são criptografadas, de modo que só o destinatário estabelecido consegue ter acesso ao conteúdo. Dessa forma, mesmo que alguém intercepte uma mensagem, não conseguirá interpretar as informações contidas nela, uma vez que a segurança das informações que trafegam nas redes eletrônicas é garantida pelo método de criptografia de chave pública Rivest, Shamir e Adleman (RSA).

De acordo com Coutinho (2009), a Criptografia RSA trabalha com algoritmos computacionais utilizando a chave pública. Esse código foi inventado em 1978, por R. L. Rivest, A. Shamir e L. Adleman, que, na época, trabalhavam no *Massachussets Institute of Technology* (M.I.T.). As letras RSA correspondem às iniciais dos nomes dos inventores do código. A segurança desse sistema criptográfico está baseada na dificuldade de obterem-se os fatores primos de um número dado. A RSA explora essa situação ao utilizar um número de aproximadamente 231 algarismos, e que é o produto de dois números primos muito grandes.

De modo geral, Coutinho (2009) define que a implementação do método RSA exige dois parâmetros, isto é, dois números primos grandes chamados de "p" e "q". Para codificar uma mensagem é suficiente conhecer o produto "$n = p \times q$". Para decodificar é necessário conhecer "p" e "q". A segurança do método é garantida pelo fato de que se

"n" for suficientemente grande, fatorá-lo pode se tornar muito difícil. Dessa forma, a segurança do método está na dificuldade de descobrirem-se "p" e "q" com os atuais métodos de fatoração (principalmente, se "n" possui 150 algarismos ou mais). Logo, os números primos devem ser mantidos em segredo, uma vez que eles garantem a segurança das mensagens enviadas. Já "n" pode ser enviado para qualquer usuário, o qual será usado para codificar as mensagens.

Por ser um método de chave pública, o RSA permite que qualquer usuário codifique mensagens. Entretanto, como a chave de decodificação é secreta, só o destinatário legítimo pode decodificá-las.

Nos métodos de criptografia, é necessário que haja autenticidade. Nesse sentido, um recurso conhecido como assinatura digital é muito utilizado. Trata-se de um meio que permite verificar se determinada mensagem foi emitida por certa entidade ou pessoa. Vejamos um exemplo: suponha que uma pessoa "X" deseja comunicar-se com uma pessoa "Y" e queira garantir legitimidade. A pessoa "X", então, assina a mensagem utilizando sua chave privada. Em seguida, criptografa-a, utilizando a chave pública de "Y". Esta, ao receber a mensagem, deve decodificá-la com sua chave privada (o que garante sua privacidade) e, em seguida, verifica a assinatura utilizando a chave pública de "X" (garantindo a autenticidade).

É notório que, desde os primórdios até os dias atuais, a criptografia evoluiu muito. Entretanto, a sua essência continua e pode ser resumida conforme figura 1, a seguir:

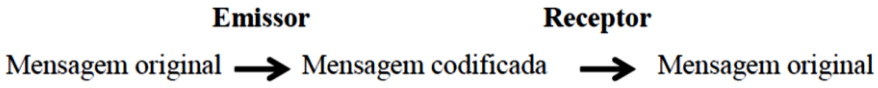

Figura 1 – Esquema da Criptografia
Fonte: Construção própria

Nesse contexto, é possível verificar que há bastante familiaridade nos conceitos de criptografia e função inversa, uma vez que o emissor deve enviar uma mensagem usando um(a) código/função "f" e o receptor, conhecendo os caminhos que desvendem a mensagem, aplica a chave de decodificação/função inversa "f^{-1}".

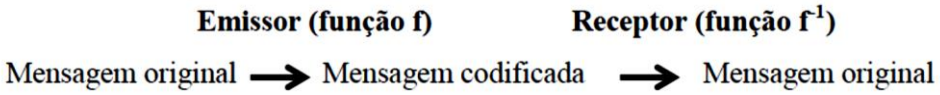

Figura 2 – Esquema da Criptografia
Fonte: Construção própria

A descrição detalhada do método de criptografia RSA exige familiaridade com conceitos da Teoria dos Números, o que não é o caso neste momento, porque fizemos a opção pelo uso da função inversa.

2.1 Um breve panorama sobre estudos que tematizam a criptografia

A temática da criptografia já é uma realidade presente em pesquisas voltadas para os processos de ensino e aprendizagem de matemática. Rosseto (2018) desenvolveu junto a estudantes da Educação Básica algumas maneiras de utilizar a criptografia como forma de trazer significado à aprendizagem e cativar o estudante. Mostrou como a Criptografia pode ser abordada em vários conteúdos do Ensino Fundamental e Médio, mais precisamente, em atividades que tratam de funções e matrizes. Em sua pesquisa, notou que não foi só o rendimento escolar que melhorou. A empatia e a disposição dos estudantes evoluíram e eles passaram a compreender e aplicar conhecimentos para o desenvolvimento de atividades em outras áreas do saber como por exemplo, Química, Física e Bologia.

Ganassoli e Schankoski (2015) desenvolveram uma investigação voltada para a motivação e o enriquecimento teórico de professores da Educação Básica. As pesquisadoras apresentaram ideias para a contextualização da Matemática com o uso da Criptografia como recurso metodológico. Para isso, sugeriram várias atividades, englobando diversos conteúdos, dentre eles: análise combinatória, matrizes, funções e o algoritmo da divisão. A pesquisa trouxe à tona a realidade de que assuntos do cotidiano podem ser investigados e aplicados em sala de aula, oportunizando aos estudantes ver a Matemática sob outra perspectiva.

Arinos (2014) relatou um pouco da história da criptografia e propôs várias atividades didáticas para motivar os estudantes para a construção do conhecimento dos conceitos de divisibilidade, funções, análise combinatória e matrizes. Foi possível notar que a criptografia aliada à atividades didáticas atraentes e à assuntos do interesse dos estudantes contribui para a aprendizagem de matemática.

Na pesquisa de Oliveira e Kripka (2011), foram definidos os conceitos gerais sobre Criptografia e as contribuições de diversos matemáticos. Esses autores sugeriram atividades para serem desenvolvidas em sala de aula, fazendo uso da Criptografia para facilitar a aprendizagem de matemática. Os resultados indicaram que a aprendizagem

tornou-se significativa para os estudantes, motivando-os a resolver problemas em sala de aula.

Assim, vemos a possibilidade de aplicação de criptografia aliada ao estudo de funções inversas, para despertar o interesse e chamar a atenção dos estudantes para a analogia existente entre os dois conceitos.

2.1 Função inversa

Do ponto de vista da Matemática, entende-se função (f) como uma relação entre os elementos de dois conjuntos, de modo que "a todo elemento (x) do conjunto de partida (A) faz-se corresponder a um único elemento (y) do conjunto de chegada (B). Ou ainda, **para todo** $x \in A$ existe **um único** $y \in B$**, em que** x se relacione com y" (DANTE, 2013). Para esse autor, "a função g: B$\rightarrow$A é a inversa da função $f: A \rightarrow B$ quando se tem $g(f(x)) = x$ e $f(g(y)) = y$ para todo $x \in A$ e $y \in B$" (DANTE, 2013, p. 187). Analogamente, Flemming e Gonçalves (2012) afirmam que, dada uma função f: A$\rightarrow$B, de modo que, para todo $y \in B$, exista um único $x \in A$, o qual $f(x) = y$, então a função inversa de f (denotada por f^{-1}) é a função $g: B \rightarrow A$, tal que $g(y) = x$.

Uma função admite sua inversa quando for, simultaneamente, injetora e sobrejetora, portanto, uma função bijetora. Dante (2012) classifica como injetora aquela função $f: A \rightarrow B$ em que elementos diferentes de A são transformados em elementos diferentes de B. Segundo esse autor, a função sobrejetora existe quando todo elemento de B é imagem de pelo menos um elemento de A, isto é, Im (f) = B. Logo, para calcular sua inversa, uma função precisa cumprir os requisitos da injetividade e da sobrejetividade.

Para melhor compreender o processo de obtenção de uma função e sua inversa, tomemos como exemplo os dados dispostos na Tabela 3 a seguir.

Tabela 3 – Relação de quantidade entre dois conjuntos "A" e "B"

A	-3	-2	-1	0	1	2	3
B	-13	-10	-7	-4	-1	2	5

Fonte: Construção própria

Esboçando as coordenadas de A e B num plano cartesiano temos:

A = (-3, -13)
B = (-2, -10)
C = (-1, -7)
D = (0, -4)
E = (1, -1)
F = (2, 2)
G = (3, 5)

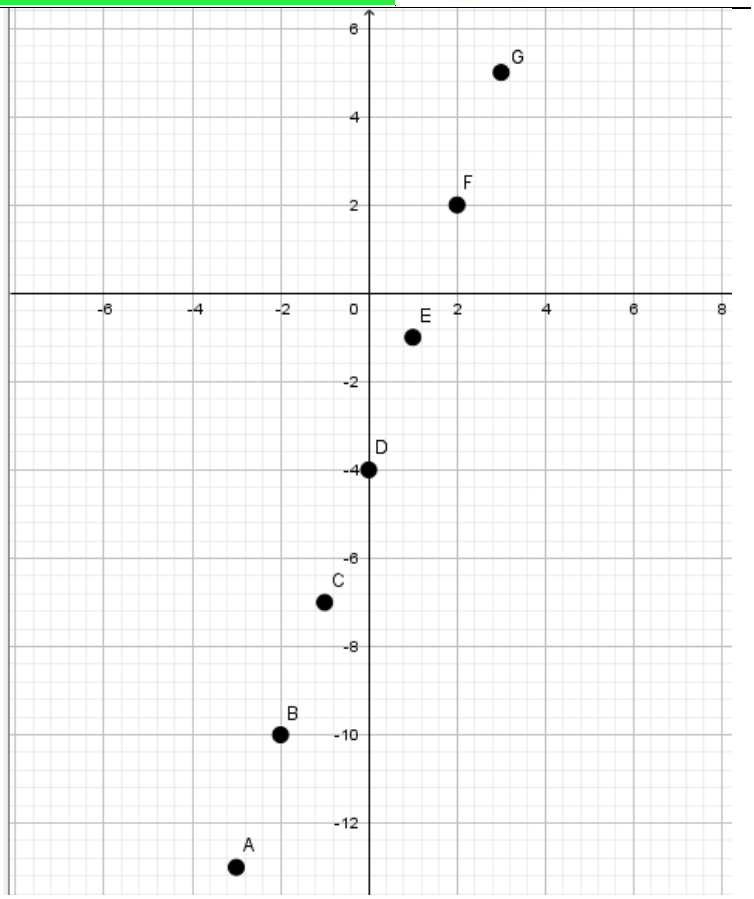

Figura 3 – Representação geométrica da relação entre os conjuntos "A" e "B"
Fonte: Construção própria

Note que os pontos estão alinhados. Por conseguinte, o conjunto A é associado a B por uma função afim $f(x) = ax + b$. De posse disso, e sabendo que $f(-3) = -13$, bem como $f(-2) = -10$, é possível montar o seguinte sistema:

$$\begin{cases} -3a + b = -13 \\ -2a + b = -10 \end{cases}$$

Multiplicando-se a segunda equação por -1, tem-se:

$$\begin{array}{l} \{-3a+b=-13 \\ \underline{+2a-b=+10} \\ -a=-3 \end{array} \quad \Rightarrow \quad a = 3$$

Uma vez que $a = 3$, temos:

$$-3 \times 3 + b = -13$$

$$-9 + b = -13$$

$$b = -13 + 9$$

$$b = -4$$

Assim, temos a função $f(x) = 3x - 4$ ou $y = 3x - 4$.

Para encontrar sua inversa, isola-se "x" no segundo membro da igualdade, assim:

$$y = 3x - 4$$
$$y + 4 = 3x$$
$$\frac{y+4}{3} = x$$

Com isso temos função f^{-1} definida como $x = \frac{y+4}{3}$ é chamada função inversa de f(x) = 3x – 4. Ou ainda, a função inversa de $f(x) = 3x - 4$ é $f^{-1}(x) = \frac{x+4}{3}$

Diante disso, podemos confrontar os dados obtidos, nas duas funções (conforme dispostos nas tabelas 4 e 5, a seguir) e assim conferir a inversão.

Tabela 4 – $f(x) = 3x - 4$

x	$f(x) = 3x - 4$
-3	$3 \times (-3) - 4 = -9 - 4 = -13$
-2	$3 \times (-2) - 4 = -6 - 4 = -10$
-1	$3 \times (-1) - 4 = -3 - 4 = -7$
0	$3 \times 0 - 4 = 0 - 4 = -4$
1	$3 \times 1 - 4 = 3 - 4 = -1$
2	$3 \times 2 - 4 = 6 - 4 = 2$
3	$3 \times 3 - 4 = 9 - 4 = 5$

Fonte: Construção própria

Tabela 5 – $f^{-1}(x) = \frac{x+4}{3}$

x	$f^{-1}(x) = \frac{x+4}{3}$
-13	$\frac{-13+4}{3} = \frac{-9}{3} = -3$
-10	$\frac{-10+4}{3} = \frac{-6}{3} = -2$
-7	$\frac{-7+4}{3} = \frac{-3}{3} = -1$
-4	$\frac{-4+4}{3} = \frac{0}{3} = 0$
-1	$\frac{-1+4}{3} = \frac{3}{3} = 1$
2	$\frac{2+4}{3} = \frac{6}{3} = 2$
5	$\frac{5+4}{3} = \frac{9}{3} = 3$

Fonte: Construção própria

Uma propriedade importante das funções inversas é que elas são simétricas em relação à função $h(x) = x$, a chamada função identidade. Dessa forma, das funções representadas temos:

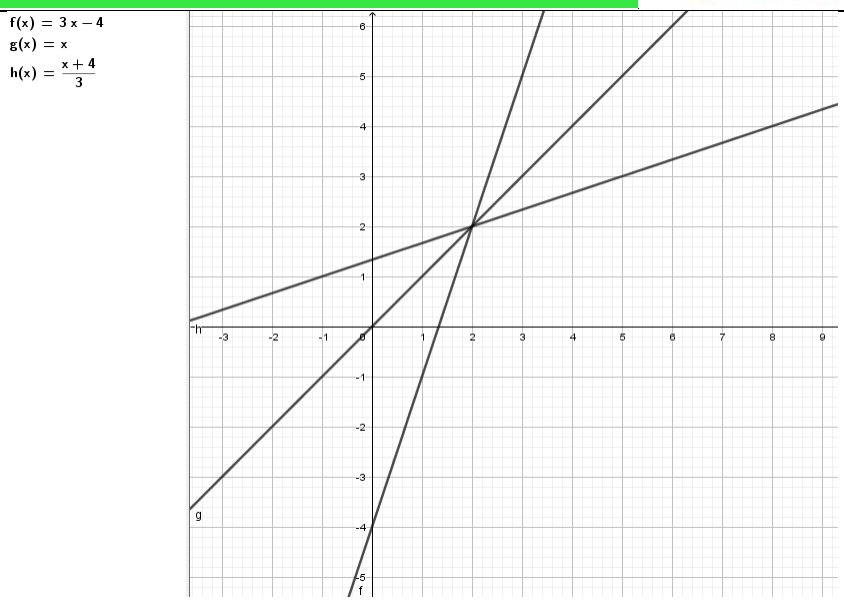

Figura 4 – Representação geométrica da função identidade
Fonte: Construção própria

É importante ressaltar que nem toda função $f: \mathbb{R} \to \mathbb{R}$ possui inversa. Segundo Flemming e Gonçalves (2012), uma função f possui inversa se, e somente se, toda reta paralela ao eixo das abscissas intersectar o gráfico de f num único ponto.

Por exemplo, a função $y = 3x - 4$ satisfaz essa condição:

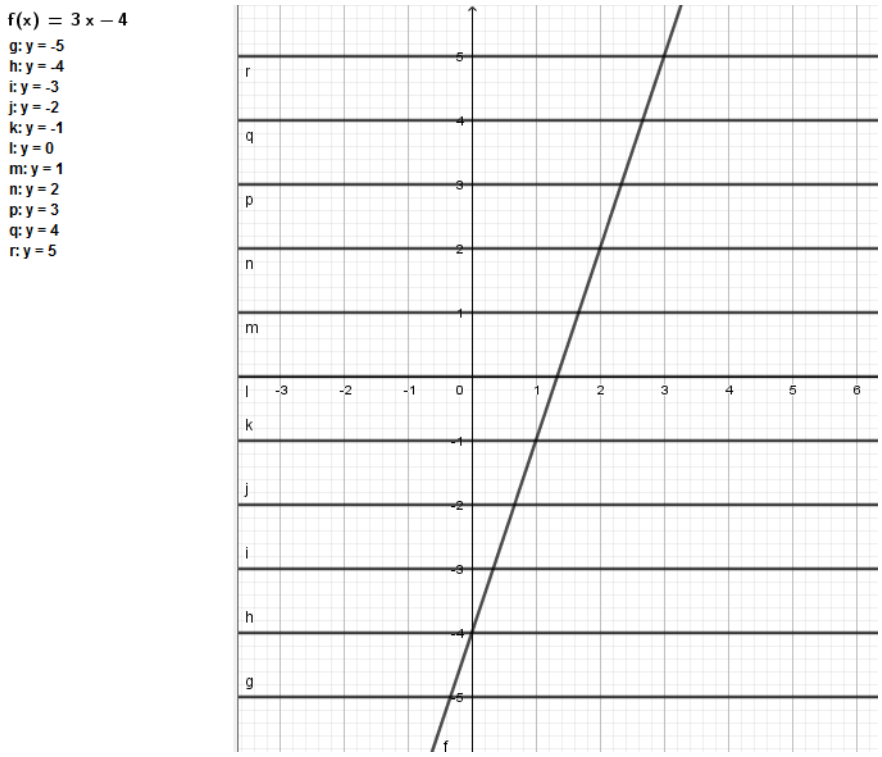

Figura 5 – Retas paralelas ao eixo das abscissas intersectando a função y = 3x – 4
Fonte: Construção própria

Conhecer as principais propriedades das funções facilita o processo de estabelecimento da função inversa e, por conseguinte, da decodificação.

2.3 Codificando e decodificando mensagem a partir da função inversa

Imagine que você tenha que enviar, de forma cifrada a seguinte mensagem "Criptografar é uma arte". Inicialmente é preciso pensar na pré-codificação, a qual requer a substituição de letras por números. Com o propósito de exemplificar esse processo, o primeiro passo consiste em converter uma mensagem que se deseja criptografar em uma sequência de números. Para tanto, veja as informações constantes na tabela 03, a seguir.

Optamos por corresponder cada letra a um número maior ou igual a 10 para evitar ambiguidades, haja vista que, caso fizéssemos corresponder a letra "A" ao número 1, "B" ao número 2, e assim por diante, poderia haver confusão de interpretação do número 23, pois não saberíamos se era "BC" ou "W" (23ª letra do alfabeto). Registra-se também que os espaços entre as palavras serão preenchidos pelo número 99.

Tabela 6 – Correspondência entre cada letra do alfabeto e um número maior ou igual a 10

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Q	R	S	T	U	V	W	X	Y	Z						
26	27	28	29	30	31	32	33	34	35						

Fonte: Construção própria

Nesse contexto, a frase "Criptografar é uma arte", é convertida em:

12271825292416271015102799149930221099102729 14

Na codificação da mensagem, devemos quebrar em blocos a sequência de números produzidos na pré-codificação. Assim, a sequência de números pode ser quebrada nos seguintes blocos, o que não é uma condição *sine qua non*.

12-2-71-8-25-29-2-41-62-7-10-15-10-27-9-9-14-9-9-30-22-10-9-9-10-2-72-9-14

Cada bloco deve ser codificado separadamente. Depois disso, não poderão mais ser unidos sob o risco de tornar impossível decodificação da mensagem. De modo geral, para codificar a mensagem precisamos de uma função "f", tal que "f" seja invertível. Usaremos "f" como chave de codificação. A chave de decodificação será a função f^{-1}. Portanto, dado um bloco "b" o emissor aplica a função ao bloco obtendo $f(b)$. O receptor, por sua vez, aplica f^{-1} a $f(b)$ e obtém assim a mensagem original.

Tomemos, por exemplo, a função invertível $f(x) = 3x - 4$ como chave de codificação.

Desse modo, aplicando "f" ao primeiro bloco (12):

$f(12) = 3 \times 12 - 4 = 32$

Segundo bloco (2):

$f(2) = 3 \times 2 - 4 = 2$

Terceiro bloco (71):

$f(71) = 3 \times 71 - 4 = 209$

Quarto bloco (8):

$f(8) = 3 \times 8 - 4 = 20$

Os demais blocos também são codificados de maneira análoga. Com isso obtemos a mensagem criptografada:

32-2-209-20-71-83-2-119-182-17-26-41-26-77-23-23-38-23-23-86-62-26-23-23-26-2-212-23-38

Para decodificar a mensagem criptografada, precisamos da função inversa de $f(x) = 3x - 4$, portanto, $f^{-1}(x) = \frac{y+4}{3}$.

Nesse sentido, decodificamos os blocos codificados aplicando f^{-1}, assim:

Primeiro bloco (32):

$$f^{-1}(32) = \frac{32 + 4}{3} = 12$$

Segundo bloco (2):

$$f^{-1}(2) = \frac{2+4}{3} = 2$$

Terceiro bloco (209):

$$f^{-1}(209) = \frac{209 + 4}{3} = 71$$

Quarto bloco (20):

$$f^{-1}(20) = \frac{20 + 4}{3} = 8$$

Assim como na codificação, todos os blocos são decodificados de maneira análoga, obtendo-se a sequência: 12-2-71-8-25-29-2-41-62-7-10-15-10-27-9-9-14-9-9-30-22-10-9-9-10-2-72-9-14. Suprimido os traços entre os blocos, teremos a sequência original:

3 TECENDO CONSIDERAÇÕES

Este artigo expõe que a utilização da Criptografia no processo de envio de mensagens/informações não é algo recente na história da humanidade, mas que, com o advento das novas tecnologias de informação e comunicação, amplia seus espaços, mostrando-se como fonte promissora de estudos, haja vista que viabiliza a transmissão de dados e informações, muitas vezes sigilosos. Ademais, ela pode constituir-se como motivação ao processo de ensino e aprendizagem, inclusive de matemática, nos diversos níveis de escolarização. A vantagem da Criptografia reside na segurança máxima que a mesma propicia aos meios de comunicação, o que se torna possível mediante conhecimentos de sistemas de algoritmos e matemática.

Dada a grande aplicabilidade da Criptografia na transmissão de informações via redes, e sendo ela pouco conhecida por professores e estudantes, torna-se importante sua inclusão no processo de ensino e aprendizagem de matemática, especialmente, pela curiosidade que ela pode suscitar nos estudantes. Assim, a Criptografia apresenta-se também como agente motivador para incentivar o desenvolvimento de atividades didáticas e trabalhar os conceitos de conjuntos, números primos, equação, função e matriz, dentre outros.

O desenvolvimento de atividades didáticas envolvendo Criptografia requer que professores e estudantes desempenhem papéis ativos no processo de ensino e aprendizagem. Assim, o planejamento das ações de sala de aula deve:

i. atender as curiosidades e/ou necessidades dos estudantes;
ii. considerar os conhecimentos que já dispõem sobre o assunto e auxiliá-los na compreensão do que estão fazendo;
iii. levá-los a conjecturar e propor alternativas para solucionar o enigma;
iv. deixar claro os objetivos a serem alcançados;
v. municiá-los com dados e informações que propiciem condições para que respondam ao que lhes é demandado;
vi. propiciar um ambiente de estudo/trabalho colaborativo;
vii. permitir reflexões e trocas de ideias;

viii. avaliar as aprendizagens, bem como, outras condições que favoreçam as aprendizagens.

Codificar e decodificar mensagens consiste num processo de fazer e desfazer algo, o que coincide com o princípio da função inversa. Assim, a abordagem de codificação e decodificação de mensagens aqui expostas (Criptografia) pode conceber um bom recurso pedagógico para que os professores lancem mão, principalmente, no desenvolvimento de atividades didáticas referentes ao conceito de função inversa.

REFERÊNCIAS

ARINOS, Edgard José dos Santos. Criptografia: aplicações no ensino fundamental e médio. 2014. 100 f. Dissertação (Mestrado Profissional) – Instituto de Matemática, Universidade Federal de Mato Grosso de Sul, Campo Grande, MS.

BRASIL, Parâmetros Curriculares Nacionais. Matemática: ensino de quinta a oitava séries. Brasília, 1998.

CAMPOS, Dinah Martins de Souza. Psicologia da adolescência. Rio de Janeiro: Vozes, 1996.

CERVO, Amado Luiz; BERVIAN. Pedro Alcino. Metodologia científica: para uso dos estudantes universitários. São Paulo: McGraw-Hill do Brasil, 1983.

COUTINHO, Severino Collier. Números Inteiros e Criptografia RSA. 2. Ed. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada - IMPA, 2009.

COUTINHO, Severino Collier. Criptografia. Rio de Janeiro, Programa de Iniciação Científica da OBMEP (PIC-OBMEP), 2015. Instituto Nacional de Matemática Pura e Aplicada – IMPA. nº 7, 1ª edição.

DALFOVO, Michael Samir; LANA, Rogério Adilson; SILVEIRA, Amélia. Métodos quantitativos e qualitativos: um resgate teórico. Revista Científica Aplicada, Blumenau, v. 2, n. 4, p. 01-13, Sem II. 2008.

DANTE, Luiz Roberto. Matemática: contexto e aplicações. 2 ed. São Paulo: Ática, 2013.

FLEMMING, Diva Marília; GONÇALVES, Mirian Buss. Cálculo A. 6. ed. São Paulo: Pearson, 2012.

FONSECA, João José Saraiva da. Metodologia da pesquisa científica. Fortaleza: UEC, 2002. Apostila.

GANASSOLI, Ana Paula; SCHANKOSKI, Fernanda Ricardo. Matemática e Criptografia. 2015. 103 f. Dissertação (Mestrado Profissional - PROFMAT) – Departamento de Matemática, Universidade Federal do Paraná, Curitiba, PR.

OLIVEIRA, Daiane de; KRIPKA, Rosana Maria Luvezute. O uso de criptografia no ensino de matemática. In: XIII CIAEM-IACME, Recife, Brasil, 2011.

ROSSETO, Cintia Kohori. Criptografia como recurso didático: uma proposta metodológica aos professores de matemática. 2018. 84 f. Dissertação (Mestrado Profissional - PROFMAT) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas, São José do Rio Preto, SP.

SINGH, Simon. O Livro dos Códigos: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: Record, 2003.

SINGH, Simon. O Livro dos Códigos. trad. Jorge Calife. 4 ed. Rio de Janeiro: Record, 2004.

Submetido em: 03 de abril de 2019.

Aprovado em: 15 de abril de 2019.