UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
CAMPUS DE TRÊS LAGOAS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

RAFAEL DE OLIVEIRA LIMA

# A CRIPTOGRAFIA USADA COMO FERRAMENTA CAPAZ DE FIXAR CONTEÚDOS E DE DESPERTAR O INTERESSE PELA MATEMÁTICA NO ENSINO MÉDIO E SUPERIOR

TRÊS LAGOAS - MS
2019

**UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL**
**CAMPUS DE TRÊS LAGOAS**
**PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT**

# A CRIPTOGRAFIA USADA COMO FERRAMENTA CAPAZ DE FIXAR CONTEÚDOS E DE DESPERTAR O INTERESSE PELA MATEMÁTICA NO ENSINO MÉDIO E SUPERIOR

Dissertação apresentada ao Programa de Mestrado Profissional em Rede Nacional – PROFMAT, da Universidade Federal de Mato Grosso do Sul, Campus de Três Lagoas, como parte dos requisitos para obtenção do título de Mestre em Matemática.

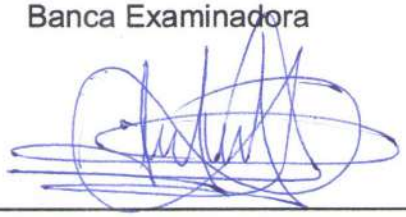
Orientador: Prof. Dr. Fernando Pereira de Souza

**TRÊS LAGOAS – MS**
**2019**

LIMA, Rafael de Oliveira. **A CRIPTOGRAFIA USADA COMO FERRAMENTA CAPAZ DE FIXAR CONTEÚDOS E DE DESPERTAR O INTERESSE PELA MATEMÁTICA NO ENSINO MÉDIO E SUPERIOR.** 2019. Dissertação (Mestrado em Matemática) – Universidade Federal de Mato Grosso do Sul, Campus de Três Lagoas, Três Lagoas, 2019.

Aprovado em: 14/11/2019

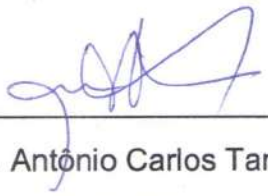
Banca Examinadora



Prof. Dr. Fernando Pereira de Souza

(Orientador)

UFMS/CPTL



Prof. Dr. Antônio Carlos Tamarozzi

UFMS/CPTL

Profª. Dra. Nair Rodrigues

IFMS – Campus de Três Lagoas

Novembro de 2019

## Dedicatória

Dedico este trabalho às minhas queridas tias,

Aurora e Oneida.

# AGRADECIMENTOS

Agradeço a Deus, sempre em primeiro lugar, por me permitir chegar tão longe e me amparar em todos os momentos difíceis durante essa jornada.

Ao meu orientador Prof. Dr. Fernando Pereira de Souza, agradeço pela força e pela ajuda, principalmente na escolha do tema e dos aspectos abordados referentes ao desenvolvimento do mesmo. Sou grato, ainda, a todos os professores do curso por acreditarem que conseguiríamos.

Agradeço também aos colegas de curso pela amizade, pelo carinho, pelas risadas, por fazer nossos sábados mais divertidos e é claro, pela troca de experiências e conhecimentos. Em especial, ao meu amigo Fabrício, companheiro de mestrado e também meu ex-professor que me manteve sempre confiante e que me fez acreditar que tudo daria certo.

Igualmente, agradeço aos meus queridos alunos do Ensino Médio, com destaque aos alunos Ana Beatriz Molina Ramos e Ítalo Fucci, por contribuírem de forma significativa, com interesse, força de vontade e curiosidade durante todas as atividades realizadas. Certamente foram o meu maior combustível durante toda essa caminhada.

Aos amigos e familiares, que neste período desculparam e compreenderam a minha ausência. E, em especial, também agradeço a todos aqueles que com suas orações e pensamentos positivos contribuíram para o êxito do desenvolvimento do meu projeto.

# RESUMO

Este trabalho objetiva apresentar criptografia aos alunos do ensino médio de duas maneiras: como agente motivador do despertar do interesse matemático por assuntos que tenham relevância em sua aplicabilidade e como ferramenta para fixar conteúdos importantes presentes nas atuais diretrizes educacionais. Uma breve abordagem histórica também será feita, mostrando um pouco da evolução da criptografia, bem como sua importância em cada época. Ainda, será proposta uma sequência de atividades didáticas, com intuito de que a evolução, no seu entendimento e estudo, seja gradativa. No início, uma abordagem com criptografias intuitivas terá como objetivo desenvolver o raciocínio lógico e o poder de trabalhar de forma cooperativa, em que os educandos serão os agentes do processo, criando seus próprios sistemas criptográficos e assumindo o protagonismo durante as aulas. Numa etapa posterior, a criptografia será incorporada ao estudo das funções afins e das matrizes, partindo do pressuposto de que o aluno tenha conhecimento prévio em tais assuntos e que assim, tal metodologia possa ser usada para fixação de conteúdos matemáticos relevantes e sempre presentes nas matrizes curriculares das mais variadas unidades didáticas. Por fim, uma apresentação do método de criptografia RSA, que por se tratar de um assunto mais aprofundado da Teoria dos Números, será feito com o intuito de sugerir uma maneira atrativa de abordar e de aperfeiçoar o estudo de tal ramo matemático no ensino superior, visto que sua abordagem nesta etapa do ensino muitas vezes é pouco prática e considerada enfadonha. O método apresentará a importância da existência de uma criptografia de chave pública segura e que possa ser amplamente usada num mundo de constantes avanços tecnológicos em consonância com sérias ameaças de quebras de segurança. O RSA foi criado exatamente para suprir as necessidades de uma sociedade que, cada vez mais, realiza suas transações bancárias, comerciais e sociais via web.



**Palavras-chave:** Criptografia; Funções Afins; Matrizes; Teoria dos Números; RSA.

# ABSTRACT

This work aims to present cryptography to the high school students in two ways: as a motivating agent for arousing interest by mathematic subjects that are relevant in their applicability and as a tool to fix important content in current educational guidelines. A brief historical approach will also be made, showing a little of the evolution of cryptography, as well as its importance in each epoch. Still, a sequence of didactic activities will be proposed, with the intention that evolution, in its understanding and study, is gradual. At the beginning, an intuitive encryption approach will aim to develop logical thinking and the power of working cooperatively, that learners will be the agents of the process, creating their own cryptographic systems and taking the lead in class. At a later stage, encryption will be incorporated into the study of related functions and matrices, assuming that the student has prior knowledge of such matters and that such methodology may be used for setting relevant and always present mathematical content in the curriculum matrices of the most varied didactic units. Finally, a presentation of the RSA encryption method, which in turn deal with the further Theory Number, will be made with the suggest of an attractive way to approach and refine the study of such a mathematical branch in higher education, since its approach at this stage of teaching is often impractical and considered boring. The method will present the importance of the existence of an encryption secure public key that can be widely used in a world of constant technological advances in line with serious threats of security breaches. The RSA was created exactly to supply the needs of a society that increasingly carries out its banking transactions, commercial and social services on the web.



**Keywords**: Cryptography; Related Functions; Matrices; Theory of Numbers; RSA.

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE GRÁFICOS

# SUMÁRIO

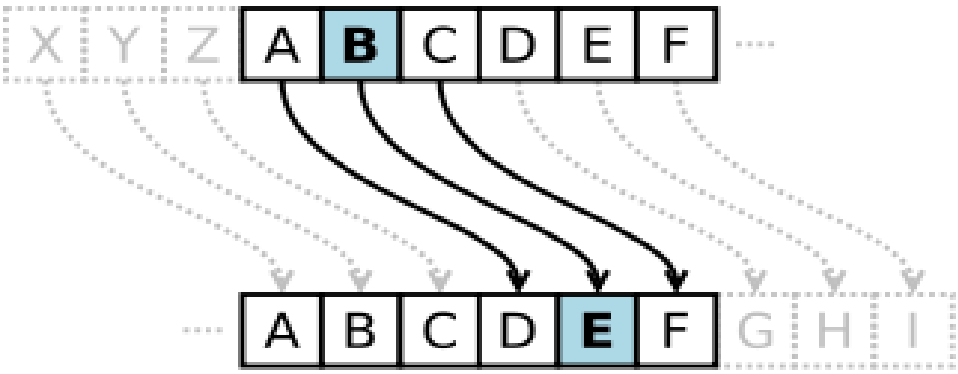
# INTRODUÇÃO

A origem do termo criptografia vem do grego, em que kryptos significa escondido ou oculto e graphein significa escrita (SINGH, 2003). A criptografia busca o estudo dos métodos para se codificar uma mensagem de modo que só seu destinatário legítimo consiga decifrá-la. É a arte ou ciência de escrever em códigos secretos (TAMAROZZI, 2001).

Os primeiros indícios de seu uso remetem a assuntos ligados à guerra, ao amor e à diplomacia entre nações, sendo que em todos são evidenciados o caráter necessariamente secreto entre a transmissão e a receptação da mensagem. Na guerra, com o intuito de que o inimigo não obtivesse a estratégia de batalha do emissor da mensagem. No amor, havia o interesse de que segredos amorosos não fossem revelados. Na diplomacia, com a necessidade do sigilo, visto que adversários poderiam estragar acordos diplomáticos importantes entre as nações.

A criptografia é muito antiga, tanto quanto a própria escrita. Em diferentes épocas e lugares, sistemas sigilosos para ocultar informações na transmissão de mensagens secretas e importantes foram criados. Por exemplo, a criptografia já se fazia presente na escrita hieroglífica usada pelos escribas no Egito. Na Palestina, analogamente, foram usadas as cifras hebraicas. Da mesma forma, o Código de César, usado pelo ditador romano Júlio César (100-44 a.C.) em suas estratégias de combate, é um dos relatos mais antigos de codificação de que se tem notícia. Nele, César aplicava uma espécie de código de substituição que transladava as letras do alfabeto três casas adiante, conforme esquema da figura:

Figura 1: Estratégia usada por César

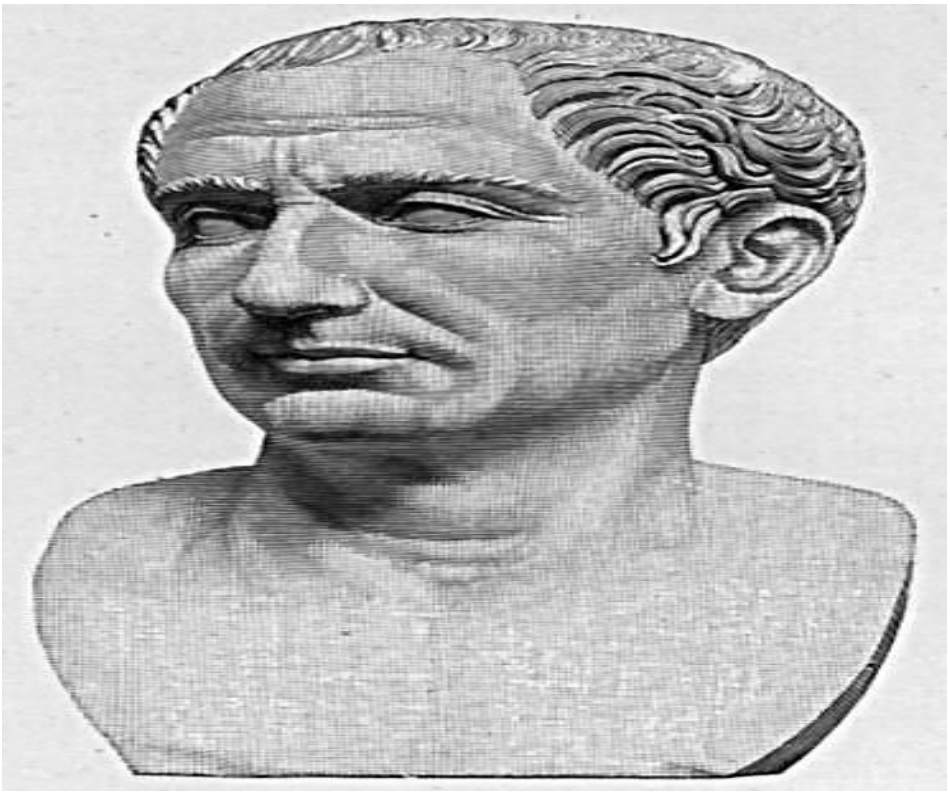



Fonte: setesys.com.br

Após um tempo, a denominação de Código de César passou a designar qualquer codificação na qual cada letra da mensagem fosse substituída por outra deslocada um número fixo de posições.

> “Discutivelmente, o esquema de criptografia mais antigo é a Cifra de Cesar, que recebeu esse nome em homenagem a Júlio Cesar, que usou este esquema para proteger importantes mensagens militares (todas as mensagens de César eram escritas em Latim, naturalmente, o que as tornava incompreensíveis para a maioria das pessoas). A Cifra de Cesar é uma maneira simples de confundir uma mensagem escrita em linguagem que forma palavras a partir de um alfabeto”. (GOODRICH, 2004. Pag.112).

Figura 2: Júlio César (100-44 a.C.)



Fonte: H. F. Helmolt (ed.): History of the World. New York, 1902

Por exemplo, a mensagem “INICIE A GUERRA”, por meio da estratégia mencionada anteriormente (translado das letras do alfabeto três casas adiante), seria codificada como:

LQLFLH D XHUUD

Um código como o de César pode não ser tão eficaz, tornando fácil de ser quebrado, principalmente nos dias de hoje, com tamanho avanço tecnológico, dotado de hackers e de investigadores em potencial.

> “Quebrar um código significa ser capaz de ler a mensagem, mesmo não sendo seu destinatário legítimo. Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto ocorre porque a frequência média com que cada letra aparece em um texto de uma dada língua é mais ou menos constante”. (Coutinho, 2015).

Esse tipo de codificação ficaria comprometida mediante a uma simples análise da frequência da utilização das letras na língua portuguesa, conforme mostra a tabela a seguir:

Tabela 1: Frequência das letras usadas no português

| Letra | % | Letra | % | Letra | % | Letra | % |
|---|---|---|---|---|---|---|---|
| A | 14,64 | G | 1,30 | N | 5,05 | T | 4,34 |
| B | 1,04 | H | 1,28 | O | 10,73 | U | 4,64 |
| C | 3,88 | I | 6,18 | P | 2,52 | V | 1,70 |
| D | 4,10 | J | 0,40 | Q | 1,20 | X | 0,21 |
| E | 12,57 | L | 2,78 | R | 6,53 | Z | 0,47 |
| F | 1,02 | M | 4,75 | S | 7,81 | | |

Fonte: Coutinho, 2015

Assim, por meio da simples contagem das letras presentes em um determinado texto codificado, poderiam ser descobertas as letras correspondentes comparando as informações com as da tabela de frequência vista acima. No entanto, é importante ressaltar que esse método de análise de frequências só funciona bem se o texto for longo. Em várias mensagens curtas, a incidência das letras não seria semelhante às da tabela, ou seja, ficaria muito difícil quebrar o código usando tal método. Caberia, então, fazer uma associação ao campo da estatística, cuja a inferência em determinado assunto se torna mais precisa quanto maior for a amostra da população consultada em determinada pesquisa.

É importante ressaltar que para que um método criptográfico funcione, é necessário que ele cumpra duas exigências:

I. Haja reversibilidade de toda a mensagem;

II. O receptor detenha a chave de decodificação.

Quando uma informação é criptografada, é necessário que seja possível descriptografá-la, ou seja, o sistema deve permitir desfazer aquilo que foi feito para se retornar a mensagem original, e também é preciso que, ao receber a mensagem codificada, o receptor de desejo do emissor detenha a chave para decodificar a mensagem, caso contrário fica praticamente impossível decodificá-la, ao menos que seja um sistema criptográfico muito simples de ser desvendado. Outro fato bastante importante, é que o sistema não pode criar ambiguidade durante o processo, isto é, deve haver uma correspondência biunívoca, em que cada mensagem criptografada retorna à sua mensagem original sem gerar dúvidas, incertezas ou ambiguidades. O mesmo se aplica a cada mensagem original que deve ser levada a uma criptografia particular sem gerar dúvidas ou falhas no processo de codificação da mensagem.

Em suma, pode ser feita uma analogia às funções bijetivas abordadas nas matrizes curriculares dos ensinos fundamental e médio das unidades didáticas. Considerando dois conjuntos, $A = \{\text{Mensagem original}\}$ e $B = \{\text{Mensagem codificada}\}$, é preciso que haja reversibilidade entre eles no processo, o que pode ser representado pelo esquema que segue:

$$\{\text{Mensagem original}\} \leftrightarrows \{\text{Mensagem codificada}\}$$

Além disso, para que a correspondência seja biunívoca e o sistema criptográfico não crie erros ou ambiguidades, os conjuntos $A$ e $B$ devem ter o mesmo número de elementos, fato que representa a necessidade da relação binária estabelecida entre os conjuntos ser uma função bijetiva.

Assim, a criptografia poderá ser abordada no estudo de funções bijetivas, em que a função original será responsável pela codificação e a sua função inversa, pela decodificação da mensagem. Esse tipo de estudo será abordado no capítulo $2$ deste trabalho como uma ferramenta importante, pois poderá ser usado por professores como uma estratégia alternativa de fixação de conteúdos matemáticos por parte dos alunos, como exemplos: funções afins e matrizes. Métodos de codificar uma mensagem por meio de funções e decodificar usando uma função inversa serão apenas usados com o intuito de fixar conteúdos, visto que podem ser quebrados facilmente em virtude da troca prévia de chaves entre emissores e receptores.

Nos dias atuais, a criptografia moderna usada nas transações eletrônicas via internet, nas quais um receptor recebe dados de milhares de emissores, deve criar uma ferramenta segura e eficaz na troca de informações, praticamente impossível de ser quebrada por terceiros. Será vista a importância de existir em tal método uma chave pública, de conhecimento e domínio de qualquer pessoa e que, mesmo sendo dessa maneira, não coloca sua credibilidade, eficiência e segurança em risco.

> "O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1977 por Ronald Linn Rivest, Adi Shamire e Leonard Max Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos sobrenomes dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais". (Coutinho, 2015).

O método RSA será apresentado no capítulo 3, evidenciando sua importância, o porquê de seu funcionamento e a dificuldade em ser quebrado. O tema também poderia ser levado aos alunos do ensino médio, no entanto, apenas a título de curiosidade, visto que tal método recorre a Teoria dos Números, ramo pouco abordado na educação básica. O despertar da curiosidade do aluno desta etapa do ensino, para a eficiência do método, poderia ser trabalhado usando a dificuldade na decomposição em fatores primos de números extremamente grandes. Entretanto, o tema será abordado voltando-se apenas para os alunos do ensino superior, como uma ferramenta capaz de aperfeiçoar o estudo do ramo da Teoria dos Números e de motivar os alunos com sua aplicabilidade prática por meio da criptografia.

Dividido em três capítulos, o presente trabalho tratou do uso da criptografia em sala de aula como uma ferramenta importante em vários aspectos da educação. No capítulo 1, após uma breve explicação expositiva feita pelo professor sobre as definições, importância e abordagem histórica da criptografia, os alunos foram tratados como protagonistas por meio de atividades em que puderam criar livremente modelos criptográficos, estimulando assim o raciocínio lógico e a capacidade de trabalhar de forma coletiva.

No capítulo 2, a criptografia foi usada como ferramenta capaz de possibilitar aos alunos a fixação de conteúdos matemáticos importantes presentes nas matrizes curriculares das mais variadas unidades didáticas. No caso deste trabalho, a

abordagem foi levada para o campo das matrizes e das funções afins, por meio de exercícios de fixação resolvidos de forma coletiva e individualizada.

O capítulo 3 foi feito com o mesmo intuito do capítulo 2, no entanto, a estratégia de usar a criptografia RSA como ferramenta de fixar conteúdos por meio de uma abordagem mais atrativa foi apresentada como sugestão para ser trabalhada no ensino superior visto que, recorre ao campo da Teoria dos Números.

Todo o trabalho foi dividido em três capítulos e desenvolvido com um grupo de 20 alunos, que cursam 2° e 3° anos do ensino médio. A participação e o comprometimento dos alunos envolvidos foram fundamentais durante todo o processo.

# 1. CRIPTOGRAFIA INTUITIVA

O presente capítulo tem como agente motivador o despertar do interesse dos alunos por meio de uma atividade em que possam criar livremente modelos criptográficos, estimulando assim o raciocínio lógico, a liberdade do pensar e a capacidade de trabalhar em grupo.

Na maioria dos casos, a noção intuitiva de criptografia pode parecer natural aos educandos, visto que muitos já criaram códigos para trocarem mensagens secretas entre si ou até mesmo para anotarem informações sigilosas em seus blocos de notas e diários. Geralmente, estes códigos costumam ser representados por símbolos que representam letras. Dessa forma, o professor poderá se aproveitar dessa noção intuitiva para introduzir a noção desejada de criptografia e de seus elementos importantes, assim como mostrar a necessidade real da criação de um código seguro, com o objetivo de evitar a decodificação e leitura da mensagem por terceiros.

A atividade, visando todo o entendimento citado anteriormente, foi feita com uma amostra de 20 alunos, que cursam 2° e 3° anos do ensino médio, e que foram divididos em grupos. Cada um deles foi responsável pela criação de um modelo de criptografia e de enviar aos outros grupos, inimigos criptográficos, uma mensagem codificada. Assim, cada grupo teve a missão de criar um próprio sistema de codificação e de tentar decodificar a criação dos demais. O professor, nesse caso, atuou apenas como mediador do processo, um coadjuvante, deixando o papel de protagonista aos alunos. Atividades como esta, estimulam o raciocínio lógico, a liberdade do pensar e o cooperativismo em grupo.

Entende-se, portanto, que aulas ministradas de forma cooperativa deveriam estar presentes em todos os centros educacionais, não só na educação infantil, como são vistas com maior frequência, mas também no ensino fundamental e no ensino médio. Esse tipo de metodologia busca realizar trabalhos de forma coletiva para que os alunos desenvolvam determinadas habilidades sociais e tomem consciência da importância do esforço individual de cada um dos membros do grupo para alcançar os objetivos propostos. Além disso, ajudam a desenvolver autonomia e a promover a aprendizagem e o desenvolvimento coletivo da turma.

O professor Luís Carlos de Menezes, na revista digital Nova Escola de maio de 2009, afirma:

> “Para promover a autonomia, não bastam materiais didáticos e um professor protagonista. É preciso propor à classe atividades coletivas mais estruturadas do que as aulas expositivas, pois todos devem estar motivados e conscientes do sentido delas.
>
> Para isso, cabe ao professor atuar com seus colegas e com a coordenação pedagógica, aliás, com a mesma dinâmica que pretende propor em sala de aula. Além de se perguntar "de que forma a atividade em grupo melhora o ensino da minha disciplina?", é necessário formular outra: "De que forma minha disciplina pode promover nos grupos a aprendizagem cooperativa?" Sim, é possível também ter a disciplina a serviço dessa formação coletiva e não apenas o inverso. Com isso, tem-se o foco na aprendizagem e no desenvolvimento da turma, não somente no ensino de conteúdo”. (Menezes, 2009).

Há várias vantagens de aplicar o trabalho cooperativo nas salas de aula, entre as citadas, destacam-se o desenvolvimento da autonomia, a interação social e a aprendizagem coletiva. No entanto, devido às fortes exigências das matrizes curriculares e à rigidez das unidades didáticas com o cumprimento dos conteúdos, é comum deixar essa metodologia de lado por falta de tempo. Dessa maneira, a aprendizagem dos jovens torna-se limitada, pois veem sua educação restrita à assimilação de várias teorias desinteressantes cuja aplicabilidade na prática muitas vezes é desconhecida.

Logo, durante o processo de ensino e aprendizagem da Matemática, devem ser abordados assuntos do interesse do aluno, que estimulem a curiosidade e que permitam a construção de novos conhecimentos. Assuntos desconexos cujos educandos não enxerguem sua importância e aplicabilidade são desinteressantes e desestimulam a tentativa de adquirirem novos conhecimentos, pois dificilmente estão dispostos a buscar potencialidades meramente didáticas e dotadas de vários conteúdos que estão em descompasso com a realidade em que vivem.

A seguir, a próxima seção traz alguns dos resultados e conclusões mais relevantes conquistados com o desenrolar das atividades desenvolvidas em grupos com os alunos. A atividade foi batizada pelos próprios educandos com o nome: “Desenvolvendo modelos criptográficos de forma livre e intuitiva”. O nome escolhido,

por si só, já sugere que os alunos receberam estímulos de liberdade de criação e pensar, sendo assim, mostraram-se mais dispostos e atraídos para tal desafio.

### 1.1. Desenvolvendo modelos criptográficos de forma livre e intuitiva

Nesta seção, como já citado anteriormente, serão apresentadas as imagens das criptografias criadas de forma livre e intuitiva pelos grupos de alunos a fim de que as mesmas fossem descriptografadas por um grupo diferente daquele responsável pela elaboração da mensagem codificada.

A seguir, tem-se a imagem da primeira criptografia criada e apresentada por um dos grupos, na qual já é relatado o padrão de desenvolvimento do código e exemplificado o seu uso por meio de uma frase codificada e decodificada.

Figura 3: Criptografia 1 criada intuitivamente pelos alunos


Fonte: próprio autor

Mensagem codificada apresentada na imagem acima:

**L11 X10L4M3S7V23X7R13N3V24M12G7L4 V3 L4X8Z1N7R4M7S1L26**

**K3Z2I8Z21 Z1 O9R3Y7V6I8W1Z5W9V4**

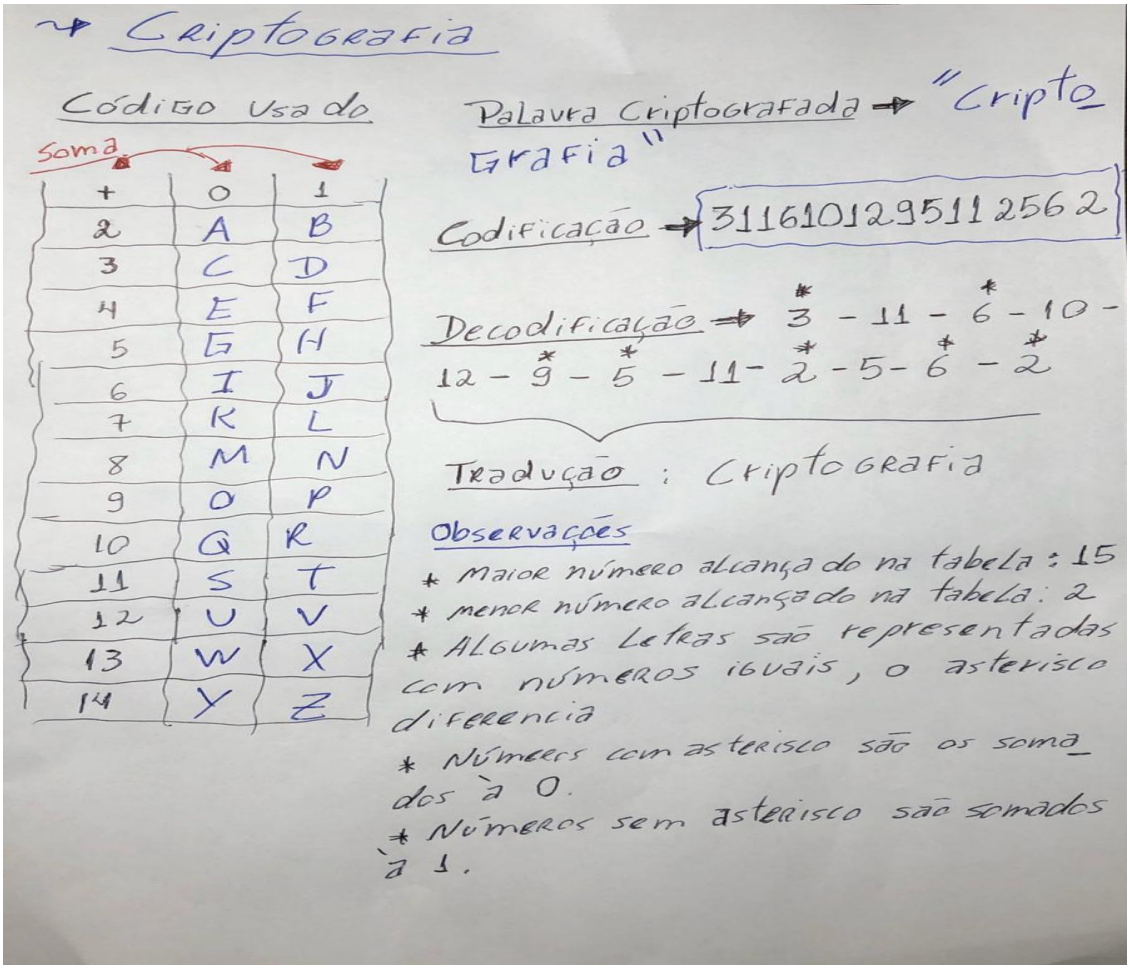
A mensagem foi criptografada transladando totalmente o alfabeto, ou seja, trocando a por z, b por y, c por w, e assim sucessivamente. Os números foram usados apenas com o efeito de confundir a tentativa de decodificar a mensagem pelos grupos inimigos. Assim, a mensagem decodificada na Língua Portuguesa corresponde a:

“O conhecimento é o caminho para a liberdade”

Os grupos adversários não conseguiram desvendar o segredo, já que a estratégia da inserção dos números apenas para confundir a decodificação surtiu efeito, segundo os próprios alunos. A mensagem só pôde ser decodificada após a revelação de como o processo de codificação foi feito, revelado pelo grupo criador.

Segue a imagem da próxima criptografia criada:

Figura 4: Criptografia 2 criada intuitivamente pelos alunos




Fonte: próprio autor

Mensagem codificada apresentada na figura anterior:

$$\mathbf{3116101295112562}$$

A codificação foi feita com base na tabela localizada na parte esquerda da imagem, em que a primeira coluna representa números de $2$ a $14$. Na segunda coluna, as letras de posição ímpar do alfabeto são representadas pelo mesmo valor localizado à esquerda da linha onde se encontram, ou seja, somando o valor de cada linha com $0$. Já na terceira coluna, as letras que ocupam as posições pares do alfabeto são representadas pelo número resultante da soma de $1$ com o valor localizado na mesma linha, à esquerda e na primeira coluna da tabela. Assim, o menor e o maior número alcançados pela tabela são $2$ e $15$, respectivamente.

Esse tipo de codificação apresentou um sério problema, pois várias letras diferentes poderiam ser representadas com números iguais, por exemplo: $B = 3 = 2 + 1$ e $C = 3 = 3 + 0$. Segundo relato dos alunos do grupo criador, essa foi a real intenção da criptografia proposta: não ser reversível de forma direta e o processo de decodificação ser feito sempre por meio de tentativas até se obter uma palavra com sentido na Língua Portuguesa.

Apresenta-se a seguir como foi feita a decodificação da mensagem, explicada pelo grupo de alunos aos demais:

A primeira etapa da decodificação consistiu em separá-los em blocos com números de um ou dois algarismos. Para isto, bastou lembrar que os números vão de $2$ a $15$, assim:

$$\mathbf{3116101295112562} = \mathbf{3} \parallel \mathbf{11} \parallel \mathbf{6} \parallel \mathbf{10} \parallel \mathbf{12} \parallel \mathbf{9} \parallel \mathbf{5} \parallel \mathbf{11} \parallel \mathbf{2} \parallel \mathbf{5} \parallel \mathbf{6} \parallel \mathbf{2}$$

A tabela, vista na figura $4$, sugeriu as seguintes possibilidades de decodificação:

$$2 = 2 + 0 = A;$$

$$3 = 2 + 1 = B \text{ ou } 3 = 3 + 0 = C;$$

$$4 = 3 + 1 = D \text{ ou } 4 = 4 + 0 = E;$$

$$5 = 4 + 1 = F \text{ ou } 5 = 5 + 0 = G;$$

$$6 = 5 + 1 = H \text{ ou } 6 = 6 + 0 = I;$$

$$7 = 6 + 1 = J \text{ ou } 7 = 7 + 0 = K;$$

$$8 = 7 + 1 = L \text{ ou } 8 = 8 + 0 = M;$$

$$9 = 8 + 1 = N \text{ ou } 9 = 9 + 0 = O;$$

$$10 = 9 + 1 = P \text{ ou } 10 = 10 + 0 = Q;$$

$$11 = 10 + 1 = R \text{ ou } 11 = 11 + 0 = S;$$

$$12 = 11 + 1 = T \text{ ou } 12 = 12 + 0 = U;$$

$$13 = 12 + 1 = V \text{ ou } 13 = 13 + 0 = W;$$

$$14 = 13 + 1 = X \text{ ou } 14 = 14 + 0 = Y;$$

e

$$15 = 14 + 1 = Z.$$

Ainda, na explicação de como foi feito o processo de decodificação mostrado na figura $4$ (à direita da imagem), também pôde ser notado o uso de asteriscos para diferenciar as letras obtidas pela soma do número com $0$ (usa-se o asterisco) das letras obtidas da soma do número com $1$ (sem o uso do asterisco), como segue:

$$\mathbf{3116101295112562} = *\mathbf{3} \parallel \mathbf{11} \parallel *\mathbf{6} \parallel \mathbf{10} \parallel \mathbf{12} \parallel *\mathbf{9} \parallel *\mathbf{5} \parallel \mathbf{11} \parallel *\mathbf{2} \parallel \mathbf{5} \parallel *\mathbf{6} \parallel *\mathbf{2}$$

Assim, a representação $*3$ indicou que o $3$ foi traduzido de $3 + 0 = C$ e a representação $11$ indicou que o mesmo veio da codificação $10 + 1 = R$. Dessa maneira, por meio de tentativas feita diante as várias dualidades possíveis no processo da decodificação, foi obtida a mensagem “CRIPTOGRAFIA”.

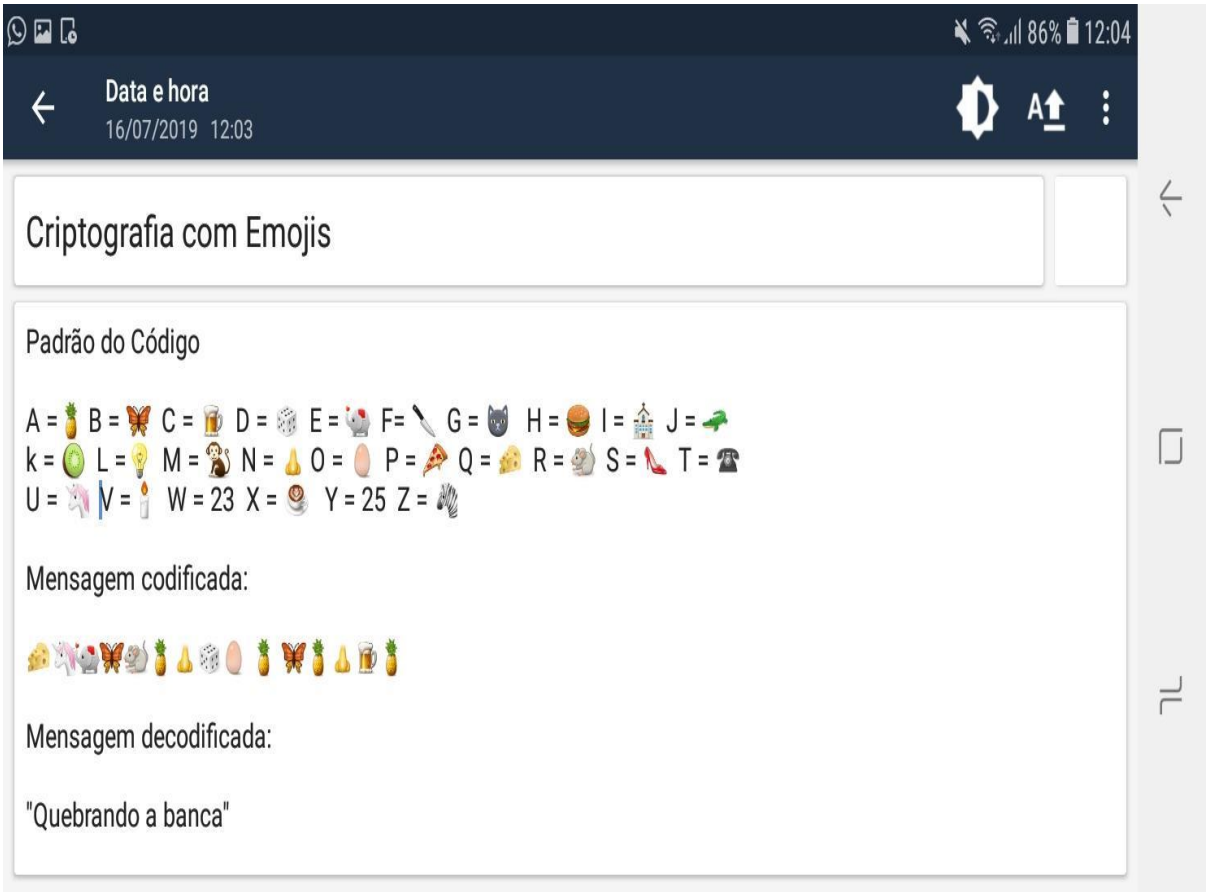
Durante a decodificação da mensagem feita e explicada pelos alunos do grupo criador, os mesmos foram abordados pelos outros grupos com a seguinte indagação: “E se durante a decodificação encontrarmos mais de uma palavra que faça sentido na língua portuguesa?”. A resposta do grupo responsável pela criação foi de que não se atentaram para tal fato, e que apenas buscaram criar algo mais difícil e seguro, evidenciando o motivo de terem usado as duplas possibilidades para o processo de decodificação da mensagem.

Como a mensagem não foi descriptografada por nenhum dos grupos, o professor, nesse caso, atuou ao término da explicação, com uma intervenção feita

ressaltando a importância de que um sistema criptográfico não gere ambiguidades durante o processo, ou seja, deve haver uma correspondência biunívoca de informações, em que cada mensagem criptografada retorne a sua mensagem original sem gerar dúvidas. O mesmo se aplica a cada mensagem original que deve ser particular no processo de codificação, fato este, não ocorrido na codificação apresentada. O conceito de correspondência biunívoca remete ao estudo de funções e será mais explorado no próximo capítulo.

A próxima imagem mostrada, feita por outro grupo, apresentou um modelo de criptografia mais simples e fácil de ser quebrado.

Figura 5: Criptografia 3 criada intuitivamente pelos alunos




Fonte: Próprio autor

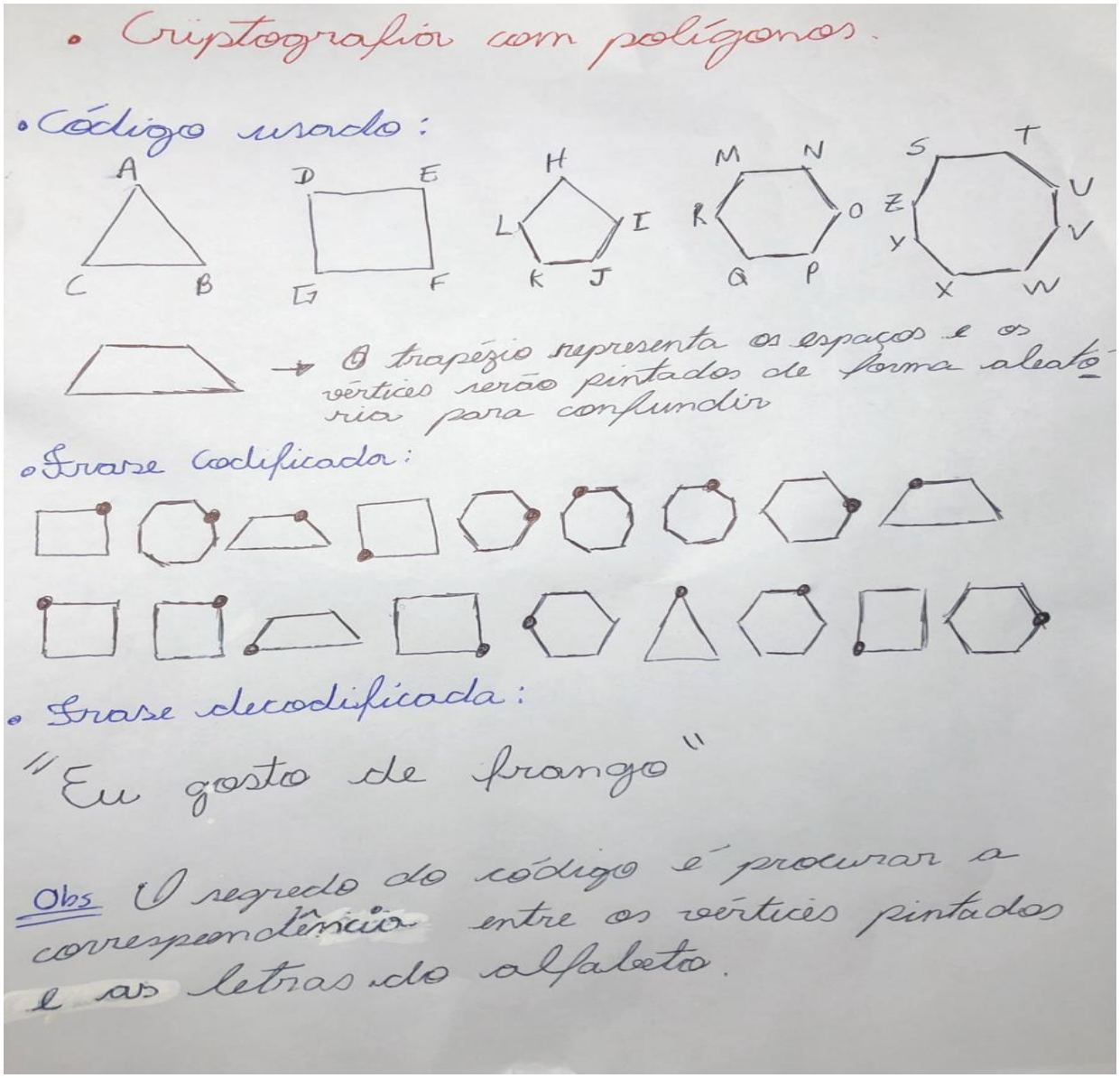
Neste modelo de codificação, mostrado na figura 5, foram usadas representações denominadas “emojis”, encontradas facilmente nos aplicativos dos aparelhos celulares dos alunos, como por exemplo o WhatsApp. Para a realização da criptografia, os alunos aproveitaram as letras iniciais das palavras que eram associadas ao significado da imagem de cada uma das figuras escolhidas. Nesse

caso, ao criar o código, o grupo apresentou dificuldades em encontrar tais associações para representar as letras W e Y, e acabaram representando-as pelos números correspondentes as posições as letras ocupam no alfabeto, ou seja, W assumiu o símbolo 23 e Y o símbolo 25.

Por fim, o grupo que usou a estratégia dos “emojis” percebeu que seu código foi facilmente quebrado pelos demais grupos e concluiu que ao menos poderia ter transladado sua codificação para confundir e tornar o padrão criado mais seguro, ou seja, poderia ter usado estratégia semelhante à usada no Código de César.

Segue a última imagem de criptografia intuitiva criada em sala de aula:

Figura 6: Criptografia 4 criada intuitivamente pelos alunos




Fonte: próprio autor

A imagem apresentada na figura anterior mostra a criação de um modelo de criptografia interessante, usando polígonos na sua codificação. Neste modelo criptográfico, ao criar a codificação feita por meio de polígonos, o grupo autor distribuiu as vinte e seis letras do alfabeto em cinco polígonos, da seguinte maneira: um triângulo cujos vértices indicaram $A, B$ e $C$; um quadrado indicando $D, E, F$ e $G$; um pentágono com $H, I, J, K$ e $L$; um hexágono com $M, N, O, P, Q$ e $R$; e por fim, um octógono representando as letras finais $S, T, U, V, W, X, Y$ e $Z$. As letras em cada vértice dos polígonos foram ordenadas de acordo com o alfabeto e no sentido horário, sempre com início no vértice superior do polígono, em que polígonos com dois vértices superiores, a representação ordenada das letras começou no vértice superior esquerdo, casos do quadrado, hexágono e do octógono.

É importante notar também, que no processo de codificação da mensagem, apenas o vértice cuja letra será usada na mensagem é pintado e que ao usar o trapézio, um de seus vértices também é pintado de forma aleatória, apenas com o intuito de confundir, visto que tal polígono será usado apenas para representar os espaços da mensagem no processo de decodificação.

Os grupos adversários tentaram sem sucesso decifrar a mensagem, até procuraram relacionar o polígono e os vértices pintados na figura com a tabela de frequências das letras na Língua Portuguesa, tabela 1 vista anteriormente. No entanto, não obtiveram sucesso na tentativa, visto que a mensagem codificada “EU GOSTO DE FRANGO” possui apenas um caractere A, e na maioria das vezes, as tentativas de quebrar o código baseiam-se na frequência específica desse caractere, já que trata-se da representação de letra de maior incidência na nossa língua (ver na tabela 1). O grupo criador da codificação garantiu que a frase foi escolhida tomando justamente o cuidado de evitar a maior frequência do caractere A.

A frase codificada só foi descoberta pelos demais grupos após ser revelada a estratégia de como foi feita a codificação, chamada pelos alunos de “segredo”, sendo de comum acordo dos demais alunos a aceitação de que dificilmente conseguiriam decodificar a mensagem sem o conhecimento de como o processo de codificação foi feito. Nesse momento, houve a intervenção do professor ressaltando a importância de que na criptografia, o receptor de desejo do emissor detenha a chave de decodificação, ou seja, o “segredo”.

## 1.2. Resultados obtidos durante a atividade

No decorrer da atividade, os alunos perceberam que quanto mais aleatório e criativo era o código criado, mais difícil se tornava a sua decodificação e leitura, e quanto maior era a mensagem escrita, mais símbolos eles conseguiam associar às letras e números, criando uma noção intuitiva da análise de frequência das letras nas palavras na Língua Portuguesa, mostradas na tabela 1.

Houve também muito interesse e empenho por parte dos alunos. O trabalho feito de forma coletiva, com liberdade de criar as estratégias de codificação e a ideia de desafiar os grupos adversários, certamente foram fundamentais para a harmonização, sucesso e o envolvimento de todos durante a atividade.

Ao fim, os grupos concluíram que se não possuíssem a chave de decodificação, dificilmente desvendariam uma mensagem codificada, a menos que o padrão fosse muito simples e fácil de ser quebrado, ou seja, apenas se conseguissem saber como o código foi pensado.

Partindo dessa percepção, houve uma intervenção do professor com a seguinte indagação: “E se esse segredo do código fosse uma função afim?”. Vários alunos assimilaram um pouco a ideia e se mostraram curiosos. Nesse caso, o professor aproveitou para destacar que esse será o verdadeiro motivo desse trabalho, isto é, usar a criptografia para trabalhar em sala de aula conteúdos matemáticos presentes nas matrizes curriculares de forma mais atrativa.

As atividades desenvolvidas neste capítulo foram realizadas no contraturno das aulas dos alunos, no período vespertino, com duração de aproximadamente 7 aulas de 50 min, realizadas em três tardes.

# 2. CRIPTOGRAFIA COM FUNÇÕES AFINS E MATRIZES

Neste capítulo, a criptografia será abordada como uma ferramenta capaz de ser usada como instrumento para a fixação de conteúdos matemáticos importantes. A abordagem será levada para o campo das funções afins e das matrizes, e feita considerando que o aluno já tenha adquirido o conhecimento prévio necessário e domine as operações que fazem parte da matriz curricular de tais assuntos no ensino médio. Desta maneira, a criptografia não será usada com o intuito de que o aluno aprenda função afim e matriz, mas sim com o objetivo de fixar os conteúdos de uma maneira alternativa e menos enfadonha. As atividades propostas foram inspiradas nas ideias de Tamarozzi (2001).

Segundo Tamarozzi, a criptografia, desde o seu surgimento, mantém o mesmo princípio básico: encontrar uma transformação (função) injetiva $f$ entre um conjunto de mensagens escritas em um determinado alfabeto (de letras, números ou outros símbolos) para um conjunto de mensagens codificadas. O fato de $f$ ser inversível, ou seja, necessariamente uma relação bijetiva, é a garantia de que o processo seja reversível e de que as mensagens possam ser reveladas pelos receptores. Assim sendo, o grande desafio de um processo criptográfico desse modelo está em ocultar eficientemente os mecanismos (chaves) para a inversão de $f$, de modo que estranhos não possam fazê-lo. O processo criptográfico descrito, com analogia as funções, pode ser mais bem visualizado pelo esquema a seguir:

$$\boxed{\textbf{Mensagem Original}} \xrightarrow{f} \boxed{\textbf{Mensagem Codificada}} \xrightarrow{f^{-1}} \boxed{\textbf{Mensagem Original}}$$

A tarefa de enviar a mensagem original codificada cabe ao emissor, por meio de $f$. Já ao receptor da mensagem, fica a missão de decodificar a mensagem transformando-a na mensagem original, por meio de $f^{-1}$(inversa da função $f$).

As atividades e os exemplos mostrados a seguir tiveram como foco principal mostrar como codificar e decodificar mensagens usando matrizes e funções afins, cujos conceitos já aplicados em sala de aula foram novamente explorados com os alunos, principalmente no que diz respeito a determinar a inversa tanto de uma função afim como de uma matriz quadrada. Com isso, o principal objetivo desse capítulo

concentrou-se apenas na finalidade didática de fixar conteúdos, visto que a quebra de uma criptografia usando como chave de decodificação uma função inversa é simples de ser feita, e também, pela inconveniência de existirem trocas prévias de chaves de decodificação (funções e matrizes) pelos usuários.

O processo de codificação das mensagens, usando funções afins e matrizes, foi feito mediante uma pré-codificação, ou seja, primeiramente as letras da mensagem criptografada foram transformadas em números, conforme indicam as correspondências alfabeto-numéricas da tabela abaixo:

Tabela 2 - Pré-codificação das mensagens

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

Fonte: próprio autor

O número $0$ mostrado na tabela foi associado aos espaços em branco das frases a serem criptografadas.

A atividade também poderia ter sido feita usando outros tipos de funções inversíveis, tais como: as funções exponenciais, logarítmicas e quadráticas. Sendo assim, tal fato ainda poderia contribuir com a importante finalidade didática de mostrar que a função logarítmica é a inversa da função exponencial e vice-versa. Como o tempo para se trabalhar os conteúdos nas unidades didáticas é relativamente curto, trabalhar tais funções mencionadas anteriormente fica apenas como sugestão, visto que não serão exploradas neste trabalho.

## 2.1. Trabalhando criptografia com função afim

As atividades propostas nessa seção se condicionaram ao aprimoramento do estudo de funções afins com coeficientes inteiros, ou seja, funções do tipo $f(x) = ax + b$, com $a$, $b$ inteiros, $a \neq 0$, definidas no conjunto $\{0, 1, 2, 3, 4, 5, \dots, 26\}$ devido as correspondências presentes na tabela $2$. Nada impede o uso de coeficientes reais, no entanto, a escolha dos inteiros foi feita para facilitar o dinamismo e o entendimento

dos alunos. Tal fato ficou evidenciado imediatamente no exemplo instrutivo que será mostrado a seguir e que foi apresentado em sala de aula pelo docente, servindo assim, de modelo para que os alunos pudessem resolver de forma autônoma os exercícios que foram propostos posteriormente na seção 2.3 pelo professor.

**Exemplo instrutivo apresentado:** A frase **EU AMO MATEMÁTICA** de acordo com a tabela 2 será pré-codificada como

**5 21 0 1 13 15 0 13 1 20 5 13 1 20 9 3 1**

Note que, ao pré-codificar essa mensagem, se não fossem usados espaços entre cada um dos números, seriam criados problemas de entendimento, ou seja, a mensagem numérica **52101131501312051312093 1** escrita sem espaços geraria problemas de ambiguidade. Por exemplo, o número 113 poderia ser interpretado como 1 e 13, ou como 11 e 3, ou ainda como 1, 1 e 3. Nesse caso não seria possível saber ao certo quais números seriam levados até a função cifradora para concluir o processo de codificação da mensagem, o que também traria problemas no processo de decodificação. Esse problema poderia ser sanado se fosse usada a seguinte tabela:

Tabela 3 – Nova pré-codificação das mensagens

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

Fonte: próprio autor

Assim, as funções do tipo $f(x) = ax + b$, com $a$, $b$ inteiros, $a \neq 0$, passariam a ser definidas no conjunto $\{10, 11, 12, 13, 14, 15, \ldots, 36\}$, e a utilização dos números de dois algarismos para representar cada uma das letras do nosso alfabeto sanaria o problema de gerar ambiguidades, visto que mesmo não utilizando espaços na mensagem pré-codificada, seria possível prever que cada número de dois algarismos surgiu da substituição de uma letra do alfabeto conforme indica a tabela 3.

Para facilitar todo o processo e gerar mais dinamismo durante as atividades, os exercícios de fixação dos conteúdos, propostos na seção 2.3, foram resolvidos pelos alunos mediante a incorporação dos dados da tabela 2. Assim, a tabela 2 foi utilizada tanto para pré-codificação das mensagens no estudo das funções afins desta

seção, como também para o mesmo estudo envolvendo matrizes, que será visto na seção 2.2, ou seja, a mensagem pré-codificada pelo emissor foi sempre levada até o receptor contendo espaços entre cada letra. O professor aproveitou aqui para chamar esse tipo de sistema de “Criptografia em blocos”, cujos espaços citados serão usados como separação de cada um dos blocos a serem codificados.

Nesse caso, admitindo que a função cifradora seja dada por $f(x) = 3x + 1$. Aplicando bloco a bloco da mensagem fornecida no exemplo instrutivo na função cifradora e organizando os resultados em uma tabela, tem-se:

Tabela 4 – Codificação da mensagem

| $x$ | $f(x) = 3 \cdot x + 1$ | $x$ | $f(x) = 3 \cdot x + 1$ |
|---|---|---|---|
| 5 | $f(5) = 3 \cdot 5 + 1 = 16$ | 20 | $f(20) = 3 \cdot 20 + 1 = 61$ |
| 21 | $f(21) = 3 \cdot 21 + 1 = 64$ | 5 | $f(5) = 16$ |
| 0 | $f(0) = 3 \cdot 0 + 1 = 1$ | 13 | $f(13) = 40$ |
| 1 | $f(1) = 3 \cdot 1 + 1 = 4$ | 1 | $f(1) = 4$ |
| 13 | $f(13) = 3 \cdot 13 + 1 = 40$ | 20 | $f(20) = 61$ |
| 15 | $f(15) = 3 \cdot 15 + 1 = 46$ | 9 | $f(9) = 3 \cdot 9 + 1 = 28$ |
| 0 | $f(0) = 1$ | 3 | $f(3) = 3 \cdot 3 + 1 = 10$ |
| 13 | $f(13) = 40$ | 1 | $f(1) = 4$ |
| 1 | $f(1) = 4$ | _ | _____ |

Fonte: próprio autor

A mensagem codificada enviada pelo emissor seria:

$$\mathbf{16\ 64\ 1\ 4\ 40\ 46\ 1\ 40\ 4\ 61\ 16\ 40\ 4\ 61\ 28\ 10\ 4}$$

O receptor que detém a função cifradora $f(x) = 3x + 1$, e agora de posse da mensagem criptografada, precisa encontrar a chave para decodificá-la. Para isso, basta que encontre a inversa da função $f$, ou seja, encontrar $f^{-1}$, capaz de transformar a mensagem codificada na mensagem original. Antes disso, no entanto, será feita uma retomada da definição de função inversa e de uma maneira prática de obtê-la.

**Função Inversa**

**Definição:** Dada a função $f: A \to B$, chama-se função inversa de $f$, indicada por $f^{-1}(x)$, a função $f^{-1}: B \to A$ que associa cada elemento $y$ pertencente ao conjunto $B$ a um elemento $x$ pertencente ao conjunto $A$, tal que $y = f(x)$. Atrelada a esta definição

não pode ser esquecido o fato de que apenas as funções bijetoras admitem função inversa.

**Regra Prática para obtenção de uma Função Inversa:**

$i)$ Substituir $f(x)$ ou a função que está sendo representada por $y$.

$ii)$ Trocar $x$ por $y$ e $y$ por $x$.

$iii)$ "Isolar" $y$ para representá-lo como função de $x$.

$iv)$ Substituir $y$ pela representação $f^{-1}(x)$.

De acordo com a definição e aplicando a regra prática citada na função cifradora $f(x) = 3x + 1$, segue que:

$$i)\ y = 3x + 1.$$

$$ii)\ x = 3y + 1.$$

$$iii)\ x = 3y + 1 \Leftrightarrow 3y = x - 1 \Leftrightarrow\ y = \frac{x-1}{3}.$$

$$iv)\ f^{-1}(x) = \frac{x-1}{3}.$$

Assim, calculando as imagens de $f^{-1}(x) = \frac{x-1}{3}$ (inversa da função cifradora) referentes às mensagens em blocos enviadas pelo emissor, tem-se a tabela:

Tabela 5 – Decodificação da mensagem

| $x$ | $f^{-1}(x) = (x-1) \div 3$ | $x$ | $f^{-1}(x) = (x-1) \div 3$ |
|---|---|---|---|
| 16 | $f^{-1}(16) = (16-1) \div 3 = 5$ | 61 | $f^{-1}(61) = (61-1) \div 3 = 20$ |
| 64 | $f^{-1}(64) = (64-1) \div 3 = 21$ | 16 | $f^{-1}(16) = 5$ |
| 1 | $f^{-1}(1) = (1-1) \div 3 = 0$ | 40 | $f^{-1}(40) = 13$ |
| 4 | $f^{-1}(4) = (4-1) \div 3 = 1$ | 4 | $f^{-1}(4) = 1$ |
| 40 | $f^{-1}(40) = (40-1) \div 3 = 13$ | 61 | $f^{-1}(61) = 20$ |
| 46 | $f^{-1}(46) = (46-1) \div 3 = 15$ | 28 | $f^{-1}(28) = (28-1) \div 3 = 9$ |
| 1 | $f^{-1}(1) = 0$ | 10 | $f^{-1}(10) = (10-1) \div 3 = 3$ |
| 40 | $f^{-1}(40) = 13$ | 4 | $f^{-1}(4) = 1$ |
| 4 | $f^{-1}(4) = 1$ | _ | _____ |

Fonte: próprio autor

Logo, com as imagens de $f^{-1}(x)$ o receptor encontra

$$\mathbf{5\ 21\ 0\ 1\ 13\ 15\ 0\ 13\ 1\ 20\ 5\ 13\ 1\ 20\ 9\ 3\ 1},$$

e utilizando a correspondência alfabeto-numérica (tabela 2), obtém a mensagem original **EU AMO MATEMÁTICA**.

Um aspecto interessante, e que também poderia ser abordado com os alunos, é supor que o receptor tenha perdido a chave ou que a mensagem tenha sido interceptada; se o estranho souber que a mensagem foi codificada utilizando-se uma função afim inversa, fica fácil quebrar o código, já que seriam necessárias apenas duas associações corretas para determinar a lei de formação da função afim. O desafio de encontrar tais associações poderia ser resolvido por meio da análise de frequências, que também fica como sugestão a ser usada pelo docente como estratégia de fixar conteúdos relacionados ao ramo da estatística.

## 2.2. Trabalhando criptografia com matriz

No que diz respeito ao processo atual do estudo de matrizes, usado nas escolas, podemos dizer que este se caracteriza pela repetição de exercícios pouco motivadores para os alunos. O ensino de matrizes apresenta-se de forma desconexa com o seu real emprego e importância nos avanços tecnológicos.

A seguir, ao ser abordada uma maneira de codificar mensagens usando matrizes, o processo acaba sendo útil para o aprimoramento de alguns pontos importantes e que estão presentes nas atuais estruturas curriculares deste conteúdo, tais como: a multiplicação e a inversão de matrizes. Desta forma, usando criptografia no estudo de tais conceitos, o aluno poderá se sentir mais atraído, enxergando utilidade em seu estudo, visto que atualmente a criptografia é amplamente utilizada e que nesse momento do trabalho tal fato já é de conhecimento dos alunos. O processo, em relação à criptografia com funções afins, ganha um pouco mais de complexidade ao se codificar e decodificar uma mensagem, no entanto, também possui o mesmo caráter, apenas instrutivo, usado como instrumento para motivar o interesse dos discentes e também como estratégia de fixar conteúdo.

Primeiramente é preciso escolher uma matriz codificadora, sendo necessariamente uma matriz quadrada e inversível, pois sua inversa será posteriormente usada como a matriz decodificadora da mensagem. A seguir, será apresentado como modelo instrutivo e para facilitar a compreensão dos alunos, um exemplo de como todo o procedimento é feito usando uma matriz quadrada de ordem $2$. Os exemplos e exercícios podem ser estendidos ao estudo de matrizes quadradas de ordens superiores a $2$, no entanto, a utilização de tal ordem é feita aqui com o intuito de dinamizar as aulas e facilitar o primeiro contato dos alunos com o assunto.

Assim como foi dito no estudo da criptografia com funções afins, as atividades desta seção partem do pressuposto de que o aluno já tenha o conhecimento prévio necessário dos conceitos que serão usados (multiplicação e inversão de matrizes). No entanto, antes da apresentação do exemplo instrutivo será feita uma breve retomada de tais conceitos. Tal retomada será feita de forma bastante sucinta e levando em conta que alguns conhecimentos a respeito de matrizes já sejam do entendimento do leitor (definição de matriz, ordem, tipos de matriz, propriedades relativas a matrizes inversas, determinantes, ...).

**Inversão de Matrizes**

**Definição:** Dadas duas matrizes quadradas $A$ e $B$, de ordem $n$, a matriz $B$ será a inversa da matriz $A$ se, e somente se, $A \cdot B = B \cdot A = I_n$, em que $I_n$ é a matriz identidade de ordem $n$. A matriz B, inversa da matriz $A$, será representada por $A^{-1}$. Assim, podemos escrever $A \cdot A^{-1} = A^{-1} \cdot A = I_n$. Atrelada a esta definição também é importante lembrar que uma determinada matriz quadrada $A$ só é inversível se, e somente se, $\det A \neq 0$.

**Multiplicação de Matrizes**

**Definição:** Dadas as matrizes $A = (a_{ij})_{m \times p}$ e $B = (b_{ij})_{p \times n}$ , o produto das matrizes $A = (a_{ij})_{m \times p}$ e $B = (b_{ij})_{p \times n}$ é a matriz $C = (c_{ij})_{m \times n}$, em que cada elemento $c_{ij}$ é obtido por meio da soma dos produtos dos elementos correspondentes da $i$-ésima linha de $A$ pelos elementos da $j$-ésima coluna de $B$. Da definição, temos que a matriz produto $C = A \cdot B$ só existe se o

número de colunas de $A$ for igual ao número de linhas de $B$, o que já evidencia um fato relevante no estudo de matrizes: a multiplicação de matrizes não é comutativa.

A seguir, será apresentado o exemplo, de criptografia trabalhada com matrizes, que foi explicado pelo professor em sala de aula, exemplo este, feito com o intuito de que os alunos pudessem compreender e aplicar o conhecimento assimilado nos exercícios propostos na seção 2.3, e também fixar de maneira satisfatória conceitos importantes como a inversão e multiplicação de matrizes.

**Exemplo instrutivo apresentado:** Seja a matriz $A = \begin{bmatrix} 2 & 1 \\ 2 & 3 \end{bmatrix}$, a matriz codificadora. Note que, $\det A = 4$, sendo assim, como já faz parte do conhecimento do aluno, $A$ é uma matriz inversível. No processo, é fundamental obter a inversa da matriz $A$. Sendo assim, tomando $A^{-1} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ como a matriz inversa a ser encontrada, decorre da definição que

$$A \cdot A^{-1} = I_n \Leftrightarrow$$

$$\Leftrightarrow \begin{bmatrix} 2 & 1 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} 2x + z & 2y + w \\ 2x + 3z & 2y + 3w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\Leftrightarrow \begin{cases} 2x + z = 1 \\ 2x + 3z = 0 \\ 2y + w = 0 \\ 2y + 3w = 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = {}^{3}/_{4} \\ y = {}^{-1}/_{4} \\ z = {}^{-1}/_{2} \\ w = {}^{1}/_{2} \end{cases}.$$

Assim,

$$A^{-1} = \begin{bmatrix} {}^{3}/_{4} & {}^{-1}/_{4} \\ {}^{-1}/_{2} & {}^{1}/_{2} \end{bmatrix}$$

é a inversa da matriz $A$.

Usando a mesma mensagem que foi trabalhada com função afim, ou seja, **EU AMO MATEMÁTICA**, e também a correspondência afabeto-numérica da tabela 2, conclui-se que sua pré-codificação em blocos, é dada por

$$\mathbf{5\ 21\ 0\ 1\ 13\ 15\ 0\ 13\ 1\ 20\ 5\ 13\ 1\ 20\ 9\ 3\ 1}$$

A matriz $M$, a ser criptografada será dada por

$$M = \begin{bmatrix} 5 & 21 & 0 & 1 & 13 & 15 & 0 & 13 & 1 \\ 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 & 0 \end{bmatrix},$$

cujos blocos foram dispostos ordenadamente, da esquerda para a direita, em duas linhas. Note que a mensagem, pré-codificada em blocos, indica um número ímpar de caracteres (letras e espaços) correspondentes a mensagem original, desse modo o $0$ foi usado de forma estratégica como último bloco tornando par o número de caracteres e preenchendo a sobra (último campo da segunda linha da matriz $M$), visto que $0$ representa o espaço em branco na correspondência da tabela $2$ e não alterará o significado da mensagem no momento da decodificação.

A matriz $B$ fornecida ao receptor, será dada por $B = A \cdot M$, daí o fato da matriz $M$ ser disposta em duas linhas, possibilitar a multiplicação de matrizes de acordo com a definição. Dessa maneira, usando a definição de multiplicação de matrizes, tem-se:

$$B = \begin{bmatrix} 2 & 1 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 5 & 21 & 0 & 1 & 13 & 15 & 0 & 13 & 1 \\ 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 10+20 & 42+5 & 0+13 & 2+1 & 26+20 & 30+9 & 0+3 & 26+1 & 2+0 \\ 10+60 & 42+15 & 0+39 & 2+3 & 26+60 & 30+27 & 0+9 & 26+3 & 2+0 \end{bmatrix}$$

$$= \begin{bmatrix} 30 & 47 & 13 & 3 & 46 & 39 & 3 & 27 & 2 \\ 70 & 57 & 39 & 5 & 86 & 57 & 9 & 29 & 2 \end{bmatrix}$$

Logo,

$$B = \begin{bmatrix} 30 & 47 & 13 & 3 & 46 & 39 & 3 & 27 & 2 \\ 70 & 57 & 39 & 5 & 86 & 57 & 9 & 29 & 2 \end{bmatrix}.$$

A matriz $B$, gerou uma mensagem que será disposta ordenadamente tomando os elementos da primeira linha escritos da esquerda para a direita, e posteriormente, fazendo o mesmo com a segunda linha. Dessa maneira, a mensagem equivale a sequência numérica:

$$\mathbf{30\ 47\ 13\ 3\ 46\ 39\ 3\ 27\ 2\ 70\ 57\ 39\ 5\ 86\ 57\ 9\ 29\ 2}$$

Para que o receptor consiga traduzir a mensagem recebida, deverá voltar a matriz $M$ usando a inversa de $A$ pela relação $M = A^{-1} \cdot B$. Note que, a relação apresentada para voltar a matriz $M$ pode ser deduzida pelo professor enfatizando algumas propriedades, válidas e de conhecimento do aluno, relativas as matrizes inversas. Neste caso, segue uma dedução análoga a feita pelo professor em sala de aula:

$$B = A \cdot M \Leftrightarrow$$

$$\Leftrightarrow A^{-1} \cdot B = A^{-1} \cdot A \cdot M$$

$$\Leftrightarrow A^{-1} \cdot B = I_n \cdot M$$

$$\Leftrightarrow I_n \cdot M = A^{-1} \cdot B$$

$$\Leftrightarrow M = A^{-1} \cdot B.$$

Agora, calculando $M$, obtém-se:

$$A^{-1} \cdot B = \begin{bmatrix} 3/4 & -1/4 \\ -1/2 & 1/2 \end{bmatrix} \cdot \begin{bmatrix} 30 & 47 & 13 & 3 & 46 & 39 & 3 & 27 & 2 \\ 70 & 57 & 39 & 5 & 86 & 57 & 9 & 29 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 21 & 0 & 1 & 13 & 15 & 0 & 13 & 1 \\ 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 & 0 \end{bmatrix} = M.$$

Os elementos da matriz $M$, como descrito anteriormente, foram preenchidos pela sequência

$$\mathbf{5\ 21\ 0\ 1\ 13\ 15\ 0\ 13\ 1\ 20\ 5\ 13\ 1\ 20\ 9\ 3\ 1,}$$

correspondente a mensagem **EU AMO MATEMÁTICA** pré-codificada pela tabela 2. Assim, concluiu-se o modelo de criptografia com matrizes apresentado em sala de aula.

## 2.3. Atividades desenvolvidas em grupos

As atividades desta seção, tiveram como objetivo principal a utilização da criptografia como ferramenta de fixação de conteúdos importantes presentes nas matrizes curriculares do ensino médio dos mais variados centro educacionais, no caso

desta atividade, funções afins e matrizes. Todas as atividades foram desenvolvidas tomando como referência a pré-codificação da tabela 2, vista no capítulo anterior. Também foi considerado o fato de que o aluno já havia adquirido, em aulas anteriores, o embasamento necessário para o desenvolvimento de conceitos, relacionados a funções afins e a matrizes, necessários no desenvolvimento dos exercícios.

É de suma importância frisar, que as atividades propostas a seguir, só foram concretizadas pelos educandos após a abordagem didática feita pelo docente dos exemplos mostrados nas seções 2.1 e 2.2.

**Atividades propostas para serem trabalhadas em grupos**

**01**. Dado o código

$$35 \quad 27 \quad 39 \quad -3 \quad 5 \quad 7 \quad -3 \quad 9 \quad 7 \quad 41 \quad 7 \quad 33 \quad 7 \quad 15 \quad 33 \quad 27$$

gerado pela função cifradora $f(x) = 2x - 3$, decodifique a mensagem usando a chave secreta, ou seja, usando a função inversa de $f$.

**02.** Discuta e crie, com o seu grupo, uma mensagem pré-codificada pela tabela 2 e a codifique por meio de uma função afim. Envie a mensagem criada a um inimigo criptográfico (outro grupo) e peça que tente descobrir a mensagem original. Após certo tempo, caso o inimigo não tenha descoberto a mensagem, forneça a função cifradora criada pelo seu grupo para que decodifique a mensagem por meio da função inversa (chave de decodificação).

**03.** A mensagem

$$37\ 7\ 39\ 9\ 31\ 33\ 17\ 25\ 43\ 9\ 45\ 7\ 17\ 7\ 13\ 9\ 33\ 39\ 17\ 9\ 37\ 7\ 33\ 49\ 35\ 15\ 25\ 9\ 31$$

foi codificada usando uma função afim e a pré-codificação da tabela 2. Descubra qual é a mensagem por trás da mensagem codificada.

Sugestão: a função cifradora pode ser descoberta por meio da análise de frequência das letras na Língua Portuguesa, mostrada na tabela 1 do capítulo 1.

**04.** Considerando a mensagem “BEBA ÁGUA” e a matriz codificadora

$$A = \begin{bmatrix} 6 & 1 \\ 5 & 2 \end{bmatrix},$$

determine o que se pede:

**a)** Pré-codifique a mensagem “BEBA ÁGUA”, usando a tabela $2$, encontrando a matriz $M$ a ser criptografada;

**b)** Determine a matriz $B$ por meio da ralação $A \cdot M$ e escreva a mensagem criptografada obtida;

**c)** Encontre $A^{-1}$, ou seja, a inversa da matriz $A$;

**d)** Calcule $A^{-1} \cdot B$;

**e)** O que se pode concluir a respeito da matriz encontrada no item anterior?

**05.** Decodifique a mensagem

$$68\ \ 84\ \ 20\ \ 8\ \ 72\ \ 4\ \ 56\ \ 16\ \ 60\ \ 17\ \ 24\ \ 5\ \ 8\ \ 21\ \ 43\ \ 23\ \ 7\ \ 15,$$

criptografada por meio da matriz codificadora

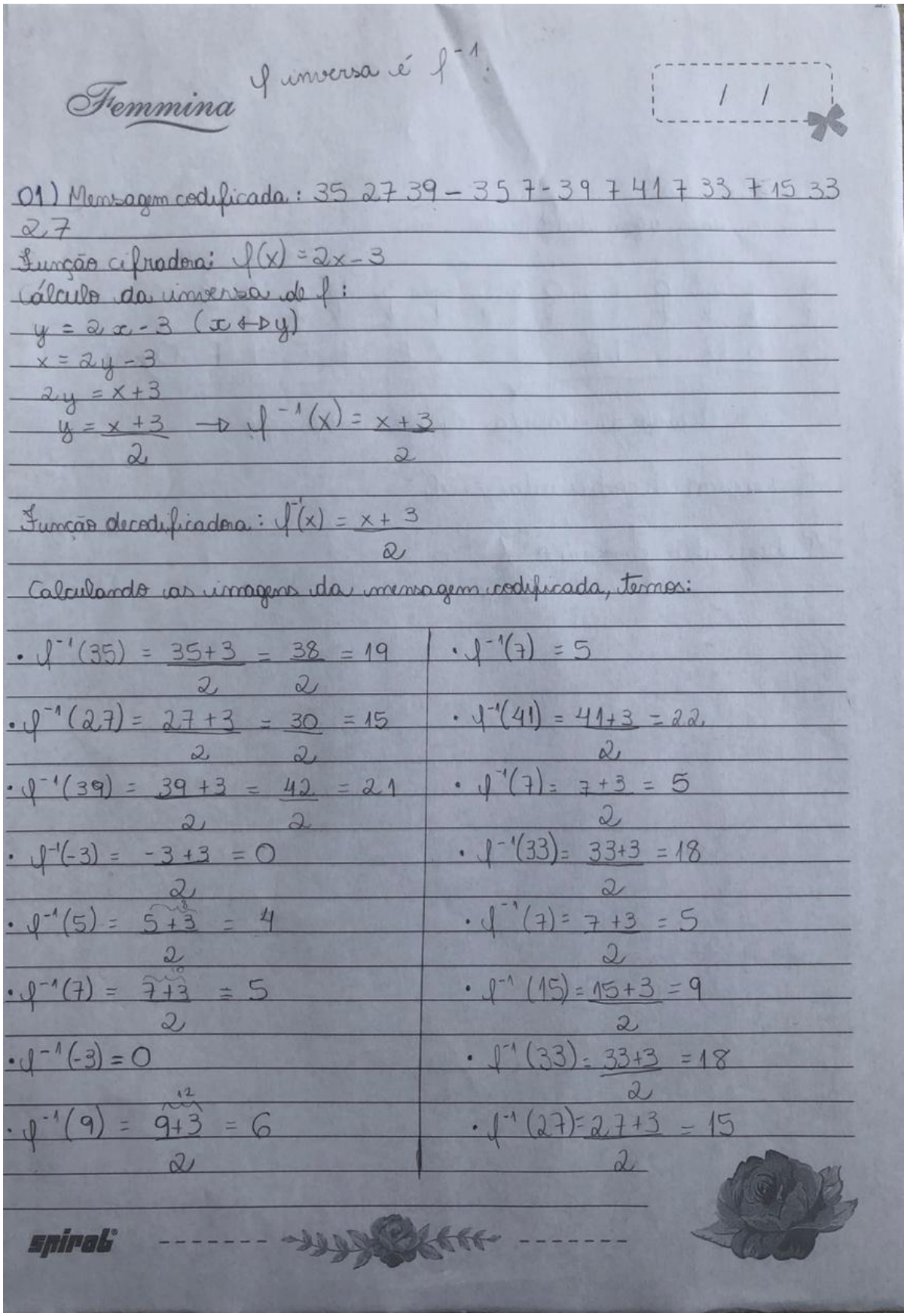
$$A = \begin{bmatrix} 4 & 0 \\ 1 & 3 \end{bmatrix}.$$

**06.** Crie e criptografe, em grupo, uma mensagem usando matriz, envie a mensagem e a matriz codificadora aos outros grupos com o intuito de que descubram a sua mensagem original por meio do processo de decodificação envolvendo matrizes inversas.

## 2.4. Soluções desenvolvidas pelos grupos

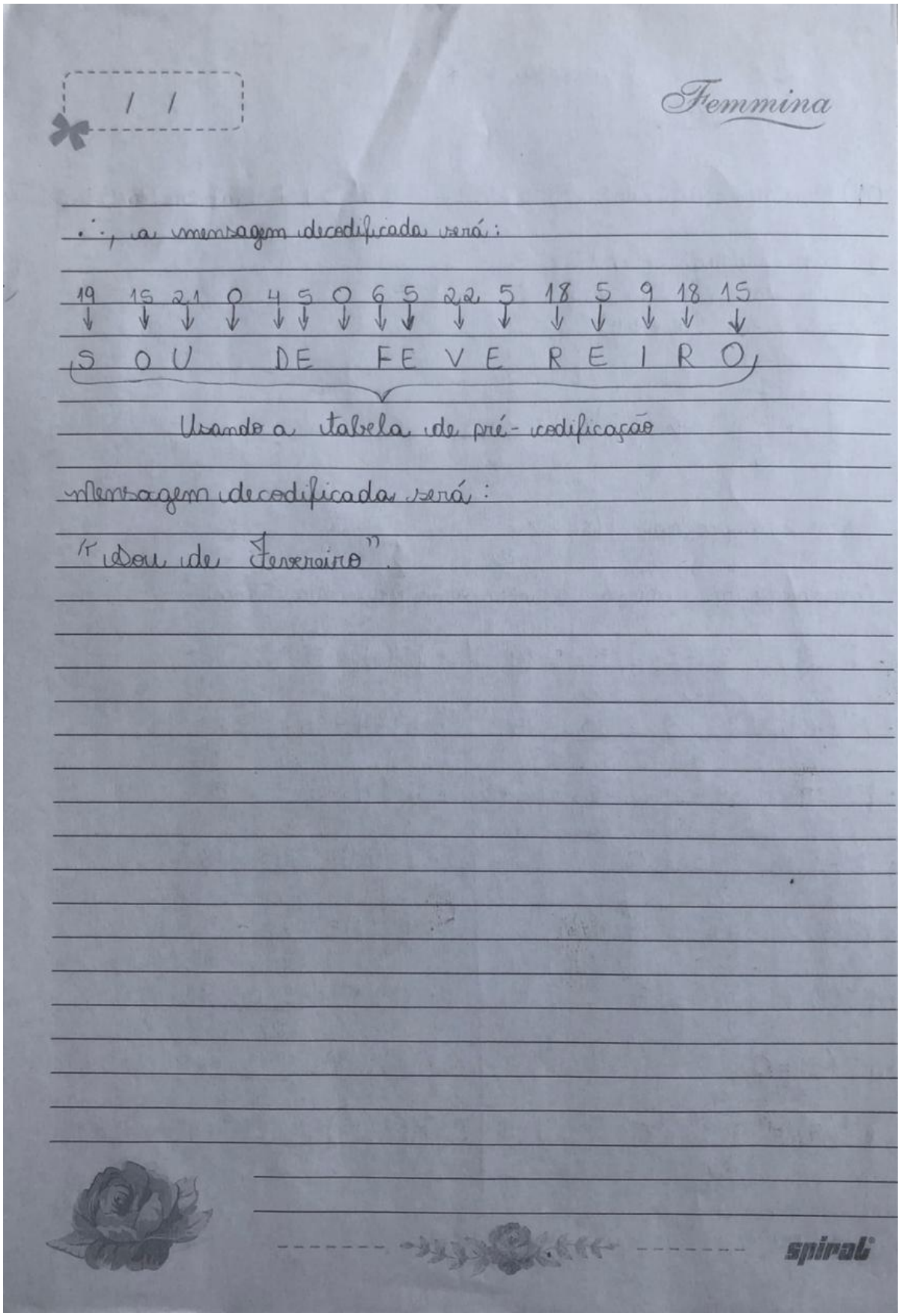
A seguir, serão mostrados um conjunto de imagens das resoluções de cada um dos exercícios propostos na seção anterior. Foi escolhida, para ser anexada neste trabalho, uma resolução por grupo, no entanto, todos os grupos lograram êxito e concluíram de forma satisfatória as atividades propostas.

Figura 7: Solução do Exercício 1 apresentada por um dos grupos



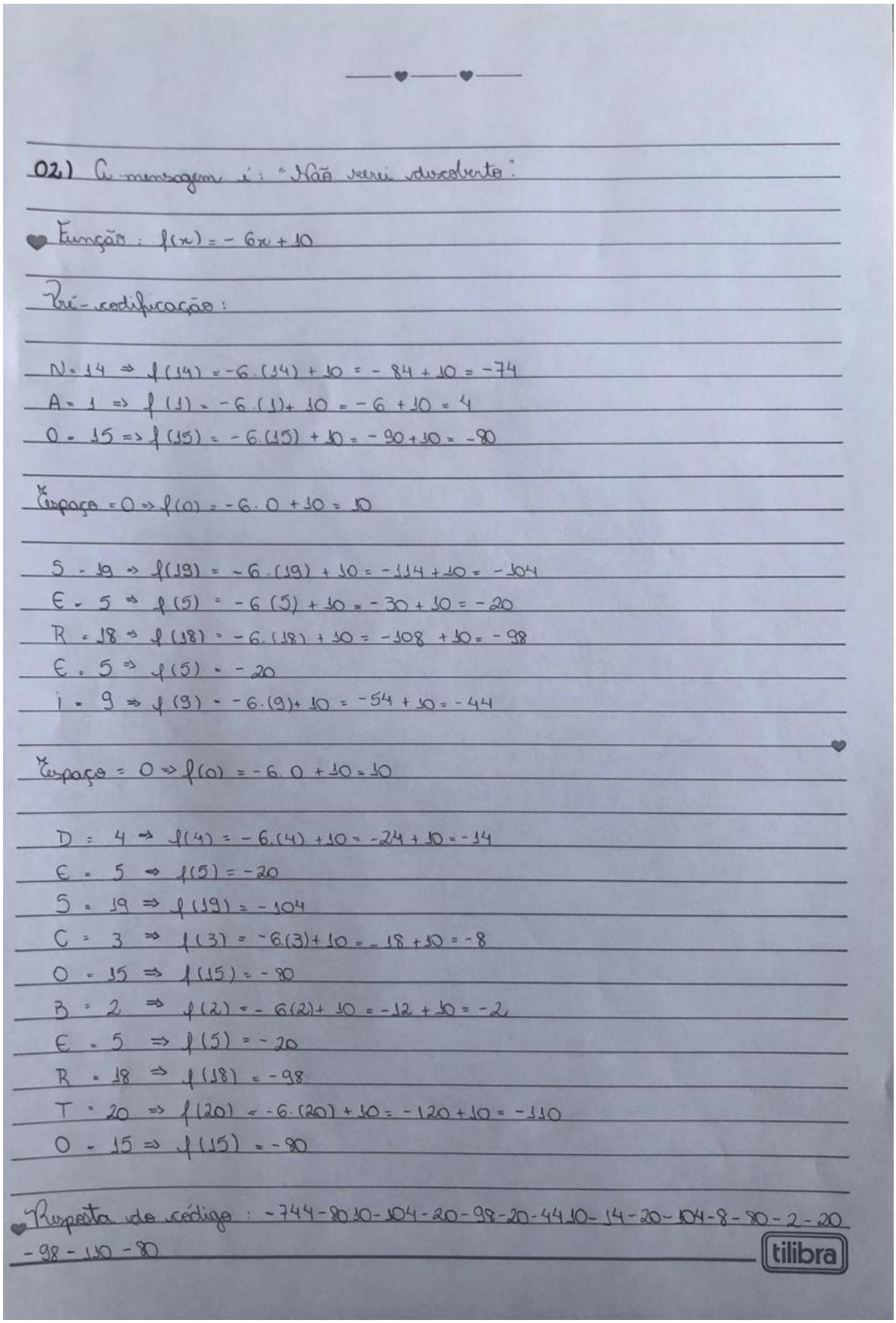

Fonte: Próprio autor

Figura 8: Continuação da resolução do exercício 1



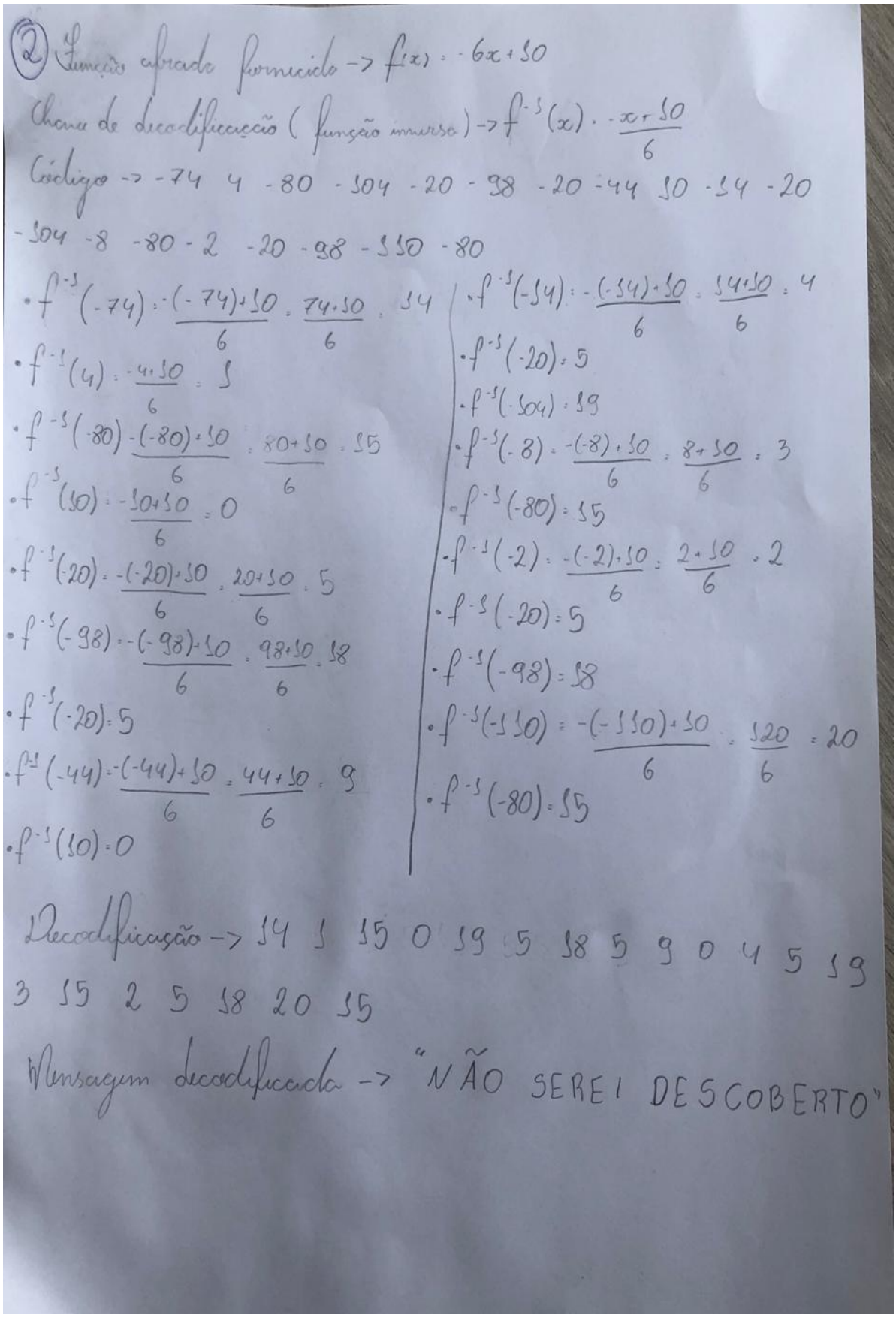

Fonte: Próprio autor

Figura 9: Elaboração da proposta do exercício 2 feita por um dos grupos



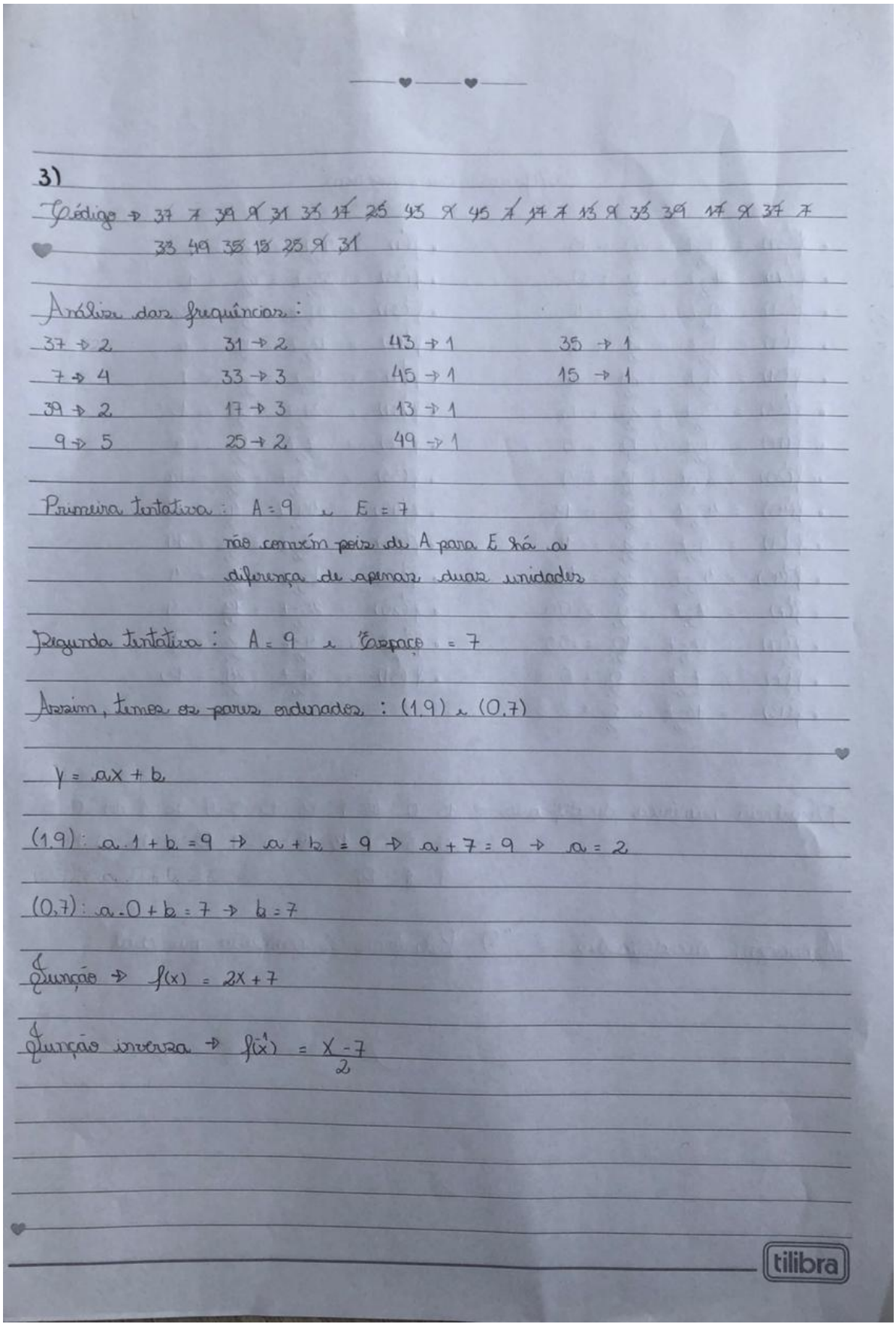

Fonte: Próprio autor

Figura 10: Solução do exercício 2 feita por um dos grupos



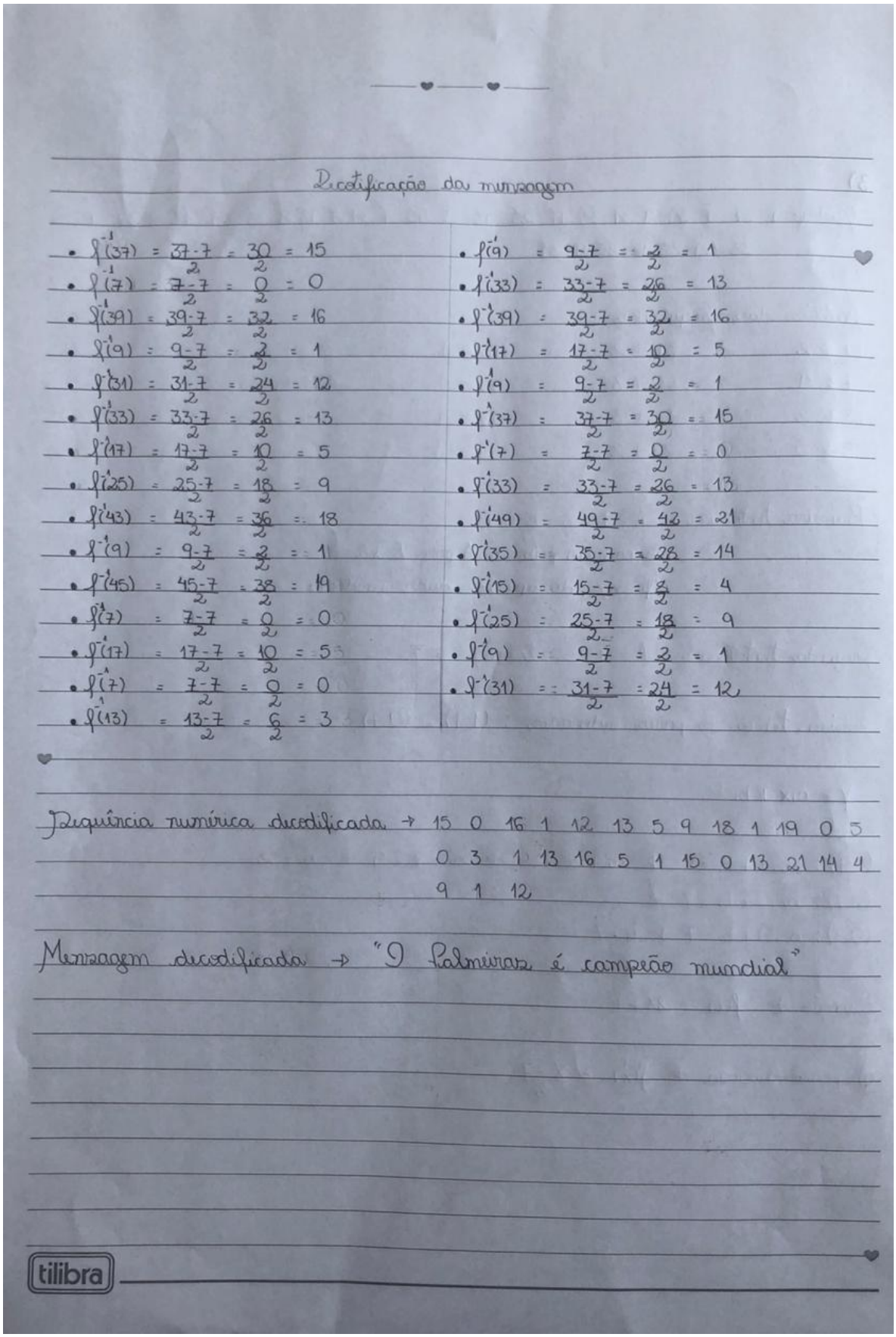

Fonte: Próprio autor

Figura 11: Solução do exercício 3 apresentada por um dos grupos



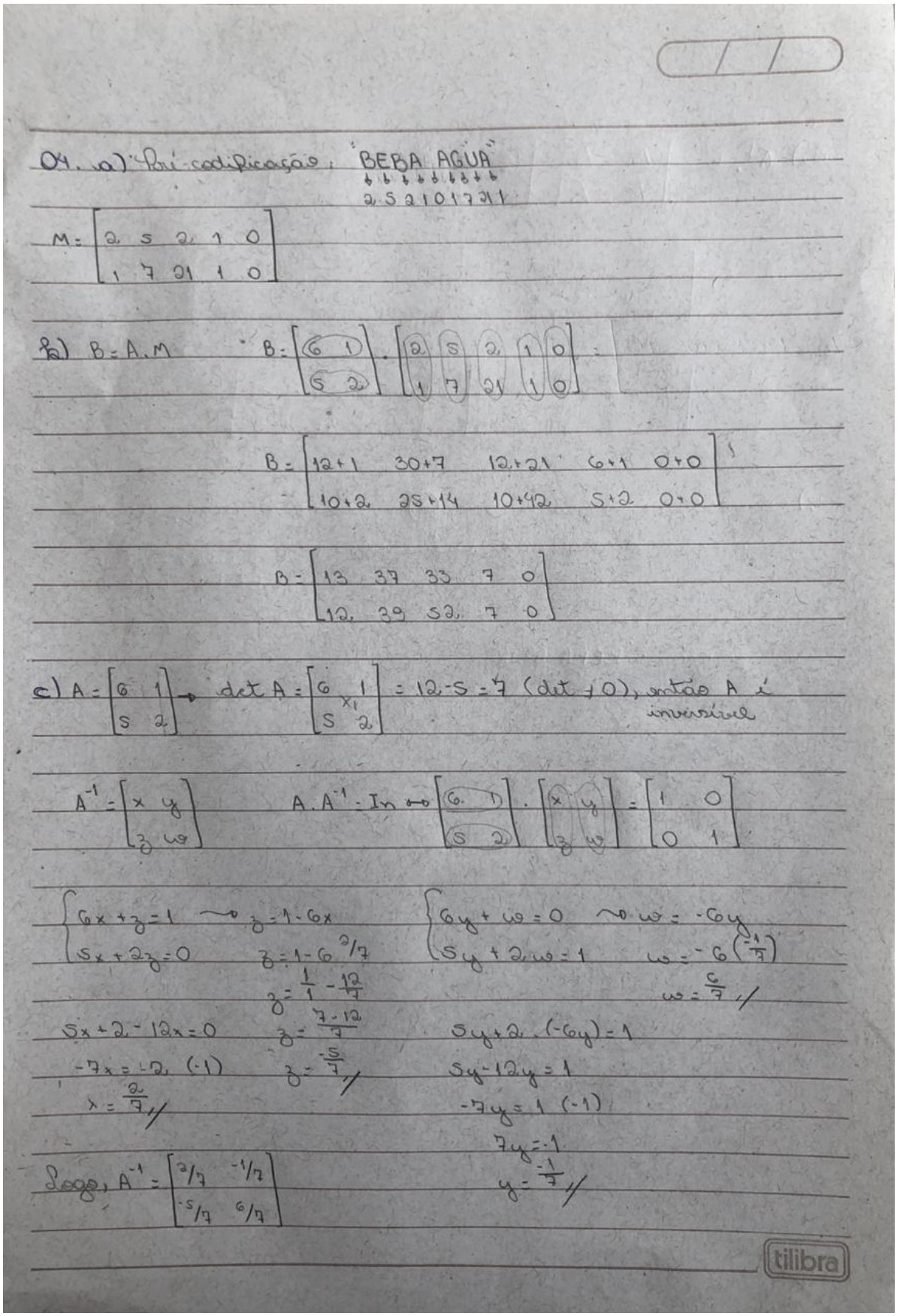

Fonte: Próprio autor

Figura12: Continuação da resolução do exercício 3



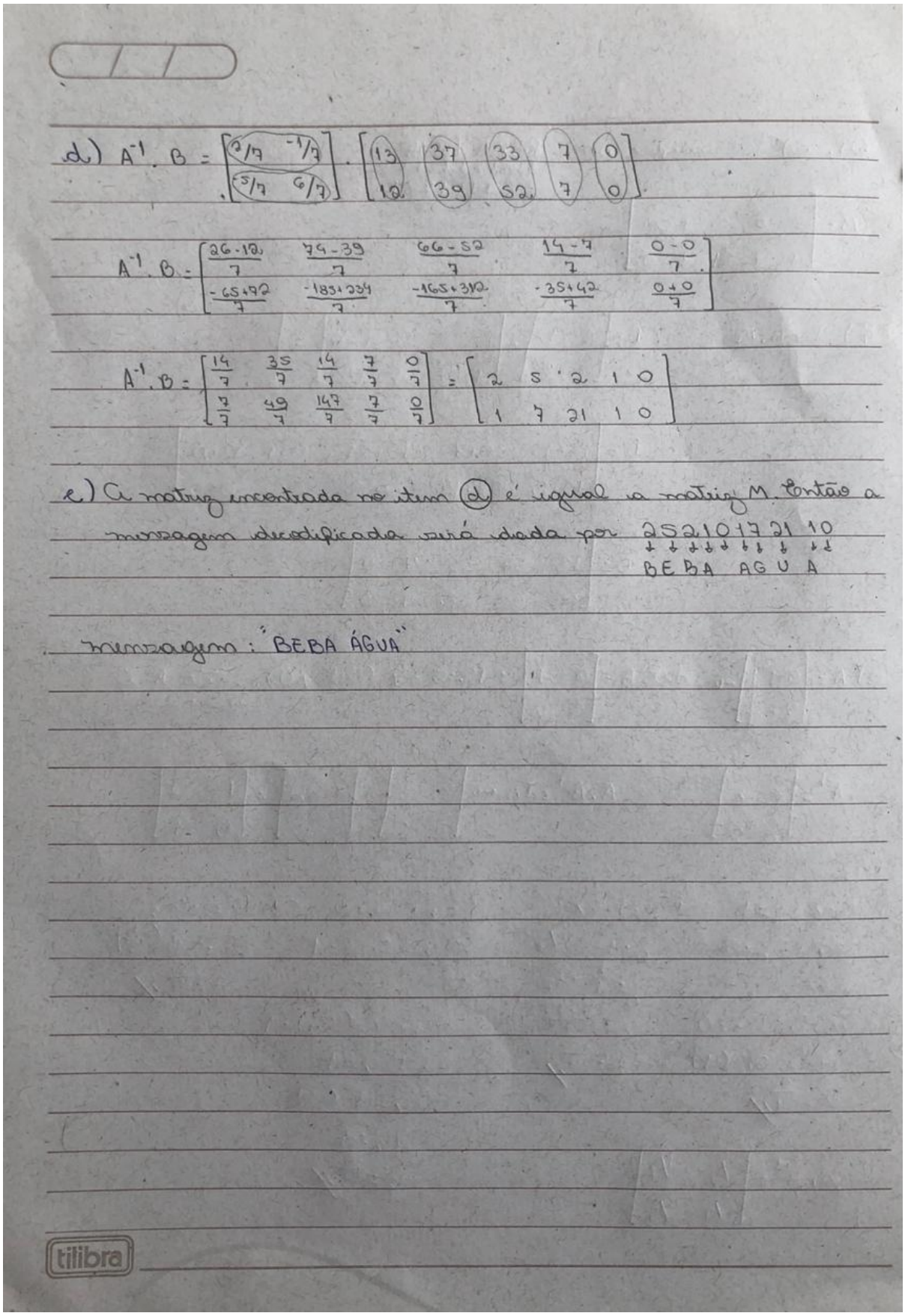

Fonte: Próprio autor

Figura 13: Solução do exercício 4 apresentada por um dos grupos



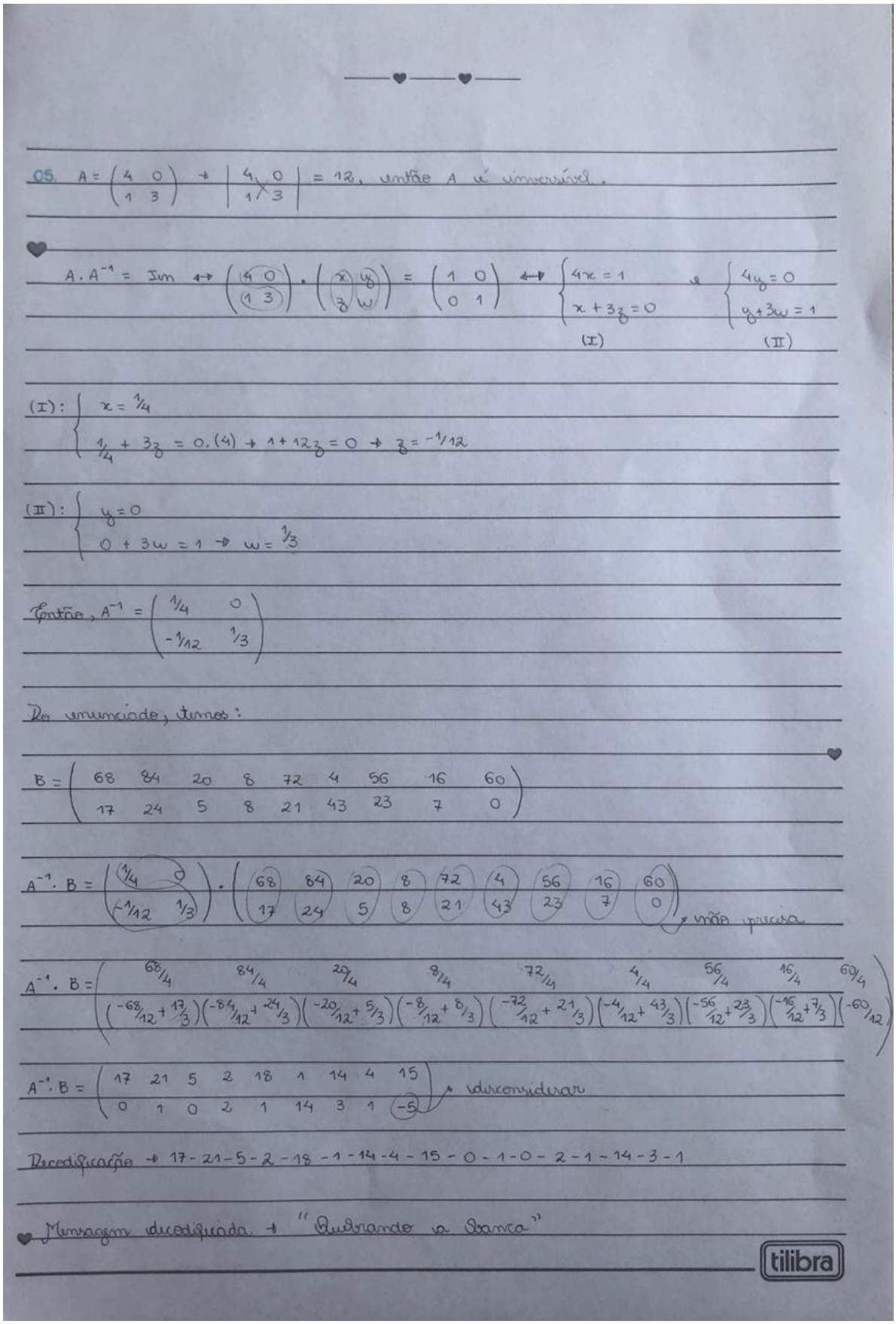

Fonte: Próprio autor

Figura 14: Continuação da resolução do exercício 4



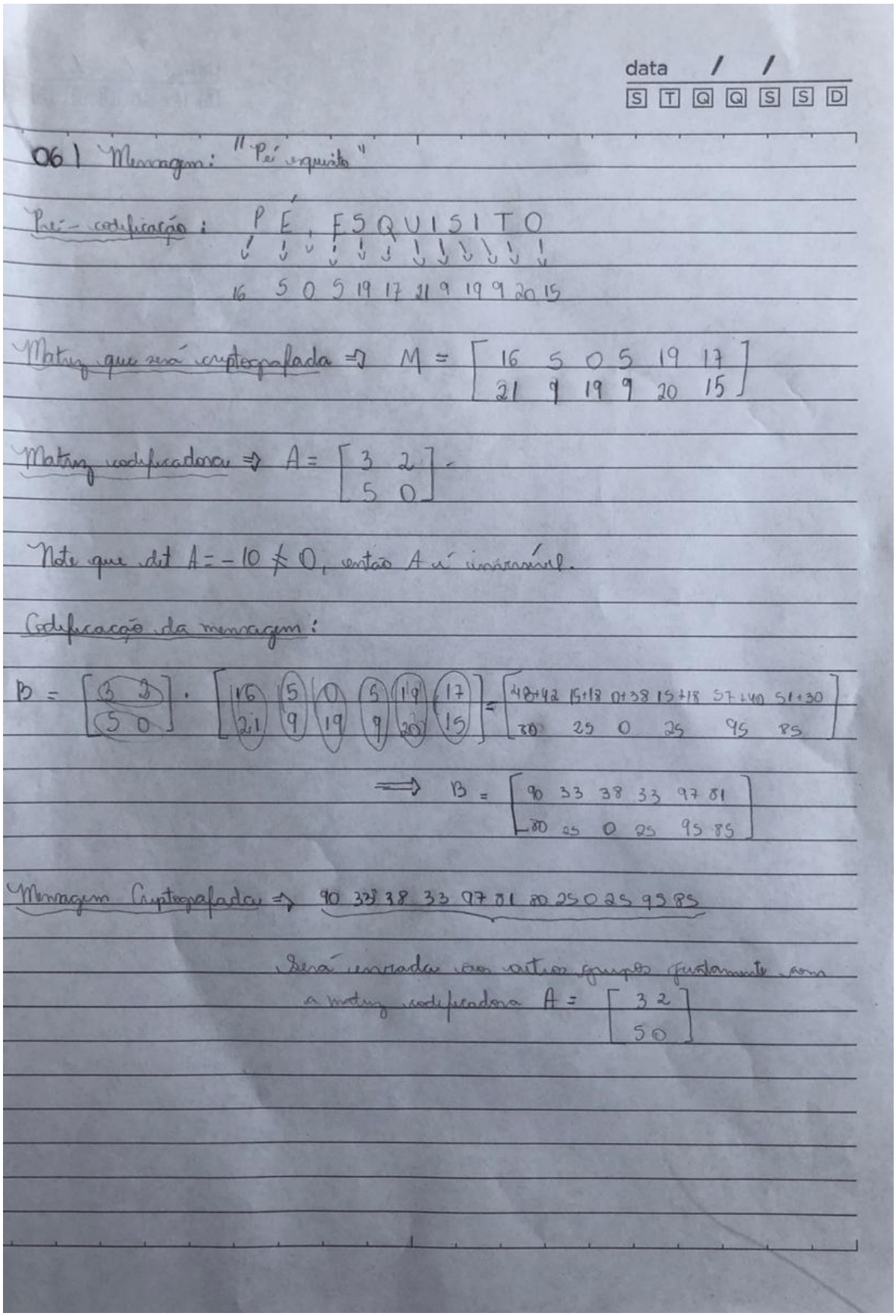

Fonte: Próprio autor

Figura 15: Solução do exercício 5 apresentada por um dos grupos



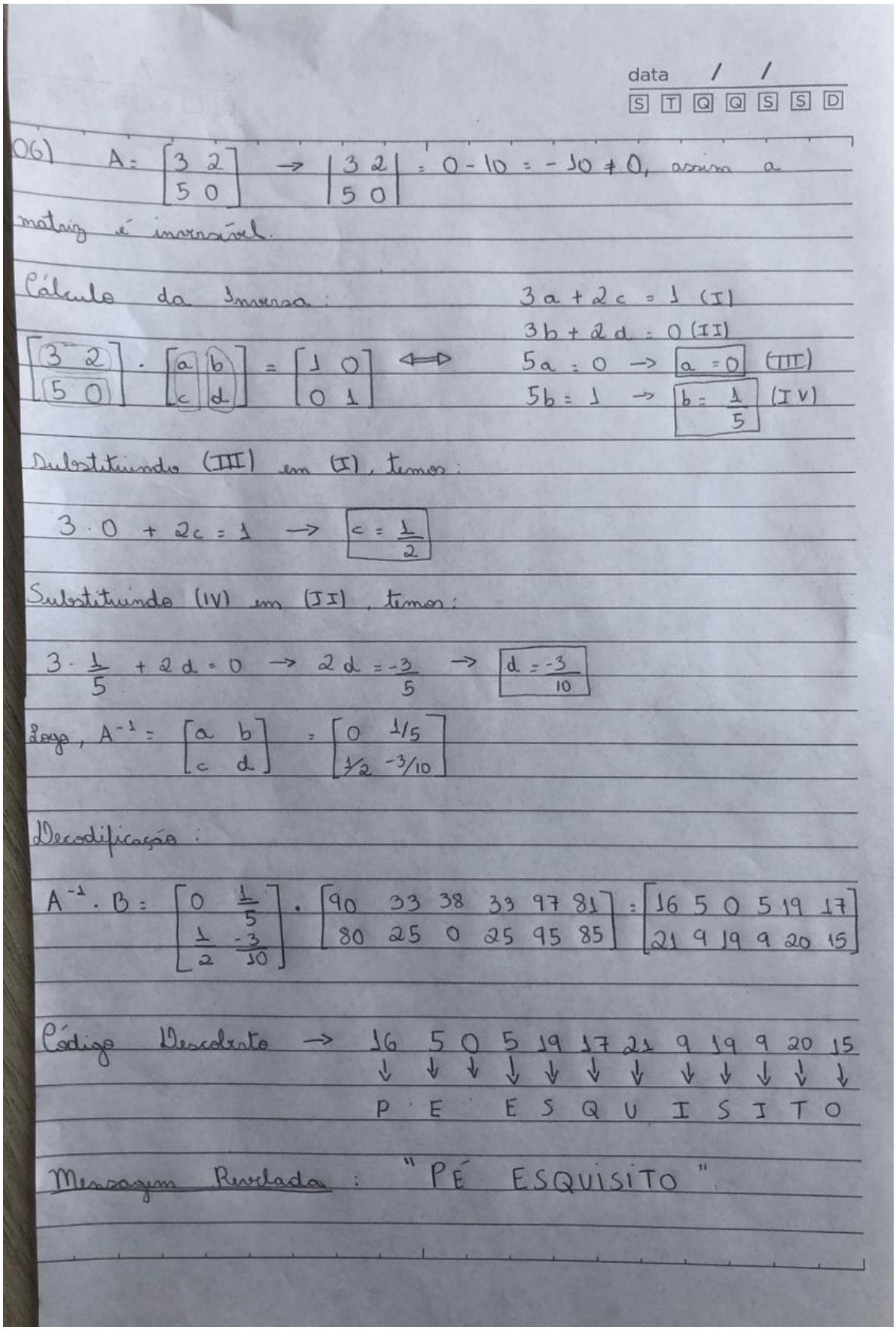

Fonte: Próprio autor

Figura 16: Elaboração da proposta do exercício 6 feita por um dos grupos




Fonte: Próprio autor

Figura 17: Solução do exercício 6 feita por um dos grupos




Fonte: Próprio autor

As atividades foram desenvolvidas pelos grupos de alunos de forma cooperativa e organizada. Ao término, todos os grupos conseguiram concluir e entender os exercícios propostos de forma satisfatória, alguns até mesmo sem a necessidade da intervenção e ajuda do professor.

Além disso, o cooperativismo em grupo e o interesse em desmistificar mensagens ocultas contribuíram de forma significativa para o desenrolar de todo o processo. Os grupos se comportaram de forma exemplar, visto que entre os $20$ alunos que iniciaram as atividades não houve se quer um único abandono.

No entanto, para concluir que o objetivo de fixar conteúdos matemáticos por meio da criptografia foi realmente alcançado, ainda se fez necessário ter a certeza de que os alunos também conseguiriam resolver exercícios, análogos aos feitos em grupo, de forma individual e autônoma.

Desta maneira, duas questões foram elaboradas com o intuito de serem resolvidas pelos educandos de forma individual. A primeira questão foi feita para verificar o aprendizado relacionado ao estudo das funções afins, já a segunda, relacionada ao campo das matrizes. A intenção real, por meio das duas questões extras, foi a de identificar eventuais falhas durante a aprendizagem cooperativa. Sendo assim, foram feitos gráficos dos desempenhos individuais dos alunos obtidos por tipo de questão (função afim ou matriz) e por quantidade de questões acertadas, com o intuito de que o educador ainda pudesse intervir e sanar possíveis defasagens de assimilação de conteúdos por parte de um ou outro aluno específico. Os discentes não tinham conhecimento de que tais atividades seriam aplicadas, dessa maneira, as questões foram aplicadas de forma surpresa pelo professor.

## 2.5. Atividades propostas para serem trabalhadas de forma individual

**01.** Dado o código

$$7\ 52\ 58\ 19\ 46\ 16\ 31\ 4\ 22\ 67\ 46\ 13\ 7\ 49\ 4\ 7\ 22\ 31\ 43$$

gerado pela função cifradora $f(x) = 3x + 4$, decodifique a mensagem usando a chave secreta, ou seja, usando a função inversa de $f$.

**02.** Decodifique a mensagem

$$40\ 43\ 86\ 33\ 63\ 83\ 3\ 18\ 28\ 44\ 10\ 36\ 38\ 2$$

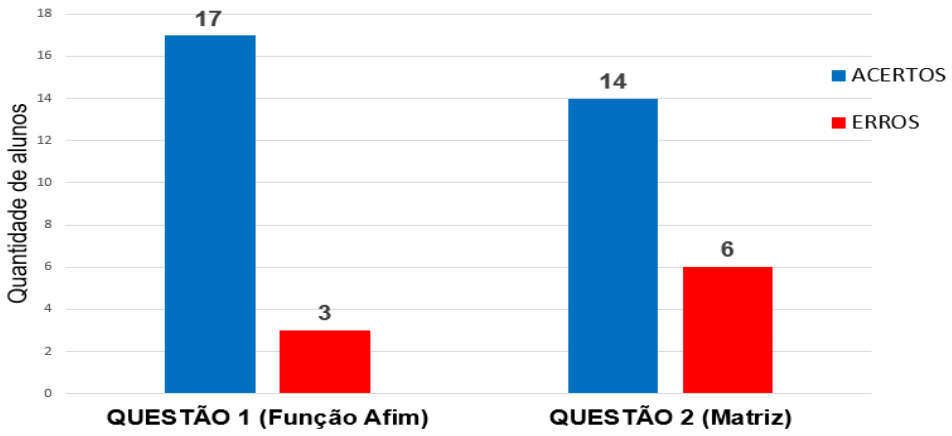
criptografada por meio da matriz codificadora

$$A = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}.$$

## 2.6. Desempenho obtido pelos alunos na atividade individual

Diferentemente do que foi feito na seção 2.4, não serão apresentadas as imagens das resoluções obtidas por cada um dos vinte alunos que realizaram as atividades. A análise do desempenho feita pelo docente, após a correção das questões, foi dada por meio de dois gráficos que possibilitaram diagnosticar falhas no processo de assimilação dos conteúdos e também, a necessidade de propostas de intervenção, a fim de que todos os alunos lograssem êxito no principal objetivo de todo o capítulo 2: fixar de forma satisfatória os conteúdos relacionados a funções afins e matrizes usando criptografia.

Gráfico 1 – Número de acertos e erros dos alunos por questão

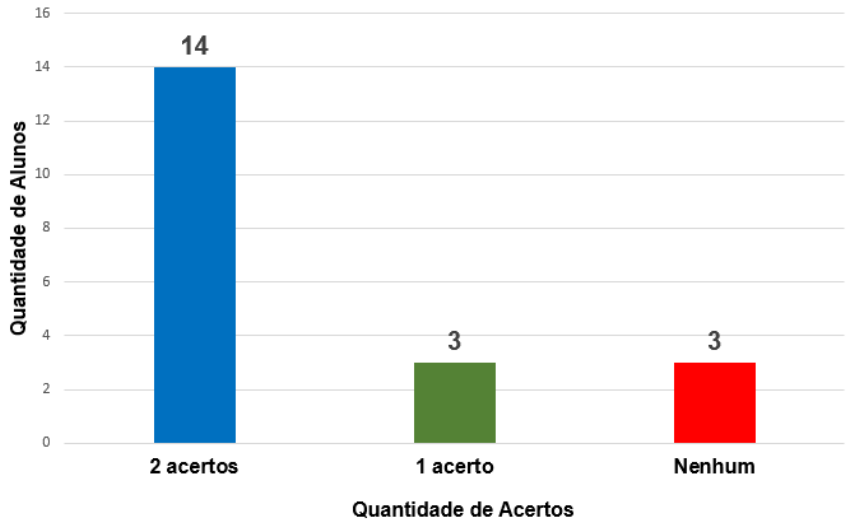



Fonte: Próprio autor

A análise do gráfico 1 revela que os desempenhos individuais dos alunos envolvidos foram de certa maneira bastante satisfatórios, visto que 17 alunos (85%)

acertaram a questão envolvendo funções afins e 14 alunos (70%) acertaram a questão que utilizava matrizes. A diferença entre o número de acertos das questões 1 e 2, evidenciou um domínio, por parte dos alunos envolvidos, ligeiramente maior de um conteúdo em relação ao outro, fato que já havia sido previsto na seção 2.2, quando mencionado um ganho de complexidade no trabalho de criptografias com matrizes em relação ao feito com funções afins.

Gráfico 2 – Quantidade de questões acertadas pelos alunos




Fonte: Próprio autor

O gráfico 2 possibilita outro tipo de análise. Por meio dele, o professor poderia elaborar intervenções pedagógicas a serem trabalhadas com os seis alunos que erraram uma ou duas questões, notando também que três destes alunos não obtiveram acerto em nenhuma das questões. A porcentagem alta de acertos e de bom desempenho dos alunos só aumenta o embasamento de que as atividades realizadas de forma cooperativa trazem bons resultados e contribuem de forma significativa para o aprendizado, afinal, foi por meio das atividades resolvidas em grupos que os alunos adquiriram os conhecimentos necessários para tamanha assertividade nas atividades feitas de forma individual.

Entretanto, os gráficos 1 e 2 também revelam a necessidade de existirem, atreladas as atividades cooperativas, atividades realizadas de forma individual, pois somente por meio destas é possível diagnosticar de forma mais precisa e específica a quantidade de alunos com falhas no processo de ensino-aprendizagem. Neste caso específico, o professor dedicou um tempo para ajudar os alunos que não conseguiram

assimilar e desenvolver corretamente as atividades. É muito importante citar, nesta etapa do trabalho, que alguns alunos, que dominaram totalmente os processos descritos para a resolução dos exercícios, ajudaram de forma significativa, juntamente com o professor, a sanar as falhas obtidas no processo de ensino-aprendizagem dos demais colegas.

## 2.7. *Considerações sobre as atividades do capítulo*

As atividades propostas neste capítulo foram trabalhadas durante 13 aulas de 50 minutos, realizadas no contraturno do horário de aula dos alunos. Ao término das atividades, os alunos agradeceram e pediram para que experiências como esta fossem repetidas por mais vezes na escola, enfatizando, assim, a importância de se trabalhar as matérias escolares de maneira mais atrativa e trazendo os alunos para contextos que os aproximem de assuntos de aplicação real do seu cotidiano.

# 3. EVOLUÇÃO DA CRIPTOGRAFIA E O MÉTODO RSA

A transmissão de informação por meio de mensagens codificadas é bastante antiga e passou por várias modificações mediante o desenvolvimento de cada época, sendo assim, a criptografia foi evoluindo de acordo com as necessidades e evoluções tecnológicas da sociedade.

Em tempos antigos, as estratégias de guerra dependiam muito do sucesso na transmissão de informações. Estas deveriam ser codificadas, pois caso o mensageiro fosse capturado por tropas inimigas ainda teriam a difícil missão de decifrar a mensagem. Nessa época a transmissão de informações poderia ser extremamente lenta, visto que dependia da maneira como o mensageiro iria percorrer enormes distâncias.

Com o advento do telégrafo, as mensagens poderiam percorrer grandes distâncias de forma rápida e sem a necessidade de um mensageiro. No entanto, mesmo com essa facilidade na transmissão de mensagens, não havia uma garantia de que a linha não estivesse sujeita a interceptações, o que mantinha a necessidade de codificação.

Com o surgimento do telefone, as mensagens poderiam ser transmitidas por meio de conversas a longas distâncias. Todavia, assim como no caso do telégrafo, o telefone também poderia sofrer interceptações por meio de grampos e escutas telefônicas, colocando em risco as informações confidenciais. Nessa época, a codificação continuou a ser importante, dessa vez na linguagem em códigos, pois se a conversa caísse em escutas inimigas, ainda teriam a árdua tarefa de desvendar um novo nível de fala feito com a incorporação de códigos.

Nas mais diferentes épocas é notório o interesse em transmitir informações confidenciais de forma segura, em contrapartida, o interesse em desvendar tais informações também sempre se fez presente. A Criptoanálise, ciência que estuda a decodificação de uma mensagem sem conhecer o seu segredo (chave), também caminhava a passos largos e sua evolução sempre foi uma espécie de combustível para que um novo sistema, sempre mais seguro que o anterior, fosse criado.

Uma verdadeira guerra intelectual entre povos e nações foi surgindo mediante o avanço da criptografia, estabelecendo uma breve analogia a Guerra Fria, em que havia uma corrida armamentista e tecnológica a fim de mostrar poderio bélico, no caso da criptografia, poderíamos chamá-la de corrida armamentista intelectual, como pregava Singh no relato abaixo:

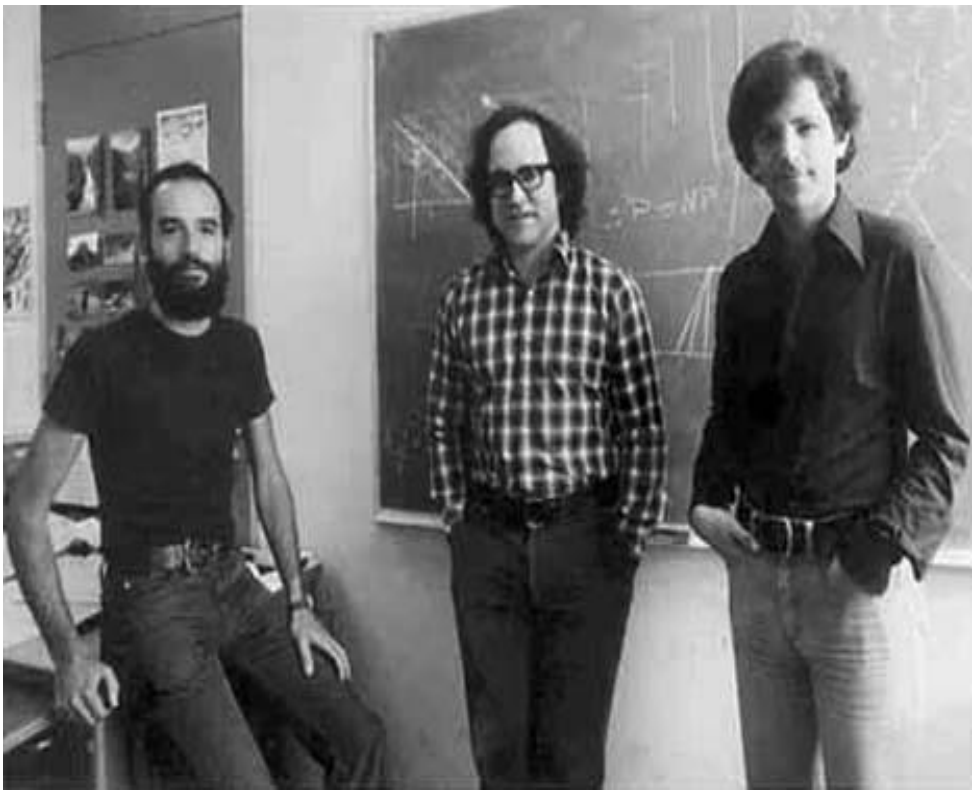
> "A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de código e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana" (Singh, 2003).

Nos tempos atuais, com toda a tecnologia relacionada as informações transmitidas de forma instantânea via internet, a problemática de se transmitir mensagens seguras se faz ainda mais presente. Todos os tipos de operações eletrônicas usadas atualmente precisam ser codificados, tais como: pagamentos de boletos, compras com cartão de crédito, transferências, transações comerciais, financeiras e diversas outras. A própria rede social atual é composta por mensagens protegidas por criptografias, fato que também ocorre em vários sites e lojas virtuais, sendo assim, surge a necessidade de existir um sistema de codificação extremamente seguro, até mesmo porque o avanço da Criptoanálise acompanha todo o processo e cada vez mais experts em informática ("hackers") estão dispostos e interessados em invadir dispositivos eletrônicos confidenciais.

Os dados de hoje em dia são todos transmitidos via cabo telefônico ou rádio, logo, as informações continuam correndo constante perigo, análogos aos enfrentados nas épocas do telégrafo e do telefone. Então a saída continuava a mesma: codificar as mensagens para tornar a transmissão dos dados mais segura.

A evolução da Criptoanálise, fez-se tornar necessária a invenção de novos códigos, que mesmo com o auxílio de algoritmos e computadores, fossem difíceis de decifrar. Em 1977, surgiu o método RSA, com segurança e aplicabilidade garantidas pela Matemática, em especial pelo campo da Teoria dos Números. O método inventado pelos americanos Ronald Rivest, Adi Shamir e Leonard Adleman, é até hoje a criptografia de chave pública mais usada no mundo. Um método que consiste na utilização de duas chaves distintas, sendo uma delas disponibilizada publicamente, daí o nome "chave pública'. No RSA a chave usada para codificar uma mensagem não é capaz de decodificar a mesma. Será mostrado adiante que todo o processo é muito fácil de ser feito e extremamente difícil de ser desfeito.

Figura 18: Criadores do método RSA



Fonte: <http://viterbi.usc.edu/news/news/2011/len-adleman-and.htm>. Acesso em: 12/08/19

## 3.1. Descrição do método e aplicação de um exemplo

Nesta e nas próximas seções deste capítulo, ao ser abordado o método RSA, será considerado que o aluno, agora do ensino superior, já tenha domínio de assuntos relacionados à Teoria dos Números, ramo pouco abordado nas matrizes curriculares da educação básica e que possui certo descompasso no ensino superior, entre como é abordado e a sua real aplicabilidade em assuntos importantes do cotidiano. Conhecer temas como: Números Inteiros, Congruências, Teorema de Fermat, Inversos Modulares, Algoritmo Chinês dos Restos, Números Primos e outros da Teoria dos Números, serão fundamentais para o bom uso e entendimento do método RSA. Como sugestão aos leitores mais interessados em explorar ou relembrar tais temas, fica a excelente obra de Coutinho citada na referência [ 1 ] deste trabalho e que foi a maior motivadora das ideias presentes neste capítulo.

A criptografia RSA também poderia ser apresentada aos alunos do ensino médio a título de interesse. Uma boa ideia seria despertar a curiosidade do aluno, nessa etapa do ensino, para a eficiência e segurança do método trabalhando a complexidade na decomposição em fatores primos de números extremamente grandes. No entanto, será apresentada como uma estratégia de trabalhar Teoria dos Números no ensino superior de forma mais prática e atrativa, visto que abordagens mais cativantes podem auxiliar na fixação de conteúdos como foi visto no capítulo $2$.

A chave de codificação utilizada neste método, conhecida como chave pública, é fornecida por um número $n$ formado pelo produto de dois números primos distintos $p$ e $q$. Já a chave de decodificação, conhecida como chave privada, por dois números primos $p$ e $q$, que devem ser mantidos em segredo para que o método realmente funcione. Mesmo havendo uma aparente proximidade entre ambas, não é possível encontrar a chave privada a partir da chave pública $n$, pois, para isso, seria necessário decompor a chave $n$, tal fato decorre do método RSA ser usado mediante escolha de números primos muito grandes, originando assim um número $n$ ainda maior.

Decompor um número muito grande em fatores primos é uma tarefa praticamente impossível devido ao tempo necessário para fazê-lo com os métodos conhecidos atualmente e até mesmo com o auxílio dos computadores mais modernos. Esse impasse na dificuldade de fatorar números extremamente grandes poderia ser amplamente abordado até mesmo com os alunos da educação básica, como citado anteriormente, visto que decomposição em fatores primos é um tema presente nas matrizes curriculares de Matemática em todas as unidades de ensino. O processo ainda poderia ajudar o aluno a entender posteriormente por que o método é seguro e despertar seu interesse pela matemática ao relacionar a temática com a sua importância vivida atualmente nas transações realizadas via web. Aproximando-os assim, de uma abordagem com finalidade concreta já que muitas vezes a Matemática é vista pelos discentes como um processo enfadonho e sem finalidade alguma.

Abaixo segue uma tabela que ilustra bem essa dificuldade de fatorar números extremamente grandes, feita com base no método usual das tentativas de se decompor um número em fatores primos. Também é importante ressaltar a dificuldade em identificar se um número muito grande é primo, mesmo com vários testes de primalidade já conhecidos atualmente.

Tabela 6 – Tempo necessário para quebrar o número $n$

| nº de algarismos de $n$ | tempo necessário para "quebrar" o *RSA* |
|---|---|
| 50 | 3,9 horas |
| 75 | 104 dias |
| 100 | 74 anos |
| 200 | $3{,}8 \times 10^{7}$ séculos |
| 300 | $4{,}9 \times 10^{13}$ séculos |
| 500 | $4{,}2 \times 10^{23}$ séculos |

Fonte: Criptografia e a importância das suas aplicações. RPM 12.

A seguir serão apresentados os dados necessários para a execução de uma criptografia usando o método RSA:

- Escolha de dois números primos distintos $p$ e $q$ grandes o suficiente (geralmente com $100$ ou mais algarismos) e cálculo do produto $p \,.\, q$, resultando $n$ ($n = p \,.\, q$);

- $n$ será utilizado para codificar a mensagem ($n$ será a chave pública);

- $p$ e $q$ serão utilizados para decodificar a mensagem ($p$ e $q$ serão as chaves privadas);

- para quebrar o código RSA será necessário fatorar $n$ descobrindo assim os números $p$ e $q$, porém ao se utilizar números grandes o suficiente ($100$ ou mais dígitos), fatorá-los se torna um processo inviável devido ao tempo que os métodos atuais levariam, tornando assim impossível a descoberta de tais números.

Feito isso, as chaves de codificação e de decodificação serão números, e a codificação será realizada por meio do cálculo de uma potência módulo $n$ (chave

pública de codificação). Para que isso seja possível, a mensagem a ser codificada precisa ser um número inteiro e, portanto, quando tal mensagem estiver em formato de texto deverá ser convertida em uma sequência de números para que assim seja possível codificá-la, ou seja, primeiramente deverá ser feito um processo de pré-codificação alfabeto-numérico, análogo ao que foi feito ao trabalharmos outros tipos de criptografia nos capítulos anteriores.

A seguir uma explicação de forma básica de como se aplica na prática o método RSA, por meio de uma espécie de "receita detalhada" feita passo a passo e dividida em oito etapas:

Etapa $1$ – Conversão das letras da mensagem criptografada em números de dois dígitos para evitar ambiguidades, conforme foi visto em $2.1$, feita por meio da tabela $7$ mostrada abaixo:

Tabela $7$ – Pré-codificação das mensagens em RSA

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **10** | **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** |

Fonte: Próprio autor

Nesta conversão, o espaço entre duas palavras será codificado pelo número $36$ e, assim, poderemos ter toda a mensagem convertida para uma sequência numérica.

Etapa $2$ – Escolha dos números primos distintos $p$ e $q$, os quais serão chamados de chaves secretas, calculando assim a chave pública $n$ por meio do produto $p \cdot q$, ou seja, $n = p \cdot q$.

Etapa $3$ – Quebra da sequência numérica em blocos, de modo que cada um dos blocos produzidos seja menor que $n$. Os blocos podem ser quebrados livremente desde que respeitem esta restrição imposta, no entanto, também devem estar atrelados ao fato de que nenhum deles pode ser iniciado com o número $0$, a fim de evitar eventuais problemas na hora da decodificação da mensagem. Ao concluir esta etapa também será sanado o problema de uma possível decodificação da mensagem por análise de frequências, visto que esses blocos não correspondem a símbolos, letras ou qualquer outro tipo de unidade linguística.

Etapa $4$ – Nesta etapa, tem-se o início do processo de codificação da mensagem. Para codificar a mensagem, é usada a chave pública, composta pelos números $n$ e $k$, em que $k$ é um número inteiro positivo e invertível módulo $\phi(n)$, ou seja, $mdc\big(k, \phi(n)\big) = 1$. Note que o cálculo de $\phi(n)$ se torna possível por meio da posse da chave de decodificação, pois $n = p \cdot q$ e assim, temos: $\phi(n) = \phi(p \cdot q) = (p-1) \cdot (q-1)$. Dessa maneira, para codificar a mensagem, será necessário saber o valor de $k$ juntamente com a chave $n$, ou seja, $k$ também fará parte da chave de codificação.

Etapa $5$ – Seja $b$ o bloco a ser codificado, logo $b$ será um inteiro positivo e menor que $n$ (restrição imposta na etapa $3$). Tomando o bloco codificado como $C(b)$, obteremos $C(b)$ por meio do seguinte processo: $b^k \equiv C(b)\ mod\ n$, sendo $0 \leq C(b) \leq n$, dessa maneira, pode-se dizer que o bloco codificado $C(b)$ corresponde ao resto da divisão de $b^k$ por $n$. Após a codificação de cada um dos blocos pelo processo descrito, os mesmos não poderão mais ser agrupados de modo a formarem um grande número, pois caso isso venha a ocorrer, será impossível conseguir organizar o processo de decodificação.

Etapa $6$ – Nesta etapa, tem-se o início do processo de decodificação da mensagem. Para a realização da decodificação, é necessário a posse de dois números: $n$ e $d$, em que $d$ corresponde ao inverso de $k$ módulo $\phi(n)$. Dessa forma, $d$ e $k$ serão os números que formarão a chave de decodificação. De posse de $d$ e $k$, a próxima etapa mostrará os passos que irão permitir a compreensão do processo da reconstrução dos blocos originais formados antes do processo de codificação.

Etapa $7$ – Seja $a$ o bloco codificado, cuja decodificação é necessária, e $D(a)$ o resultado do bloco decodificado. O cálculo de $D(a)$ será feito da seguinte maneira: $a^d \equiv D(a)\ mod\ n$, sendo $0 \leq D(a) \leq n$, assim pode ser concluído que $D(a)$ corresponde ao resultado do resto da divisão de $a^d$ por $n$. Desta forma, o objetivo principal desta etapa consiste em encontrar $d$, que poderá ser facilmente encontrado por meio do algoritmo euclidiano estendido, desde que sejam conhecidos $\phi(n)$ e $k$.

Etapa $8$ – Por fim, como última etapa, é necessário provar que $D\big(C(b)\big) = b$, em que $b$ corresponde a um bloco da mensagem original. O fato mostra que ao se decodificar um bloco da mensagem codificada, sempre será encontrado o bloco correspondente a mensagem original. Feito a decodificação de todos os blocos pelo processo descrito,

basta dispor novamente os blocos em uma sequência longa de números e, com o auxílio da tabela 7, convertê-los na mensagem original novamente.

Segue abaixo um exemplo de aplicação da criptografia RSA, seguindo as oito etapas descritas, objetivando compreender melhor o seu funcionamento na prática. Com a finalidade de dinamizar e facilitar o processo nos cálculos de congruências com expoentes e números que os tornem trabalhosos, os alunos poderão usar calculadoras científicas.

**Exemplo:** A mensagem **"ATACAR PELO LESTE"** será codificada.

Etapa 1

Conversão das letras em números por meio da tabela 7. Assim, a seguinte sequência numérica é obtida:

$$\mathbf{10291012102736251421243621142829 14}$$

Etapa 2

Escolha dos primos $p$ e $q$. Para que o processo seja facilmente entendido, serão escolhidos números primos pequenos a fim de facilitar os cálculos e o entendimento do aluno.

Sejam $p = 11$ e $q = 17$ os números primos escolhidos para a realização deste exemplo, decorre que $n = p \cdot q = 11 \cdot 17 = 187$.

Etapa 3

Nesta etapa, a sequência numérica, obtida na etapa 1, deverá ser quebrada em blocos. Os blocos devem respeitar as seguintes restrições: serem formados por números menores que 187 e não podem começar com 0.

Seguem os blocos obtidos separados apenas por espaçamentos:

$$102\ 9\ 101\ 12\ 102\ 73\ 62\ 51\ 42\ 124\ 36\ 21\ 142\ 82\ 9\ 14$$

Etapa 4

Agora é feito o cálculo de $\phi(187)$ com o intuito de escolher um número $k$ de maneira que $mdc\big(k, \phi(187)\big) = 1$. Assim, tem-se:

$$\phi(187) = \phi(11 \cdot 17) = (11-1) \cdot (17-1) = 10 \cdot 16 = 160$$

Note que $160 = 2^5 \cdot 5$, assim convenientemente será escolhido $k = 7$. A escolha de um número primo considerado pequeno (7) tem como objetivo facilitar os cálculos e o entendimento de todo o processo. Assim, com $7$ e $187$, a chave pública necessária para o processo de codificação da mensagem poderá ser produzida.

Etapa $5$

Agora, de posse da chave descrita na etapa anterior, pode ser dado início ao processo de codificação. Tomando cada bloco codificado como $C(b)$, este poderá ser obtido por meio do seguinte processo:

$$b^7 \equiv C(b)\ mod\ 187, \text{ sendo } 0 \leq C(b) \leq 187.$$

Dessa maneira, o bloco codificado $C(b)$ corresponde ao resto da divisão de $b^7$ por 187, onde $b$ representa os blocos obtidos na etapa $3$.

Fazendo a codificação da maneira descrita acima, no primeiro bloco, tem-se:

$$102^7 \equiv 102^2 \cdot 102^2 \cdot 102^2 \cdot 102\ mod\ 187,$$

mas como

$$102^2 = 10404 = 55 \cdot 187 + 119,$$

então,

$$102^2 \equiv 119\ mod\ 187.$$

Logo,

$$102^7 \equiv 119 \cdot 119 \cdot 119 \cdot 102\ mod\ 187.$$

De modo análogo,

$$119 \cdot 119 = 14161 = 75 \cdot 187 + 136$$

e

$$119 \cdot 102 = 12138 = 64 \cdot 187 + 170.$$

Assim,

$$119 \cdot 119 \equiv 136\ mod\ 187$$

e

$$119 \cdot 102 \equiv\ 170\ mod\ 187.$$

Desta maneira,

$$102^7 \equiv\ 136 \cdot 170\ mod\ 187.$$

Por fim,

$$136 \cdot 170 = 23120 = 123 \cdot 187 + 119.$$

Portanto,

$$102^7 \equiv\ 119\ mod\ 187.$$

Usando o mesmo raciocínio nos demais blocos, encontram-se:

- $9^7 \equiv 70\ mod\ 187$
- $101^7 \equiv 84\ mod\ 187$
- $12^7 \equiv 177\ mod\ 187$
- $102^7 \equiv 119\ mod\ 187$
- $73^7 \equiv 61\ mod\ 187$
- $62^7 \equiv 105\ mod\ 187$
- $51^7 \equiv 17\ mod\ 187$
- $42^7 \equiv 15\ mod\ 187$
- $124^7 \equiv 163\ mod\ 187$
- $36^7 \equiv 9\ mod\ 187$
- $21^7 \equiv 98\ mod\ 187$
- $142^7 \equiv 65\ mod\ 187$
- $82^7 \equiv 91\ mod\ 187$
- $9^7 \equiv 70\ mod\ 187$
- $14^7 \equiv 108\ mod\ 187$

Após a realização de todos as codificações feitas acima, o processo resulta nos blocos que seguem:

$$119\ \ 70\ \ 84\ \ 177\ \ 119\ \ 61\ \ 105\ \ 17\ \ 15\ \ 163\ \ 9\ \ 98\ \ 65\ \ 91\ \ 70\ \ 108$$

Etapa 6

Nesta etapa, é dado o início do processo de decodificação da mensagem. Para a realização da decodificação é necessário a posse de dois números: $n$ e $d$, onde $d$ é o inverso de $k$ modulo $\phi(n)$, ou seja, $d$ deverá ser dado pela relação $d \cdot k \equiv 1\, mod\, \phi(n)$. Para $k = 7$ e $\phi(n) = 160$, tem-se:

$$d \cdot 7 \equiv 1\, mod\, 160.$$

Sabemos que $mdc(7, 160) = 1$, assim existem $x_0, y_0 \in \mathbb{Z}$ tais que $7x_0 + 160y_0 = 1$. Desta forma, pela relação $7x_0 \equiv 1\, mod\, 160$ encontramos o número $d$.

Assim, a chave privada necessária para o início do processo de decodificação da mensagem será composta por $n = 187$ e $d = 23$.

Etapa 7

De posse da chave privada, seja $a$ a denominação de cada um dos blocos codificados na etapa 5 que serão decodificados, e $D(a)$ o resultado de cada um dos blocos decodificados, $D(a)$ será obtido da seguinte maneira:

$$a^d \equiv D(a) mod\, n, \text{ sendo } 0 \leq D(a) \leq n.$$

Como $n = 187$, $d = 23$ e sabe-se, um por um, os blocos codificados (valores de $a$), pode ser dado início ao processo de decodificação de cada um dos blocos, por meio da relação:

$$a^{23} \equiv D(a) mod\, 187, \text{ sendo } 0 \leq D(a) \leq 187.$$

No processo de decodificação do primeiro bloco deve ser encontrado o resto da divisão de $119^{23}$ por 187. Como $187 = 11 \cdot 17$, calcula-se de maneira mais prática o resto da divisão de $119^{23}$ por 11 e 17.

Note que

$$119^{23} \equiv 9^{23}\, mod\, 11.$$

Pelo Teorema de Fermat, tem-se:

$$9^{10} \equiv 1\, mod\, 11,$$

assim,

$$119^{23} \equiv 9^{23} \equiv\ 9^{2 \cdot 10+3} \equiv (9^{10})^2 \cdot 9^3\ \equiv 9^3\ \equiv 729\ \equiv 3\, mod\, 11.$$

Pode ser notado também que

$$119^{23} \equiv 0^{23} \equiv 0 \; mod \; 17,$$

desta forma, obtêm-se:

$$119^{23} \equiv 3 \; mod \; 11$$

e

$$119^{23} \equiv 0 \; mod \; 17.$$

Portanto, deve ser encontrada a solução do seguinte sistema de congruência:

$$\begin{cases} X \equiv 3 \; mod \; 11 \; (i) \\ X \equiv 0 \; mod \; 17 \; (ii) \end{cases}.$$

De $(i)$ segue que $X = 11k + 3$, e substituindo em $(ii)$, tem-se:

$$11k + 3 \equiv 0 \; mod \; 17$$

$$11k \equiv -3 \; mod \; 17$$

$$11k \equiv 14 \; mod \; 17 \; (*)$$

Agora, o inverso de 11 módulo 17 deve ser encontrado, para isto, usa-se o algoritmo de Euclides da seguinte maneira:

$$17 = 1 \cdot 11 + 6$$

$$11 = 1 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

Assim,

$$\begin{aligned} 1 &= 6 - 1 \cdot 5 \\ &= 6 - 1 \cdot (11 - 6) \\ &= 6 - 11 + 6 \\ &= 2 \cdot 6 - 11 \\ &= 2 \cdot (17 - 11) - 11 \\ &= 2 \cdot 17 - 2 \cdot 11 - 11 \end{aligned}$$

$$= 2 \cdot 17 - 3 \cdot 11$$

Desta maneira,

$$2 \cdot 17 - 3 \cdot 11 = 1.$$

Logo,

$$2 \cdot 17 - 3 \cdot 11 \equiv 1 \; mod \; 17$$

$$-3 \cdot 11 \equiv 1 \; mod \; 17$$

$$14 \cdot 11 \equiv 1 \; mod \; 17$$

Portanto, o inverso de $11$ módulo $17$ é $14$.

Multiplicando $(*)$ por $14$, tem-se:

$$14 \cdot 11k \equiv 14 \cdot 14 \; mod \; 17$$

$$k \equiv 9 \; mod \; 17,$$

assim,

$$k = 17k_2 + 9, \text{ com } k_2 \in \mathbb{Z}.$$

Então,

$$X = 11(17k_2 + 9) + 3$$

$$= 187k_2 + 102.$$

Pelo Teorema Chinês dos Restos, segue que

$$119^{23} \equiv 102 \; mod \; 187.$$

Utilizando raciocínio análogo nos demais blocos, conclui-se que:

- $70^{23} \equiv 9 \; mod \; 187$
- $84^{23} \equiv 101 \; mod \; 187$
- $177^{23} \equiv 12 \; mod \; 187$
- $119^{23} \equiv 102 \; mod \; 187$
- $61^{23} \equiv 73 \; mod \; 187$

- $105^{23} \equiv 62\ mod\ 187$
- $17^{23} \equiv 51\ mod\ 187$
- $15^{23} \equiv 42\ mod\ 187$
- $163^{23} \equiv 124\ mod\ 187$
- $9^{23} \equiv 36\ mod\ 187$
- $98^{23} \equiv 21\ mod\ 187$
- $65^{23} \equiv 142\ mod\ 187$
- $91^{23} \equiv 82\ mod\ 187$
- $70^{23} \equiv 9\ mod\ 187$
- $108^{23} \equiv 14\ mod\ 187$

Etapa 8

Para que seja concluída a última etapa, deve-se juntar os blocos formados na etapa anterior, de modo que formem uma grande lista de números. Feito isso, basta que converter novamente os números em letras com o auxílio da tabela 7.

Sequência numérica formada: $\mathbf{10291012102736251421243621142829 14}$

Usando a correspondência alfabeto-numérica da tabela 7, formada por associações de números de dois algarismos a letras, obtém-se a mensagem

**“ATACAR PELO LESTE”**.

### 3.2. Funcionamento do método RSA

O funcionamento do método RSA consiste em demonstrar que ao decodificar uma mensagem, esta deve retornar ao seu formato original. Se o fato ocorrer sempre, é garantido que o método é válido, caso contrário, o algoritmo é falho e sem sentido.

O objetivo, nesta seção, é garantir o funcionamento do método, ou seja, mostrar que para cada bloco codificado $C(b)$ e cada bloco decodificado $D(a)$, aplicando o processo de decodificação em um determinado bloco codificado, obtém-se o bloco correspondente da mensagem original, ou seja, $D\big(C(b)\big) = b$.

**Demonstração:** Sejam $C(b)$ os blocos codificados e $D(a)$ os blocos decodificados, tem-se que os blocos podem ser calculados, respectivamente, pelas relações $b^k \equiv C(b)\ mod\ n$ e $a^d \equiv D(a)\ mod\ n$. Assim, para decodificar uma mensagem codificada, é feito: $D\big(C(b)\big) \equiv\ C(b)^d \equiv b^{kd} mod\ n$. Como $d$ é o inverso de $k$ modulo $\phi(n)$, tem-se que $d \cdot k \equiv 1\ mod\ \phi(n)$, ou seja, $d \cdot k = 1 + t\phi(n)$, em que $t$ é um inteiro. Então, conclui-se que $D\big(C(b)\big) \equiv\ C(b)^d \equiv (b^k)^d \equiv\ b^{kd} \equiv b^{1\ +\ t\phi(n)} \equiv b \cdot \big(b^{\phi(n)}\big)^t mod\ n$. Da relação $n = p \cdot q$, segue que $\phi(n) =\ \phi(p \cdot q) = (p-1) \cdot (q-1)$, o que implica que $D\big(C(b)\big) \equiv\ \big(b^{(p-1)}\big)^{(q-1)\cdot t} \cdot b\ mod\ n$. Se $p$ não divide $b$, aplicando o Pequeno Teorema de Fermat, $b^{p-1} \equiv 1\ mod\ p$, obtém-se $b^{kd} \equiv b\ mod\ p$, ou seja, $D\big(C(b)\big) \equiv b\ mod\ p$. No entanto, se $p$ divide $b$, segue que $b \equiv 0\ mod\ p$, ou seja, $\big(b^{(p-1)}\big)^{(q-1)\cdot t} \cdot b\ \equiv 0\ mod\ p$. De forma análoga, também pode ser mostrado que $D\big(C(b)\big) \equiv b\ mod\ q$ e como $p$ e $q$ são primos, é garantido que $mdc\ (p, q) = 1$, sendo que $pq$ divide $b^{kd} - b$. Como $n = p \cdot q$, conclui-se que $D\big(C(b)\big) \equiv b\ mod\ n$. Assim, $D\big(C(b)\big) = b$, o que assegura o funcionamento do método.

### 3.3. Segurança do método RSA

Na seção anterior, foi mostrado que o método RSA realmente funciona, amparado por condições e conceitos garantidos pela Teoria dos Números. O objetivo agora é garantir a segurança do método, visto que é amplamente usado nos mais variados tipos de operações sigilosas e transações financeiras no mundo todo.

A segurança do método consiste no fato de que o codificador dos dados tem acesso apenas a chave pública ($n$ e $k$), enquanto que para decodificar os dados é necessário conhecer a chave privada ($n$ e $d$), ou seja, o RSA se torna extremamente seguro devido à grande dificuldade em calcular $d$ conhecendo apenas $n$ e $k$, dificuldade esta que será melhor explicada a seguir.

Tomando $p$ e $q$ como os parâmetros do sistema usado para aplicar o algoritmo RSA, com $p$ e $q$ primos e seja $n = p \cdot q$, a chave pública precisa de um inteiro $k$ primo com $\phi(n) = (p-1) \cdot (q-1)$, ou seja, $mdc\big(k, \phi(n)\big) = 1$. Assim, o par $(n, k)$, representará a chave de codificação (chave pública). Já a chave privada irá depender

de um inteiro $d$, tal que $d \cdot k \equiv 1 \, mod \, \phi(n)$. O par $(n, d)$ representará a chave de decodificação (chave privada). Portanto, o RSA só será seguro se for difícil calcular $d$ a partir de $n$ e de $k$. Para calcular $d$ é preciso ter $k$ e $\phi(n)$. O valor $\phi(n)$, em contrapartida, só pode ser obtido se for possível fatorar $n$ obtendo $p$ e $q$. Dessa maneira, um indivíduo que detenha $n$ precisaria apenas saber sua fatoração, descobrir $p$ e $q$, e em seguida obter $d$. Sabendo $d$ e aplicando a receita para decodificar uma mensagem mostrada em $3.1$, o indivíduo poderá reconstruir e ler a mensagem original. Analisando o que foi descrito, parece muito simples desvendar uma criptografia RSA, no entanto, na prática é praticamente impossível. O grande entrave do algoritmo acontece devido a escolha de números primos muito grandes, gerando um número $n$ ainda maior, e reside no fato de que não existem algoritmos e nem computadores com tecnologia suficiente que permitam fatorar um inteiro $n$ tão grande. Não pode-se esquecer que, na tabela $6$ também mostrada na seção 3.1 deste mesmo capítulo, foi visto que o tempo necessário para fatorar um número de aproximadamente cem algarismos, pelo método usual das tentativas, é enorme.

Logo, a constatação feita é sólida, pois não existe, até os dias atuais, nenhum método eficiente capaz de fatorar inteiros muito grandes. A fim de melhor compreender a situação, segue um relato de Coutinho (2015, p. 158):

> "... atualmente, as implementações comerciais do RSA usam chaves públicas com cerca de 200 algarismos, mas algumas destas implementações chegam a permitir chaves públicas com até 2467 algarismos.
>
> Durante algum tempo, o RSA Laboratory, que pertence à empresa que detém os direitos do sistema de codificação RSA, lançou desafios, que consistiam de uma possível chave pública de RSA que deveria ser fatorada.
>
> A última destas chaves a ser fatorada tem 193 algarismos e corresponde ao produto dos primos
>
> 1634733645809253848443133883865090859841783670033 0923121811108523893331001045081512121181675115 79
>
> e
>
> 1900871281664822113126851573935413975471896789968 5154936666385390880271038021044989571912614655 71.

> A fatoração foi finalizada em novembro de 2005 por F. Bahr, M. Boehm, J. Franke e T. Kleinjung no Escritório Federal de Segurança de Informação da Alemanha. Os cálculos utilizaram 80 computadores de 2.2 GHz cada um e, mesmo assim, foram necessários 5 meses para completar as contas!".

Portanto, feita uma boa escolha de primos $p$ e $q$, grandes o suficiente, a segurança do RSA é garantida pela impossibilidade e também pela inexistência de métodos eficazes para a fatoração de um número composto $n$, obtido por $n = p \cdot q$. Mesmo se fossem usados vários computadores, como no exemplo relatado acima, a decodificação continuaria sendo muito lenta e ainda se esbarraria no alto custo tecnológico.

# CONSIDERAÇÕES FINAIS

Todo o trabalho teve como principal objetivo mostrar a matemática de forma mais atrativa, com intuito de despertar entusiasmo e interesse por parte dos educandos. Para despertar tal interesse, fez-se o uso da criptografia em sala de aula como ferramenta capaz de possibilitar aos alunos a fixação de conteúdos matemáticos importantes presentes nas matrizes curriculares das mais variadas unidades didáticas, no caso, funções afins e matrizes.

Além da fixação de conteúdos, também foi possível trabalhar a criptografia de forma intuitiva, desenvolvendo outras potencialidades importantes, tais como: o raciocínio lógico, o cooperativismo em grupo e a autonomia durante o desenvolvimento da elaboração e da resolução dos exercícios.

Todas as atividades propostas nos capítulos $1$ e $2$ foram desenvolvidas durante vinte aulas de $50$ minutos, com um grupo de vinte alunos que cursam $2º$ e $3º$ anos do Ensino Médio. As atividades foram realizadas no contraturno do horário de aulas dos educandos com o aval da direção pedagógica da escola.

Os objetivos foram alcançados de forma muito satisfatória, superando até mesmo as expectativas do docente. Sendo assim, logrou-se êxito na fixação dos conteúdos abordados e no desenvolvimento das potencialidades buscadas. Os alunos mostraram muito entusiasmo, interesse e empenho, sendo importante ressaltar que não houve se quer uma única desistência. Uma das maiores motivações relatadas pelos próprios alunos foi o fato de se sentirem protagonistas durante todo o processo. Além disso, também relataram que o bom relacionamento com o professor e a vontade de contribuírem com a conclusão do projeto foi relevante.

O capítulo $3$ foi elaborado com os mesmos propósitos, no entanto, como uma sugestão para ser aplicada no ensino superior. Dessa maneira, a criptografia também foi tratada como ferramenta para fixação de conteúdos presentes nesta etapa do ensino, especificamente aos abordados no campo da Teoria dos Números. A proposta objetivou tornar o ensino da Teoria do Números mais atrativo e também acabou contribuindo para o aperfeiçoamento do docente em tal área de conhecimento.

Portanto, um dos principais focos no processo de ensino-aprendizagem deve ser exatamente atrelar os conteúdos previstos nas matrizes curriculares das escolas e universidades com assuntos do interesse do aluno. Assuntos desconexos em que educandos não enxergam sua importância e aplicabilidade são desinteressantes e desestimulam a tentativa de adquirirem novos conhecimentos, pois dificilmente estão dispostos a buscar potencialidades meramente didáticas e dotadas de conteúdos que estão em descompasso com a realidade em que estão inseridos. Neste caso, cabe sempre ao professor juntamente com a instituição de ensino em que leciona buscar ferramentas para tornar tal procedimento viável.

## REFERÊNCIAS

[ 1 ] COUTINHO, Severino. **Criptografia**. Rio de Janeiro, IMPA, 2015.

[ 2 ] COUTINHO, Severino. **Números inteiros e criptografia RSA**. Coleção Matemática e Aplicações, Rio de Janeiro, IMPA, 2013.

[ 3 ] GOODRICH, M. T.; TAMASSIA, Roberto. **Projeto de Algoritmos**. São Paulo: Bookman, 2004.

[ 4 ] MENEZES, Luis Carlos. **O aprendizado do trabalho em grupo**. Disponível em: <https://novaescola.org.br/conteudo/605/o-aprendizado-do-trabalho-em-grupo/2009/05>. Acesso em 26 ago. 2019.

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

[ 6 ] SPINA, André Vinícius. **Números primos e criptografia.** Dissertação (Mestrado Profissional em Matemática) UNICAMP, Campinas, 2014.

[ 7 ] TAMAROZZI, Antônio Carlos. **Codificando e decifrando mensagens**. Revista do Professor de Matemática 45*,* São Paulo: Sociedade Brasileira de Matemática, 2001. p. 41-47.

[ 8 ] TERADA, R. **Criptografia e a importância das suas aplicações**. Revista do Professor de matemática, volume 12. SBM, p. 1-8, 1988.