Universidade Estadual do Sudoeste da Bahia
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Ana Lourdes Moreno Rodrigues Silva

A criptografia como estímulo à aprendizagem matemática

Vitória da Conquista
2021

Ana Lourdes Moreno Rodrigues Silva

A CRIPTOGRAFIA COMO ESTÍMULO À APRENDIZAGEM MATEMÁTICA

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Estadual do Sudoeste da Bahia - UESB, como requisito necessário para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Fernando dos Santos Silva

Vitória da Conquista
2021

S578c Silva, Ana Lourdes Moreno Rodrigues.
A criptografía como estimulo à aprendizagem matemática. /
Ana Lourdes Moreno Rodrigues Silva, 2021.
168f. il.
Orientador (a): Dr. Fernando dos Santos Silva.
Dissertação (mestrado) – Universidade Estadual do Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Vitória da Conquista - BA, 2021.
Inclui referências. 125 - 127.
1. Criptografia – Ensino de matemática. 2. Matemática - Funções. 3. Matemática na educação básica. I. Silva, Fernando dos Santos. II. Universidade Estadual Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Vitória da Conquista, III. T.

CDD: 510

Catalogação na fonte: Juliana Teixeira de Assunção-CRB 5/1890

Ana Lourdes Moreno Rodrigues Silva

A criptografia como estímulo à aprendizagem matemática

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Estadual do Sudoeste da Bahia – UESB, como requisito necessário para obtenção do grau de Mestre em Matemática.

BANCA EXAMINADORA

Prof. Dr. Fernando dos Santos Silva– UESB

Prof. Dr. Júlio César dos Reis – UESB

Prof. Dr. Alcindo Teles Galvão– UFAL

Vitória da Conquista – Ba, 17 de dezembro de 2021

Agradecimentos

Meus primeiros agradecimentos são dirigidos ao Mestre dos mestres, Deus, pelo fortalecimento espiritual e companhia constante.

Aos meus pais ARLINDO E ADETINA pelos muitos sacrifícios para oferecer uma educação melhor aos filhos. MUITO OBRIGADA pelo incentivo e por acreditar na minha capacidade de ser e fazer o que quiser.

Ao meu filho BRUNO, minhas filhas LAIANA e JÉSSICA e meu esposo AVANILDO, pela parceria de sempre e o entendimento da minha ausência para assistir às aulas do curso ou reclusão para estudos. Vocês preenchem a minha vida e meu amor por cada um é infinito e incondicional.

Aos meus irmãos ADNEUSA, ADILSON, ADILMA, ALESSANDRA e ARLENE, sinto muito grata por tê-los em minha vida.

Aos amigos (as) e colegas de trabalho, pelo incentivo de sempre.

Aos meus alunos do 9º ano A e B, participantes dessa pesquisa, pela disponibilidade e pelo trabalho que realizamos juntos numa troca recíproca de saber e aprendizagem.

Aos meus maravilhosos colegas do PROFMAT, em especial aos que se tornaram amigos: Alex, Adilton, Ana Dolores, Cassislane, Carol, Eduardo, José Brilhante, Marcos, Ricardo e Rodrigo , obrigada pela companhia em todos os momentos que compartilhamos juntos, presenciais e remotos.

Meus professores admiráveis: SÉRGIO, FLAULLES, ANDRÉ, FERNANDO, ROBERTO, ALEXSANDRA e MÁRCIO que bom encontrar com vocês! O compartilhar de conhecimento será de grande valia para minha vida pessoal e profissional.

Abro parênteses para me reportar ao meu orientador, Professor Doutor Fernando, foram momentos de agonia, tensão, resiliência, dedicação, companheirismo, estímulo, compreensão, amizade. Como agradecer a tudo isso? O meu MUITO OBRIGADA por tudo.

Gratidão a minha filha LAIANA pelas correções realizadas.

Aos membros da banca examinadora, pelo tempo dispendido na leitura deste trabalho e pelas importantes sugestões apontadas.

Por fim, sabemos o quanto é difícil para um professor continuar a vida acadêmica, principalmente, quando a Universidade dista cerca de 400 km

da cidade de moradia. Logo, meu MUITO OBRIGADA à CAPES pelo apoio financeiro e pela oportunidade de obter o título de MESTRA há muito desejado.

Resumo

A criptografia está presente no nosso cotidiano e constitui ferramenta essencial para conferir segurança e confidencialidade na transmissão e depósito de informações, tendo como base saberes e procedimentos matemáticos. Dessa forma, é um tema que pode contextualizar o processo de ensino e aprendizagem, despertando no estudante o interesse para compreender os conhecimentos matemáticos relacionados com cada método de criptografia abordado. Assim, esse trabalho teve por objetivo: analisar o potencial da criptografia para estimular a aprendizagem do conceito de função nos estudantes dos 9º ano A e B do Colégio Municipal X. Para isso, foram delineados objetivos específicos que orientaram: a apresentação do contexto histórico da criptografia, a análise de pesquisas sobre o tema, o estudo de conceitos matemáticos necessários para compreensão da cifra de César e do sistema RSA, a elaboração e realização de uma intervenção para trabalhar criptografia e função. A pesquisa teve caráter qualitativo e utilizou como metodologia de ensino a Sala de Aula Invertida, que somada aos recursos digitais selecionados, contribuíram para uma avaliação positiva das atividades realizadas. A intervenção foi feita de forma remota, em virtude da pandemia da COVID-19, sendo organizada por meio de cinco planos de aula, estruturados conforme a metodologia adotada, com atividades diversificadas que foram disponibilizadas através do *Classroom*, grupos de *Whatsapp* e *Google Meet*, ferramenta utilizada para realização dos encontros síncronos. Os dados necessários a pesquisa foram coletados por meio de questionários e da observação e análise das atividades realizadas pelos discentes. Os resultados mostraram a participação ativa e um bom desempenho dos estudantes nas tarefas solicitadas, afirmando o potencial da criptografia para estimular a aprendizagem do conceito de função.

Palavras-chave: Criptografia. Matemática. Função.

Abstract

Encryption is present in our daily lives and is an essential tool to ensure security and confidentiality in the transmission and deposit of information, based on mathematical knowledge and procedures. Thus, it is a theme that can contextualize the teaching and learning process, awakening in the student the interest to understand the mathematical knowledge related to each cryptography method discussed. Thus, this work aimed to: analyze the potential of cryptography to stimulate the learning of the concept of function in 9th grade A and B students at Municipal X school. For this, specific objectives were outlined that guided: the presentation of the historical context of cryptography, the analysis of research on the subject, the study of mathematical concepts necessary to understand the Caesar cipher and the RSA system, the elaboration and execution of an intervention to work on cryptography and function. The research was qualitative in nature and used the Inverted Classroom as a teaching methodology, which added to the selected digital resources, contributed to a positive evaluation of the activities carried out. The intervention was carried out remotely, due to the COVID-19 pandemic, being organized through five lesson plans, structured according to the adopted methodology, with diversified activities that were made available through Classroom, Whatsapp groups and Google Meet, tool used to carry out synchronous encounters. The necessary data for the research were collected through questionnaires and the observation and analysis of the activities performed by the students. The results showed the active participation and good performance of students in the requested tasks, affirming the potential of cryptography to stimulate the learning of the function concept.

Keywords: Cryptography. Math. function.

Lista de Figuras

Sumário

Introdução

A matemática faz parte da minha história de vida e me faz rememorar vivências que antecedem a fase da educação formal. Em casa, somos seis irmãos e nossos pais, em meio as suas dificuldades e antes mesmo de nos enviar para a escola, se preocupavam em nos alfabetizar. As cobranças não se limitavam a aprender a ler as letras e as palavras do "ABC", cartilha que recebíamos como auxílio, mas também precisávamos aprender a tabuada que seria questionada a noite, sentada em volta de uma mesa sob a luz do velho lampião. Eram processos mecânicos, sem muita contextualização e didática, porque nossos primeiros alfabetizadores só haviam concluído o estágio, que conhecemos hoje como anos iniciais do Ensino Fundamental. No entanto, ainda nessa época, comecei a tomar gosto pela matemática e me lembro da satisfação do meu pai quando aprendi as horas no relógio analógico, me recompensando com um pequeno "oriente". No colégio, se tornou minha disciplina preferida e, mesmo sem formação específica, iniciei a profissão docente lecionando na área.

Enquanto professora reproduzi muito do que aprendi por meio do método tradicional e também me questionava sobre a necessidade de aprender alguns conteúdos que faziam parte do currículo do Ensino Fundamental. Não havia muito preocupação com a contextualização e com a aprendizagem de todos alunos. No curso de pedagogia obtive muitas respostas sobre o processo de ensino aprendizagem e pude refletir sobre a minha prática docente, mudando muito da didática que utilizava. Entretanto, sentia necessidade de melhorar minha experiência na área de matemática, por isso, busquei formações a distância para conciliar trabalho e estudo. Após graduação e especialização, enveredei para o PROFMAT, onde pude sistematizar saberes e compreender de forma, mais efetiva, a construção do conhecimento matemático ao longo da história da humanidade.

Reflito sobre minhas experiências para tentar entender a relação dos meus alunos com o conhecimento matemático. Conforme veremos neste trabalho, eles percebem a presença da matemática no seu cotidiano e sabem de sua importância, mas ainda há aversão pelo fato da disciplina envolver muitos cálculos e regras. Essa falta de empatia pode estar relacionada a abordagens descontextualizadas, nas quais os estudantes não conseguem perceber a aplicabilidade do conteúdo. Segundo Bahia (2019):

> ...cada escola deve ser suficientemente flexível para contemplar os estudantes de diferentes níveis de habilidade e deve espelhar- se em

> suas necessidades – entre estas figuram experiências matemáticas significativas e interessantes sobre outras áreas de aprendizagem. Além disso, deve oportunizar a compreensão da necessidade de continuarem estudando Matemática além dos muros da escola; e uma formação como sujeitos alfabetizados matematicamente, capazes de fazer uso social das habilidades e competências construídas no Ensino Fundamental (BAHIA, 2019, p. 335).

Dessa maneira, cabe a nós professores o desenvolvimento de atividades que favoreçam o letramento matemático, isto é, as competências e habilidades "de raciocinar, representar, comunicar e argumentar matematicamente"(BAHIA, 2019, p. 338), favorecendo a elaboração e resolução de problemas em diferentes contextos a partir do uso de conceitos, procedimentos, fatos e ferramentas da área (BAHIA, 2019).

Diante desse desafio, percebi que a criptografia poderia contribuir para o desenvolvimento das competências e habilidades elencadas, visto que faz parte do nosso cotidiano e utiliza procedimentos e ferramentas matemáticas. Assim, aliei esse fato ao meu interesse em compreender melhor o sistema RSA, surgindo o seguinte questionamento: a criptografia pode estimular à aprendizagem matemática? Um dos conteúdos planejados para trabalhar com as turmas pesquisadas seria o conceito de função, então direcionei essa inquietação para esse tema.

A criptografia é o estudo de métodos para ocultar o conteúdo de mensagens, tornando as informações incompreensíveis para pessoas não autorizadas. Faz parte da história da humanidade e atualmente, está presente em diversas situações: senhas, compras e mensagens pela internet, cartões, aplicativos, tudo que precisa ser mantido em segredo. Portanto, está relacionada às necessidades da sociedade, atrelada ao desenvolvimento tecnológico.

A busca por sistemas criptográficos mais resistentes aos ataques da criptoanálise, desenvolvimento de métodos para decifrar mensagens, deu origem a diversos tipos de cifras até chegar nas que utilizamos hoje, com algoritmos e chaves baseados em procedimentos matemáticos que conferem maior segurança na troca ou depósito de informações.

Apesar de estar presente em inúmeras atividades cotidianas, muitos de nós não sabemos o que é a criptografia, nem os procedimentos e conhecimentos matemáticos utilizados para conceder segurança as mensagens e dados. Dessa forma, julgamos que a abordagem de funções a partir da criptografia poderia despertar o interesse nos estudantes para o estudo desse conteúdo. Assim, a pesquisa desenvolvida teve como objetivo geral: "analisar o potencial da criptografia para estimular a aprendizagem do conceito de função nos estudantes dos 9º ano A e B do Colégio Municipal X".

Fundamentados no objetivo geral, elencamos os seguintes objetivos específicos:

- Apresentar os fundamentos da criptografia e sua evolução histórica, abordando métodos clássicos e modernos;

- Explorar conceitos matemáticos relacionados a criptografia;
- Desenvolver e aplicar uma intervenção para trabalhar função a partir da criptografia;
- Analisar os dados da intervenção para verificar se o objetivo geral foi alcançado.

Para o estudo e fundamentação teórica, tivemos como principais referências: Singh (2020), Cimino (2018), Coutinho (2005), Hefez (2005) e Shokranian (2012), somadas aos autores de artigos e dissertações analisadas no segundo capítulo, que muito contribuíram para o desenvolvimento da intervenção.

O trabalho teve caráter qualitativo, sendo utilizado questionários, observações e realização de atividades pedagógicas para a coleta de dados, cujos resultados foram analisados por meio de gráficos e discussões. A pesquisa foi aplicada nos anos finais do Ensino Fundamental, em duas turmas do 9º ano de um colégio municipal X da sede de uma cidade do interior baiano, localizada na mesorregião do Centro-Sul. Escolhemos essas turmas, porque sou professora de matemática em ambas, e isso facilitaria o desenvolvimento da intervenção durante a pandemia da COVID-19, uma vez que fomos submetidos ao isolamento social, devido aos números elevados de contágio e ao grau de letalidade da doença.

Em consequência do isolamento social, a instituição ainda estava desenvolvendo as atividades pedagógicas de forma remota, utilizando grupos de *Whatsapp*, *Google Meet* e *Classroom* com alunos que tinham acesso a internet em casa. Para alunos sem esse meio e outros recursos, eram entregues atividades impressas. Diante disso, optamos por aplicar a intervenção somente com aqueles que tinham acesso aos meios necessários para realização de tarefas síncronas e assíncronas, além disso, os estudantes com atividades impressas eram acompanhados por outros docentes.

Como metodologia de ensino escolhemos a Sala de Aula Invertida, na qual como atividade pré-classe os participantes estudavam o conteúdo teórico através de materiais - vídeos, filmes, textos e jogos - disponibilizados no *Classroom*. Eles também deveriam fazer anotações para que pudessem participar ativamente das discussões e atividades colaborativas realizadas por meio do *Google Meet*. Assim, essa opção pode ser justificada pelo fato de podermos aproveitar melhor os momentos síncronos com atividades mais interativas, ao invés de exposições teóricas.

O trabalho está dividido em seis capítulos, a saber:

No capítulo 1 apresentamos os fundamentos e um resumo histórico da criptografia, elecando a esteganografia, algumas cifras de substituição e transposição clássicas e modernas.

Empreendemos no capítulo 2, uma análise de trabalhos que apresentam a criptografia como proposta para contextualizar e estimular a aprendizagem de conteúdos matemáticos na Educação Básica, descrevendo suas aplicações para a sala de aula.

Já no capítulo 3 exploramos conceitos matemáticos necessários para compreensão da cifra de César e do RSA, abordados no capítulo 1 e que foram trabalhados na intervenção.

No capítulo 4 justificamos a escolha pela pesquisa qualitativa, descrevendo o contexto no qual seria aplicada. Também apresentamos a Sala de Aula Invertida (SAI) como metodologia de ensino e a organização da intervenção por meio de cinco planos de aula.

Já no capítulo 5, tabulamos as informações coletadas nos questionários de investigação e procedemos a descrição e análise das produções dos alunos.

Por fim, apresentamos as considerações finais sobre todo o trabalho realizado, revelando que a criptografia pode contextualizar e estimular à aprendizagem do conceito de função.

Logo após as referências, serão disponibilizados os planos de aula e as atividades aplicadas para que possam subsidiar a prática pedagógica de outros docentes.

Para finalizar essa parte introdutória, apresentamos o mapa mental de todo o trabalho para que o leitor possa, de forma resumida e esquematizada, ter uma visão geral de como os conceitos e ideias estão relacionados. Do primeiro ao quinto capítulo, expomos parte desse esquema, favorecendo a compreensão do que foi abordado em cada um deles.

Figura 1: Mapa Mental Completo

Fonte: Elaboração da autora.

1 Criptografia: Conceitos e História

A necessidade de proteger informações, armazenadas e transmitidas, motivou o desenvolvimento de técnicas, códigos e cifras para camuflar e/ou modificar mensagens, de forma que somente o destinatário pudesse ler seu conteúdo. Conforme as informações foram se tornando mais valiosas, criaram-se departamentos para elaborar sistemas criptográficos mais resistentes aos ataques dos criptoanalistas, intelectuais que se dedicam a decifração de códigos e cifras.

No decorrer deste capítulo apresentaremos conceitos relacionados a criptografia e uma síntese histórica relatando técnicas utilizadas pelos povos para prover segurança a documentos e ao processo de comunicação. Também abordaremos sistemas modernos de criptografia.

1.1 Conceitos iniciais

A comunicação é essencial para o convívio social, sendo uma necessidade inerente ao ser humano. Por meio dela, pode-se expressar sentimentos e vontades, além de adquirir, preservar e difundir conhecimentos. Nos seus primórdios, utilizava-se a linguagem gestual e sons guturais, até a descoberta da escrita, que segundo os historiadores, surgiu por volta de 4000 a.C., marcando a passagem do período conhecido como Pré-história para a História.

O advento da escrita contribuiu para que povos e nações começassem a ter acesso a um número crescente de informações veiculadas, inicialmente, por meio de ilustrações, símbolos e escrita própria, passando por grandes invenções como o jornal, o rádio, a televisão e o telefone, até chegar ao computador, meios móveis e internet. Esses últimos, imprescindíveis para a troca de informações na sociedade atual.

Com a evolução dos meios para troca de informações, emerge a necessidade de criar mecanismos que garantam a segurança dos dados, evitando o acesso de pessoas não autorizadas. Dessa forma, começa-se a utilização de mensagens secretas, principalmente na esfera política, militar e econômica. O objetivo era revelar o conteúdo da mensagem somente ao destinatário.

Se no passado, a segurança no processo comunicativo era importante, atualmente, com o uso da internet e comunicação instantânea, ela se torna essencial contra falsificação, destruição e interceptação de informações. Sendo valoroso tanto para empresas e governos quanto para indivíduos, devido a dependência dos meios eletrônicos para armazenamento

de dados e alto grau de conectividade entre os sistemas informatizados.

Uma das primeiras formas de agregar segurança ao processo comunicativo refere-se a esteganografia, palavra derivada do grego: *steganos* - coberto e *grafia* - escrita. Consiste numa técnica para esconder, camuflar a informação por meio de processos físico e/ou químicos.

Costa e Figueiredo (2010), citam alguns contos do historiador grego Heródoto envolvendo esteganografia. Como, a de um certo grego que para transmitir uma mensagem secretamente, raspa o cabelo do mensageiro e tatua a mensagem na cabeça raspada, sendo transmitida assim que o cabelo crescesse e revelada ao destinatário quando raspasse novamente o cabelo. Também, relata que um grego, vivendo em solo persa, transmite uma mensagem secreta escrita em tábua de madeira e coberta em cera, alertando os gregos sobre os planos persas para invadir e conquistar a Grécia.

Durante a Segunda Guerra Mundial, os alemães transmitiam mensagens usando técnicas de fotografia para microfilmar o texto, reduzindo a um ponto, o qual era colocado como ponto final em uma correspondência com assunto não suspeito. Para ter acesso ao conteúdo o destinatário procurava o ponto e ampliava.

Nos casos citados, a mensagem era escondida, mas caso fosse encontrada, seu conteúdo poderia ser lido por qualquer pessoa sem nenhum esforço. Isso mostra que a esteganografia, apesar de oferecer uma certa segurança, é vulnerável se a vigilância for rígida.

Aos mesmos passos do desenvolvimento da técnica supracitada, houve a evolução da criptografia, palavra advinda do grego, *kryptos* - secreto, e *grafia* – escrita. Seu objetivo é modificar a mensagem original por meio de processos sistematizados, a encriptação, tornando-a incompreensível para qualquer pessoa que não seja o receptor.

A criptografia é utilizada no dia-a-dia e nem sempre é percebida. Na troca de mensagens eletrônicas, nas redes sociais, nas transações eletrônicas, nas compras pela internet e nos vários aplicativos utilizados em computadores e celulares.

Mitani et al. (2007), descreve as seguintes etapas do processo de criptografia baseando-se no modelo de Shannon [1].

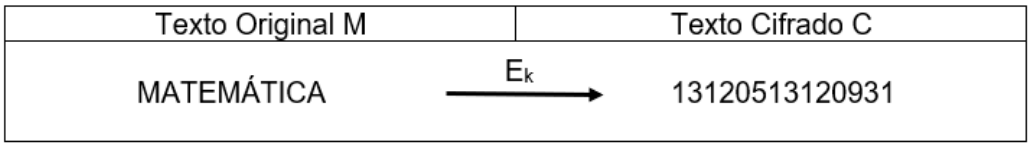
i) Inicialmente o remetente tem o texto original M, uma mensagem normal, sem criptografia. Ex.: MATEMÁTICA.

ii) Usando uma chave de criptografia E_k, esse texto é cifrado, tornando-o incompreensível para pessoas indesejadas.

iii) Ao receber a mensagem, o receptor usa uma chave de descriptografia D_k para restaurar o texto original.

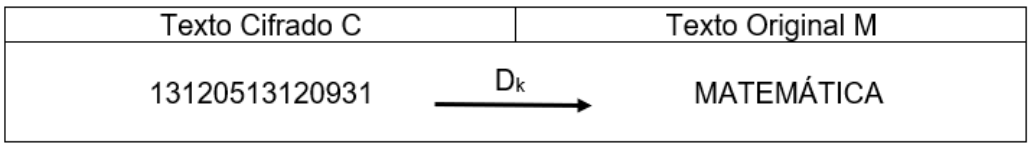
[1] Claude Shannon (1916-2001) foi um matemático inglês do século XX que ficou conhecido como o pai da teoria da informação. Ele difundiu o termo Bit e desenvolveu vários conceitos chaves para a criptografia.

Figura 1.1: Esquema de Criptografia



Fonte: Adaptado de Mitani et al. (2007, p. 20).

Figura 1.2: Esquema de Descriptografia



Fonte: Adaptado de Mitani et al. (2007, p. 20).

A chave de criptografia é o dado secreto do algoritmo de encriptação que o código utiliza para proteger o texto original. O algoritmo pode ser definido como uma série de operações numa sequência organizada para se resolver determinado problema. Como diz Santos (2013):

> Uma das formas de trocar mensagens criptografadas requer que transmissor e receptor conheçam o algoritmo utilizado para encriptar a mensagem e a chave utilizada. Algoritmo é um conjunto de procedimentos, em sequência organizada, para resolver determinado problema (SANTOS, 2013, p. 16).

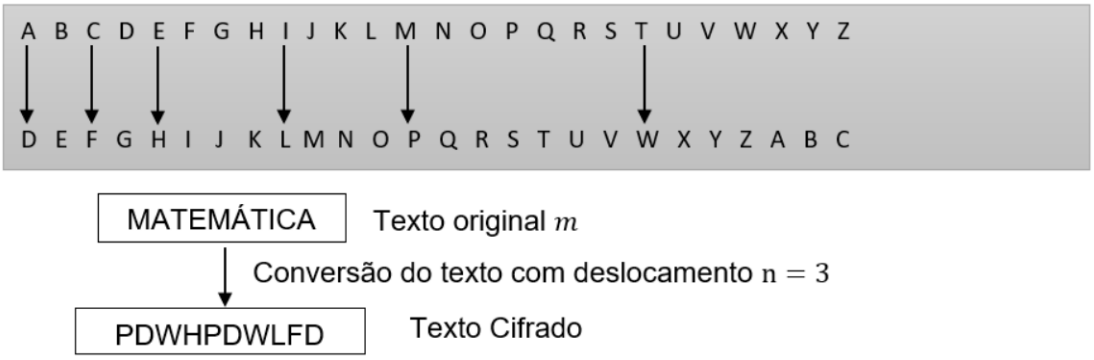
Ao longo da história, foram criados vários métodos de criptografia que, embora não sejam mais utilizados por questões de segurança, ainda são úteis para compreender como essa técnica funciona na prática. Veremos a seguir, que na etapa clássica, antes da ascensão do computador, as cifras eram baseadas em técnicas de substituição e transposição simples.

1.2 Cifras de substituição

As cifras de substituição têm por base a permutação das letras do alfabeto por outras, por símbolos ou por figuras, utilizando um padrão conhecido pelo receptor e destinatário. Um dos exemplos mais antigo é a Cifra de César que recebeu esse nome, pois foi usada pelo ditador romano Júlio César (100-44 a.C.), para comunicar-se com seus aliados, durante as guerras, sem o conhecimento dos inimigos.

"O Código de César é, na realidade, um caso particular do código de Substituição Monoalfabética, onde cada letra ou símbolo é substituído sempre por uma mesma letra ou símbolo" (FRANÇA, 2014, p. 24). Dessa forma, o algoritmo de criptografia, consiste no deslocamento de cada letra do texto original em n letras. Por exemplo, tomando $n = 3$, a palavra MATEMÁTICA seria criptografada conforme figura 1.3.

Figura 1.3: Cifragem da palavra MATEMÁTICA de acordo com o Código de César



Fonte: Adaptado de Mitani et al. (2007, p. 25).

Nessa versão, os caracteres de substituição são simplesmente o alfabeto deslocado em três posições, o que torna o espaço chave limitado a quantidade de letras do alfabeto. No caso de César, que utilizava o alfabeto romano, haveria apenas 22 chaves possíveis. No alfabeto latino seriam 26 chaves. Esse espaço poderia ser aumentado, se as letras fossem totalmente embaralhadas. Assim, cada letra do alfabeto seria substituída por qualquer outra, mas seria necessário que houvesse correspondência entre cada letra do texto simples e o caractere de substituição. Como diz Mitani et al. (2007):

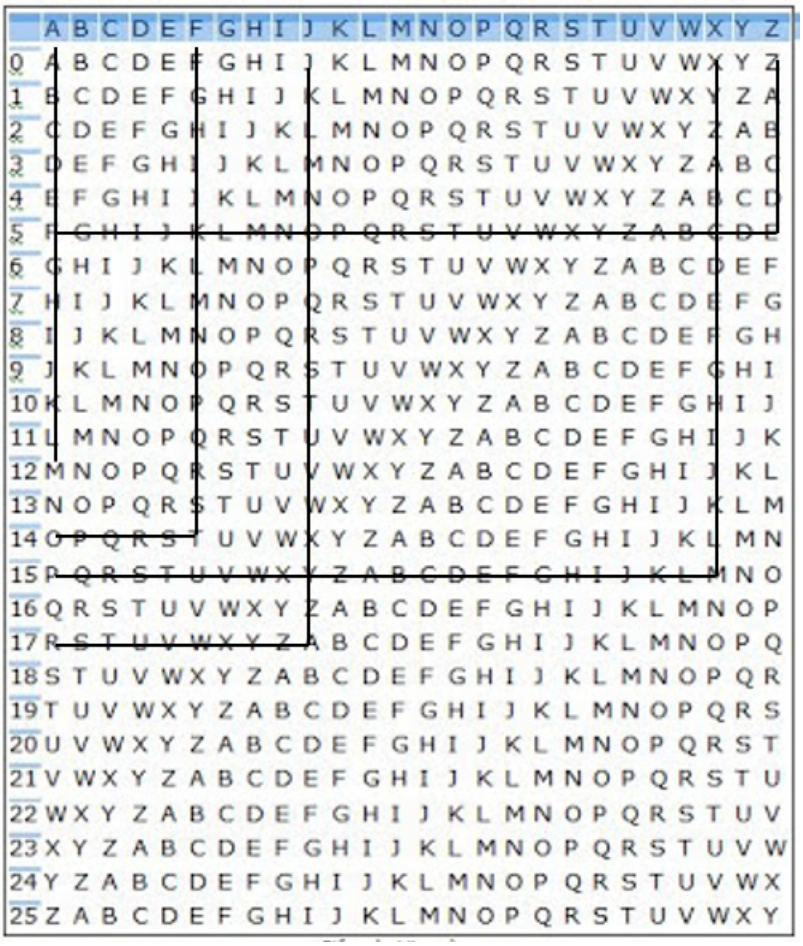
> ...Your plaintext letter would be the alphabet in order:
>
> ABCDEFGHIJKLMNOPQRSTUVWXYZ Then one exemple of a substitution with a scrambled alfhabet could be written out like this: QWERTYUIOPASDFGHJKLZXCVBNM (MITANI et al., 2007, p. 31).

A chave da cifra é o alfabeto embaralhado e, no caso do alfabeto com 26 letras, há 26! maneiras para se organizar esses caracteres para uma chave. Para a primeira letra, há 26 possibilidades, para a segunda 25 possibilidades, e assim por diante. Então, existe 26×25 possibilidades para as duas primeiras letras.

Entretanto, esses métodos são suscetíveis a um ataque criptográfico conhecido como análise de frequência, que pressupõe uma consistência entre a frequência das letras no texto original e a frequência das letras no texto cifrado. Por exemplo, a letra A aparece com mais frequência num texto em português, então se a letra P aparecer com mais frequência no texto cifrado, pode-se supor que são correspondentes. Uma forma de deixar a cifra de substituição mais segura, em relação aos ataques de análise de frequência, refere-se a polialfabética. Essa, também, é uma cifra de substituição e consiste no uso de dois ou mais alfabetos para criptografar um texto.

A cifra de substituição polialfabética surgiu com a necessidade de vencer os criptoanalistas e deixar a criptografia mais segura. Mas, conforme Ganassoli e Schankoski (2015),

Figura 1.4: Quadro de Vigenère



Fonte: Adaptado de https://efacildemais.blogspot.com/2011/08/. Acesso em 30/09/2020

isso só foi possível no século XVI quando o francês Blaise de Vigenère publicou a obra Traicté dés Chiffres, em 1586, a partir do trabalho de Leon Alberti, arquiteto italiano, considerado pai da cifra polialfabética. Assim, ele criou a cifra Le Chiffre Indechifrable, cujo significado é A Cifra Indecifrável, também chamada Cifra de Vigenère que usa 26 alfabetos diferentemente cifrados, conforme figura 1.4.

Na figura 1.4, observa-se 26 alfabetos cifrados de acordo com a Cifra de César, sendo um deles o original. Por meio deste quadro, o remetente poderá cifrar a primeira letra usando o segundo alfabeto, a segunda usando o vigésimo quinto, a terceira usando o décimo e assim por diante. Dessa forma, não seria eficiente os criptoanalistas usarem a análise de frequência das letras.

O destinatário precisa saber que linha do quadrado de Vigenère foi usada para cifrar cada letra que pode ser escrita de até 26 formas diferentes. Para não confundir a linha utilizada em cada letra, utiliza-se o alfabeto da primeira coluna para uma palavra-chave. Assim, cada letra do texto original corresponde ao alfabeto deslocado, situado na mesma linha da letra da palavra-chave, ordenadamente. Por exemplo, a palavra MATEMÁTICA cifrada com a palavra-chave PROFMAT, ficaria de acordo com a tabela 1.1.

Tabela 1.1: Exemplo da Cifra de Vigenère

PALAVRA-CHAVE	P	R	O	F	M	A	T	P	R	O
TEXTO ORIGINAL	M	A	T	E	M	Á	T	I	C	A
TEXTO CIFRADO	X	J	F	Z	A	A	A	T	M	M

Fonte: Elaboração da autora.

Acompanhando os traços feitos na figura 1.4, percebe-se que a letra M corresponde a letra X, no alfabeto começado com a letra P; a letra A corresponde a letra J, no alfabeto iniciado com a letra R; seguindo assim, até que todo o texto seja cifrado. De acordo com França (2014), essa cifra é resistente em relação a análise de frequência, visto que cada letra pode ser codificada de diferentes formas. Se forem usadas chaves mais longas e com poucas letras repetidas, a tarefa dos criptoanalistas fica mais complicada, pois quanto mais alfabetos se emprega, mais difícil será a criptoanálise.

Nessa época, o processo de criptografar era manual e trabalhoso, por isso, esse método mostrou-se pouco atraente e essa cifra ficou em desuso por mais de 200 anos.

> Foi quando criou-se a Cifra de Substituição Homofônica, na qual cada letra é substituída por uma variedade de símbolos proporcional à sua frequência. Por exemplo, a letra e na língua portuguesa poderá ser substituída por 12 símbolos distintos, pois sua frequência é de 12,57% ..., cada vez que a letra e for aparecer no texto cifrado, será escolhido ao acaso qual dos 12 símbolos usar, e assim ocorrendo com as demais letras, de modo que no final do texto, cada símbolo representará 1% do texto cifrado, despistando a técnica da análise da frequência (GANASSOLI; SCHANKOSKI, 2015, p. 14).

A Cifra de Substituição Homofônica, portanto, é uma cifra intermediária, pois representa mais segurança do que a monoalfabética e é mais fácil de usar do que a polialfabética. Entretanto, ao estudar as letras que apresentam um único símbolo para representá-la, dígrafos ou trígrafos usados comumente na língua, os criptoanalistas conseguiram quebrar essa cifra.

Com isso, a Cifra de Vigenère mostrou-se mais segura, sendo utilizada por mais de 100 anos, até que por volta de 1854, o matemático inglês Charles Babbage descreve um método para quebrá-la. Ele analisou em que frequência as letras se repetiam, descobrindo a palavra-chave usada. Porém, essa técnica só foi publicada em 1863 por Friedrich Kasiski. Diante disso, ficou evidente a vulnerabilidade das cifras de substituição e a necessidade dos criptógrafos buscarem cifras mais resistentes a criptoanálise.

1.3 Cifras de transposição

As cifras de transposição, usadas de forma paralela ao desenvolvimento das cifras de substituição, consistem em misturar as letras do texto original de acordo com uma

regra, ou seja, as letras são permutadas segundo um algoritmo e uma chave determinados. Assim, as letras são reorganizadas, gerando um anagrama. Para mensagens curtas é um método inseguro, porque as possibilidades para reorganizar as letras são muito limitadas. Entretanto, para uma palavra ou frases maiores torna-se eficaz, pois existem várias maneiras de arranjos.

Por exemplo, para palavra LUZ só existem seis anagramas: LUZ, ULZ, ZUL, UZL,ZLU LZU. Para a palavra ESCOLA existem 720 anagramas e para uma frase com 25 letras existem 25! rearranjos. Logo, quanto mais letras tiver a mensagem, maior será sua segurança. Se a transposição fosse feita sem nenhuma regra específica, a mensagem ficaria ainda mais segura, porém o destinatário não conseguiria decifrar o anagrama. Por isso, o sistema de rearranjo precisa ser previamente combinado em segredo, entre remetente e destinatário.

O Citale espartano, instrumento militar do século V a.C., foi um dos primeiros aparelhos de cifras de transposição. Também chamado Licurgo, trata-se de um bastão de madeira em volta do qual era enrolada uma tira de couro ou um pergaminho, como na Figura 1.5. Nessa técnica, a mensagem é escrita sobre o couro ao longo do comprimento do citale, depois desenrola o couro e envia ao destinatário. O mensageiro poderá utilizá-la como cinto, com as letras ocultas na face de dentro. Ao receber a mensagem, o destinatário deve enrolar a tira de couro num citale de mesmo diâmetro do que foi usado pelo remetente. Nesse caso, a chave seria o formato do bastão.

Figura 1.5: Citale Espartano

Fonte: <https://educalingo.com/pl/dic-pl/skytale>.

Outro método de cifra de transposição é a tabela espartana. Segundo Santos (2013) é descrito por Plutarco, em 90 d.C., no livro "Vida de Homens Ilustres". Consistia numa tabela comum, cuja chave de criptografia era o número de colunas, uma vez que o número de linhas dependeria do tamanho da mensagem escrita na tabela, uma letra em cada célula, da esquerda para direita e de cima para baixo (ou outra combinação). Para cifrar, considerava o texto em outro sentido ou direção. Como exemplo, veja na tabela 1.2, como ficaria o texto: "A criptografia como estímulo à aprendizagem matemática".

Tabela 1.2: Exemplo da Tabela Espartana

A	X	C	R	I	P
T	O	G	R	A	F
I	A	X	C	O	M
O	X	E	S	T	I
M	U	L	O	X	A
X	A	P	R	E	N
D	I	Z	A	G	E
M	X	M	A	T	E
M	A	T	I	C	A

Fonte: Elaboração da autora.

Nesse caso, utilizou-se a letra X no lugar do espaço, mas podem ser usadas letras aleatórias. Para tornar o texto cifrado, consideremos o texto escrito na tabela de cima para baixo, separando em blocos de cinco letras, como é usual:

ATIOM XDMMX OAXUA IXACG XELPZ MTRRC SORAA IIAOT TXEGT CPFMI ANEEA.

Quando o número de letras da tabela não for múltiplo de cinco, completa-se os blocos também com letras aleatórias. Costa (2014) cita um método similar chamado de transposição geométrica pelo fato de ter como base uma matriz retangular. "O texto original é escrito dentro da matriz no sentido das linhas, completando com X os espaços que sobram" (COSTA, 2014, p. 11). Observe na tabela 1.3 como fica o texto cifrado anteriormente.

Tabela 1.3: Exemplo de tranposição geométrica

A	C	R	I	P
T	O	G	R	A
F	I	A	C	O
M	O	E	S	T
I	M	U	L	O
A	A	P	R	E
N	D	I	Z	A
G	E	M	M	A
T	E	M	A	T
I	C	A	X	X

Fonte: Elaboração da autora.

A mensagem foi escrita numa matriz 5 por 10 e diferente do exemplo anterior, não se usa letras nos espaços. Em seguida, faz-se a matriz transposta, conforme a tabela 1.4.

Tabela 1.4: Exemplo de transposição geométrica - Matriz Transposta

A	T	F	M	I	A	N	G	T	I
C	O	I	0	M	A	D	E	E	C
R	G	A	E	U	P	I	M	M	A
I	R	C	S	L	R	Z	M	A	X
P	A	O	T	O	E	A	A	T	X

Fonte: Elaboração da autora.

Assim, o texto ininteligível será:

ATFMIANGTI COIOMADEEC RGAEUPIMMA IRCSLRZMAX PAOTOEAATX.

Para decodificá-lo basta fazer o processo inverso, escrevendo novamente a matriz dez por cinco.

Ao longo da história, foram criados outros métodos manuais de criptografia, seja de substituição, de transposição ou uma combinação de ambas, mas a criptoanálise já havia se configurado como ciência, quebrando todas as cifras desenvolvidas até então.

1.4 Mecanização da criptografia

Na busca por métodos mais resistente aos ataques dos criptoanalistas surgem, no início da idade moderna, os primeiros indícios da utilização de máquinas mecânicas no processo de criptografia. Segundo Santos (2013), em 1838, o americano Samuel Morse inventou o telégrafo eletromagnético e o código Morse, no qual as letras do alfabeto são substituídas por pontos e traços. Posteriormente, criou um receptor acústico, de modo que o destinatário ouvisse as letras através de bips.

Os militares começaram a utilizar o rádio para enviar mensagens através do código Morse. Todavia, a interceptação das mensagens também ficou mais fácil e, com isso, os criptoanalistas colecionaram vitórias na Primeira Guerra Mundial. Nessa mesma época, foi utilizada a cifra ADFGVX que combinava técnicas de substituição e transposição. Consistia num quadro 7×7 com as 6 letras ADFGVX na primeira linha e na primeira coluna, escrevendo as 26 letras do alfabeto e mais 10 dígitos aleatoriamente, conforme o exemplo da tabela 1.5.

Tabela 1.5: Exemplo de disposição da cifra ADFGVX

/	A	D	F	G	V	X
A	k	l	g	y	5	f
D	l	a	4	h	2	m
F	s	3	z	q	7	t
G	v	j	b	9	i	e
V	r	8	p	w	0	u
X	c	x	6	o	d	n

Fonte: Ganassoli e Schankoski (2015, p. 15).

As letras ADFGVX foram escolhidas por serem bem diferentes das utilizadas no código Morse. Para entender como funciona a cifra, consideremos a palavra MATEMÁTICA. Inicialmente, substitui-se cada letra pelas suas coordenadas na tabela, começando pela coluna e obtendo: XD DD XF XG XD DD XF VG AX DD. Após a técnica da substituição, é feita a transposição. Partindo de uma palavra chave (exemplo: tela) escrita num quadro, rescreve-se o texto cifrado: XD DD XF XG XD DD XF VG AX DD (tabela 1.6). Por fim, a palavra chave é arrumada em ordem alfabética, transpondo as colunas (tabela 1.7) e a mensagem cifrada final: DDDXGFXXDDD XGFVXDXDA é transmitida via rádio através do código Morse.

Tabela 1.6: Organização da cifra ADFGVX com a palavra chave

T	E	L	A
X	D	D	D
X	F	X	G
X	D	D	D
X	F	V	G
A	X	D	D

Fonte: Elaboração da autora.

Tabela 1.7: Transposição da Cifra ADFGVX

A	E	L	T
D	D	D	X
G	F	X	X
D	D	D	X
G	F	V	X
D	X	D	A

Fonte: Elaboração da autora.

De acordo com Santos (2013), a quebra dessa cifra foi essencial para evitar a invasão de Paris pelos alemães, na Primeira Guerra Mundial. Os alemães marchavam ofensivamente em direção a essa capital, desde o dia 21 de março de 1918 e após três meses, estavam há apenas 100 km do seu destino. Diante dessa situação, era vital para os franceses descobrir em qual ponto o inimigo iria atacar. Para isso, teriam que decifrar as mensagens trocadas entre os alemães que usavam o código ADFGVX. Após muitas tentativas, o criptoanalista Georges Pavin conseguiu quebrar a chave da cifra ADFGVX. Logo, todas as mensagens interceptadas puderam ser lidas, inclusive a que revelava onde seria o local do ataque. Dessa forma, o elemento surpresa foi eliminado e os alemães recuaram após cinco dias de batalha.

Nesse contexto, ficou evidente a necessidade de métodos de criptografia mais resistentes e, por isso, no final da primeira guerra mundial os cientistas começaram a desenvolver métodos e máquinas para tornar as chaves de criptografia mais seguras. Como cita Ganassoli e Schankoski (2015):

> ...então só no fim da Primeira Guerra Mundial, cientistas da América descobriram que se usassem uma frase-chave tão grande quanto o tamanho da mensagem que precisava ser enviada, a técnica de decifrar desenvolvida por Babbage e Kasiski não iria funcionar e assim começaram a desenvolver métodos e máquinas, com a tecnologia que dispunham na época, para aperfeiçoar cada vez mais as frases-chaves, até que fossem letras aleatórias, distribuídas em blocos de papel (GANASSOLI; SCHANKOSKI, 2015, p. 16).

Cimino (2018) também cita que quando os códigos dos alemães foram facilmente decifrados, recorreram ao processo mecânico: a máquina Enigma, construída e patenteada, em 23 de janeiro de 1918, pelo engenheiro elétrico Arthur Scherbius. Essa máquina era uma combinação de sistemas mecânicos e elétricos e seu segredo estava no uso de rotores que podiam oferecer protocolos diferentes, a cada combinação deles, aliados a técnica de substituição. As peças móveis da máquina mudavam de posição a cada vez que uma letra era pressionada, então se essa mesma letra fosse teclada, provavelmente teria uma cifra diferente. Com isso, evitaria a repetição de letras e garantiria imunidade aos métodos tradicionais de análise de frequência.

Parecida com uma máquina de escrever antiga, conforme figura 1.6, era composta de um teclado e um painel luminoso com as letras do alfabeto. Se fosse teclada, por exemplo, a letra "M", no painel acendia a letra correspondente que seria a codificação.

A Enigma que foi usada pelos alemães, na Segunda Guerra Mundial, era composta de cinco rotores numerados de 1 a 5, entre os quais eram escolhidos três que deveriam ser posicionados diariamente, conforme um livro de códigos que listava a chave diária. Cada rotor tinha 26 posições demarcadas por numeração e, na parte interna deles, havia um anel que também podia se deslocar 26 posições, era uma segunda forma de decodificar. Além

Figura 1.6: Máquina Enigma

Fonte: <https://www.proxxima.com.br/home/proxxima/how-to/2019/01/16/procuram-se-soldados-digitais.html>.

disso, havia um painel de plugues que conectavam duas letras através de fios elétricos que também deveriam ser mudados de posição diariamente. Sobre esse painel, Cimino (2018) explica:

> O exército alemão experimentou por pouco tempo uma máquina com oito rotores, mas optou por outra inovação: a instalação de um painel de conexão com 26 soquetes entre o teclado e o primeiro rotor. Pequenos cabos com plugues em cada ponta ligavam os pares. Se nada fosse ligado ao soquete equivalente ao A era passado como A. Mas, se A fosse ligado ao soquete equivalente a T, então T era enviado, enquanto T era enviado como A. Só isso produziria até duzentos milhões de milhões de possibilidades. Para impedir que a operação ficasse complicada demais, o exército conectava seis pares de letras, dando uma camada a mais de decodificação de doze letras. O resto era cifrado só pelos rotores (CIMINO, 2018, p. 97).

Esse autor ainda calcula o número de possibilidades totais para configurar a Enigma. Segundo ele, se fosse usada apenas uma máquina com três rotores, seria possível decifrar qualquer código no intervalo de tempo de um dia. Mas, esses rotores podiam ser removidos ou substituídos em qualquer ordem, elevando seis vezes as possibilidades para 105.456. Somando o painel de conexão que trocava os pares de seis letras das 26 letras, acrescentava mais 100.391.791.500 possibilidades. Portanto, havia no total cerca de 10.000.000.000.000.000 possíveis permutações para ajustes dos rotores e do painel de conexão.

O envio de mensagens se dava da seguinte forma: as letras eram digitadas pelo operador da Enigma e uma outra pessoa anotava as letras que apareciam no painel

luminoso, formando a mensagem criptografada que era transmitida via rádio, através do código Morse. O destinatário ouvia a mensagem, anotando letra por letra, e digitava em outra máquina, configurada conforme a do remetente que mostrava no painel luminoso as letras da mensagem original.

Diante disso, os alemães acreditavam na segurança da Enigma, porque seria impossível calcular rapidamente a chave dentre o quantitativo imenso de possibilidades, alteradas dia a dia. Enquanto os aliados não se apossassem da folha com as chaves, a comunicação permanecia segura.

Os militares alemães compraram 30 mil máquinas Enigma, garantindo-lhes o sistema mais seguro de criptografia do mundo. Eles ainda contaram com o desânimo dos franceses e americanos, depois das tentativas frustadas de quebrar a cifra da Enigma. Além disso, esses países e aliados encontravam-se em posição de domínio, após a Alemanha sair destroçada da Primeira Guerra Mundial. Como resultado, perderam o zelo pela criptoanálise, diminuindo em qualidade e quantidade seus especialistas.

Entretanto, a Polônia precisava investir esforços para quebrar a cifra da Enigma, visto que tinha restabelecido como Estado independente, após a Primeira Guerra Mundial, e sentia-se encurralada a leste pela Rússia, desejosa para espalhar seu comunismo, e a oeste pela Alemanda, querendo recuperar territórios. Frente a essa situação, foi criado um novo departamento de Cifras: o Buro Szyfrów.

O capitão Maksymilian Ciezki era o encarregado de decifrar mensagens alemãs, mas, mesmo tendo acesso a versão comercial da Enigma, não obteve sucesso, já que era diferente das usadas pelos militares. No entanto, a Polônia conseguiu as informações necessárias para construção de uma réplida com a ajuda dos franceses, que contavam com um agente secreto de codinome REX, o qual obtinha informações do traidor alemão Hans-Thilo Schimidt. Com isso, conseguiu compreender o funcionamento da Enigma alemã.

De acordo com Singh (2020) e Cimino (2018), como a Enigma era mecânica, o Escritório de Cifras (Buro Szyfrów) concluiu que uma mente científica teria mais chance contra o poder dessa máquina e convidou vinte matemáticos para um curso de criptografia. Eles tiveram que prestar juramento de sigilo e três se destacaram: Marian Rejewski, Henryk Zygalski e Jerzy Rózycki.

Rejewski usou como estratégia o fato da Enigma trabalhar com repetição: A mesma chave era usada durante todo o dia e ainda, como preocupação extra, os alemães começaram a utilizar a chave diária para transmitir uma outra chave para cada mensagem. Essa nova chave era datilografada duas vezes como forma de verificação para evitar erros de interferência e erros de operadores.

Conforme Singh (2020), como a chave era datilografada duas vezes, a primeira e a quarta letra eram cifras da mesma letra, fato que se repetia para a segunda e quinta letra e para a terceira e sexta letra. Com base nessa análise, todos os dias a equipe de Rejewski procurava padrões nas remessas de mensagens interceptadas e começou a montar

um alfabeto de relacionamentos, identificando as correntes em cada caso e o número de elos em cada uma. Ainda assim, era necessário identificar qual das 10.000.000.000.000.000 chaves diárias correspondia a uma padrão particular das correntes.

> Foi nesse ponto que Rejewski teve um insight profundo. Embora a disposição do quadro de tomadas e o ajuste dos misturados afetasse os detalhes das correntes, suas distribuições poderiam ser separadas. Em especial existe um aspecto das correntes que é totalmente dependente do ajuste dos misturadores e que não tem nada a ver com a disposição do quadro de tomadas: o número de elos nas correntes é puramente uma consequência do ajuste dos misturadores (SINGH, 2020, p. 173).

Ao separar esses dois problemas: encontrar os ajustes dos misturadores e encontrar o painel de tomadas, Rejewski simplificou a tarefa de achar a chave diária e, após cerca de um ano, conseguiu quebrar a cifra da Enigma. Com esse feito, a Polônia pode ficar mais aliviada, pois, caso a Alemanha resolvesse atacá-la, já saberia qual seria sua estratégia e poderia ter uma maior chance ao contra-atacar.

Quando a Alemanha fez reajustes na Enigma, as listas dos encadeamentos de Rejewski se tornaram inúteis, mas ele inventou um processo mecânico que verificava os possíveis ajustes dos rotores. Nas palavras de Cimino (2018, p. 109), "Em essência eram seis máquinas Enigma, cada uma com um dos seis arranjos, trabalhando em paralelo. A unidade tinha um metro de altura e era chamada Bomba". Todavia, o trabalho da Bomba e dos decifradores polaneses foi dificultado quando a Alemanha aumentou o número de rotores. Sem recursos, convidaram criptoanalistas da Grã-Bretanha e da França para conhecer o projeto, oferecendo-lhes réplicas da máquina e o projeto para construí-la.

De posse das máquinas fornecidas pela Polônia e temendo a aproximação da guerra, o governo Britânico mudou a sede da Escola de Cifras e Códigos do Governo para uma mansão em Bletchley Park, tendo em vista mais segurança e tranquilidade. Como não havia espaço suficiente, foram construídas cabanas de madeira. Nesse local, alfred Dillwyn Knox, pôs-se a trabalhar na Enigma com o material recebido dos poloneses. Logo após essa mudança, no dia 1º de setembro de 1939, a Alemanha iniciou a Segunda Guerra Mundial atacando um depósito militar polonês.

Conforme Cimino (2018), Marian Rejewski, Henryk Zygalski e Jerzy Rózycki fugiram para a França, onde continuaram o trabalho de decifração das chaves usadas pelo exército alemão. Ao passo que outros matemáticos, como Alan Turing e Peter Twinn, foram recrutados para trabalhar com Knox na Enigma.

Apoiando-se no fato de que logo os alemães perceberiam que a repetição da chave estaria comprometendo a segurança de sua cifra, Alan Turing começou a trabalhar numa outra forma de atacar a Enigma. Analisando mensagens já decifradas que foram interceptadas em Bletchley, ele acreditava que podia prever parte do conteúdo de uma mensagem não

decifrada, tendo como base quando e de onde fora enviada. Por exemplo, os alemães enviavam relatórios cifrados sobre a previsão do tempo logo após às seis horas da manhã. Se essa mensagem fosse interceptada, era quase certo que conteria a palavra *wetter*, "tempo" em alemão. Como essas mensagens costumavam ser uniformes, Turing poderia identificar esse termo dentro do texto cifrado, relacionando um pedaço do texto original com um pedaço do texto cifrado. Essa técnica é chamada cola e tal matemático tinha certeza que poderia usá-la para decifrar a Enigma.

Singh (2020) cita que Turing combinou colas, elos e máquinas conectadas eletricamente para aperfeiçoar a bomba de Rejewski e, descreve seu protótipo da seguinte forma:

> Cada uma das bombas de Turing consistia em doze misturadores Enigma conectados eletricamente e assim era capaz de lidar com elos muito mais longos de letras. A unidade completa teria dois metros de altura, por dois metros de comprimento e um metro de largura. Turing finalizou o projeto no início de 1940, e o trabalho de construção foi entregue à fábrica British Tabulating Machinery, em Letchworth (SINGH, 2020, p. 197).

A primeira Bomba de Turing foi batizada de *Victory* e seus resultados iniciais não foram satisfatórios, pois gastava cerca de uma semana para encontrar uma chave. Contudo, após quatros meses foi aperfeiçoada, sendo batizada de *Agnus Dai* e era capaz de encontrar uma chave da Enigma em uma hora.

Devido ao grande volume de mensagens cifradas nesse período, Max Newman, que fora tutor de Turing em Cambridge, achou que esse trabalho poderia ser feito por meio de máquinas eletrônicas que usassem fitas de papel e células fotoelétricas. Somado a isso, havia o fato dos alemães usarem outra máquina na comunicação entre Hitler e seus generais: a Lorenz SZ40, semelhante a Enigma, porém as bombas não podiam lidar com a sua cifra. De acordo com Singh (2020), Max Newman, baseado no conceito de Turing para uma Máquina Universal, projetou uma máquina capaz de se adaptar a diferentes problemas, todavia os diretores de Bletchley julgaram tecnicamente impossível sua implementação, arquivando o projeto.

Entretanto, Tommy Flowers, engenheiro eletricista que havia sido convocado pela equipe, prosseguiu com o projeto no centro de pesquisa dos correios, em Dollis Hill, e construiu o primeiro computador digital em grande escala, "o protótipo Colossus Mark I, com 1.500 válvulas. Em janeiro de 1944, caixotes de componentes dos laboratórios de Flowers foram entregues em Bletchley Park e montados. A máquina era do tamanho de uma saleta e pesava cerca de uma tonelada" (CIMINO, 2018, p. 170). Ainda de acordo com esse autor, apesar de creditarem a Turing a construção do Colossus, ele teve pouca contribuição.

Com a ajuda do Colossus, os criptoanalistas puderam decifrar mensagens com mais rapidez, garantindo a derrota alemã em muitas batalhas. Não obstante, esse trabalho

era dificultado por haver redes distintas de comunicação: o exército alemão da África, por exemplo, possuia redes e livros de códigos diferentes dos utilizados na Europa. Além disso, outras redes eram mais difíceis de decodificar, como a da Marinha que utilizava uma versão da Enigma com oito misturadores, o refletor era variável e seus operadores tinham o cuidado de não enviar mensagens padronizadas. Isso fez com que as comunicações navais se tornassem impenetráveis e a Alemanha começava a levar vantagem no Atlântico. Foi preciso utilizar a espionagem, o roubo e a infiltração para obter as chaves inimigas e, com estas em mãos, Bletchley Park começou a informar a localização dos submarinos alemães, mudando os rumos da guerra.

Os gênios de Bletchley Park também tiveram sucesso na decifragem de mensagens italianas e japonesas. As informações recebidas das três fontes foram nomeadas Código de Ultra e foram responsáveis por dar aos aliados vantagens no conflito. Apesar de terem desempenhado papel importante, os quebradores de códigos não sabiam como as decifrações estavam sendo usadas. Após a guerra permaneceram no anonimato e suas conquistas em segredo até o início da década de 1970, com a publicação do livro de Winterbotham: *The Ultra Secret*. Porém, muitos criptoanalistas não viveram para receber o reconhecimento merecido, como Alastair Denniston, primeiro diretor de Bletchley, e Alan Turing.

A planta do Colossus também foi destruída juntamente com muito do que havia em Bletchley. Isso fez com que outros cientistas recebessem o crédito pela invenção do computador, o Electronic Numerical Integrador And Calculator (ENIAC), construído em 1945 por J. Presper Eckert e Jonh W. Mauchly que consistia em 18 mil válvulas eletrônicas capazes de realizar cinco mil cálculos por segundo. Por conseguinte, o ENIAC foi considerado por décadas o pai dos computadores.

1.5 Criptografia computadorizada

Após ter contribuído para o resultado da guerra e para o nascimento do computador moderno, os criptoanalistas começaram a desenvolver e empregar a tecnologia computacional para quebrar cifras em alta velocidade e com a flexibilidade dos computadores programáveis. Ao mesmo tempo, os criptólogos se esforçavam para criar cifras mais seguras, iniciando, assim, uma batalha entre codificadores e decodificadores.

O proceso de cifragem de uma mensagem por meio do computador é semelhante a cifragem mecânica como a da Enigma. Conforme Singh (2020), há apenas três diferenças significativas. A primeira delas é que a máquina mecânica é limitada na prática, enquanto o computador pode simular uma máquina de alta complexidade, imitando a ação de centenas de misturadoses, girando em sentidos contrários, entre outras possibilidades. A segunda diferença é a questão da velocidade e a terceira é que o computador usa os números binários (sequências de uns e zeros, chamados de dígitos binários, abreviadamente *bits*) no lugar de letras.

Tal conversão pode ser realizada através de vários protocolos, como o Código Americano

para Troca de Informações - American Standard Code for Information Interchange (ASCII), o qual relaciona 7 dígitos para cada letra do alfabeto, conforme tabela 1.8. Apesar de usar computador e números, a cifragem ainda acontece por meio dos princípios da transposição e da substituição.

Tabela 1.8: Letras Maiúsculas em Números Binários - ASCII

A 1000001	**N** 1001110
B 1000010	**O** 1001111
C 1000011	**P** 1010000
D 1000100	**Q** 1010001
E 1000101	**R** 1010010
F 1000110	**S** 1010011
G 1000111	**T** 1010100
H 1001000	**U** 1010101
I 1001001	**V** 1010110
J 1001010	**W** 1010111
K 1001011	**X** 1011000
L 1001100	**Y** 1011001
M 1001101	**Z** 1011010

Fonte: Singh (2020, p. 271).

A exemplo da transposição simples, no computador, vamos cifrar a palavra **ALEGRIA**. Usando a tabela 1.8, traduz-se a mensagem para o ASCII:

Texto Original = ALEGRIA = 1000001 1001101 1000101 1000111 1010010 1001001 1000001

Removendo os espaços, troca-se o primeiro pelo segundo dígito, o terceiro pelo quarto e assim por diante. Nesse exemplo, o último dígito não muda, pois o número total de dígitos é ímpar.

Mensagem = Alegria
Texto Original em ASCII = 1000001100110110001011000111101001010010011000001
Texto Cifrado = 0100001100111001000111001011010110100001100100001

A mensagem cifrada é transmitida ao receptor que faz o processo inverso, encontra o texto original e converte os dígitos binários por meio do ASCII na mensagem **ALEGRIA**.

Fazendo uso da mesma palavra, será empregado uma versão simples da cifra de susbstituição no computador. Inicialmente, o texto é convertido em binário assim como a palavra chave, **LOURDES**. Em seguida, de acordo com Mitani et al. (2007), é feita

uma operação XOR, entre os dígitos correspondentes da mensagem e palavra chave. Caso os dígitos forem iguais resultam em 0 e se forem diferentes resultam em 1, tendo como resultado o texto cifrado que é enviado ao destinário que usa a mesma palavra chave para reverter a substituição, recriando o texto original que é interpretado via ASCII para obter a mensagem **ALEGRIA**.

Mensagem = alegria
Texto Original em ASCII = 100000110011011000101100011110100101001001100000 1
Chave (Lourdes) em ASCII=100110010011111010101101001010001001000101101001 1
Texto Cifrado = 000110100000100010000001010100101100001100001001 0

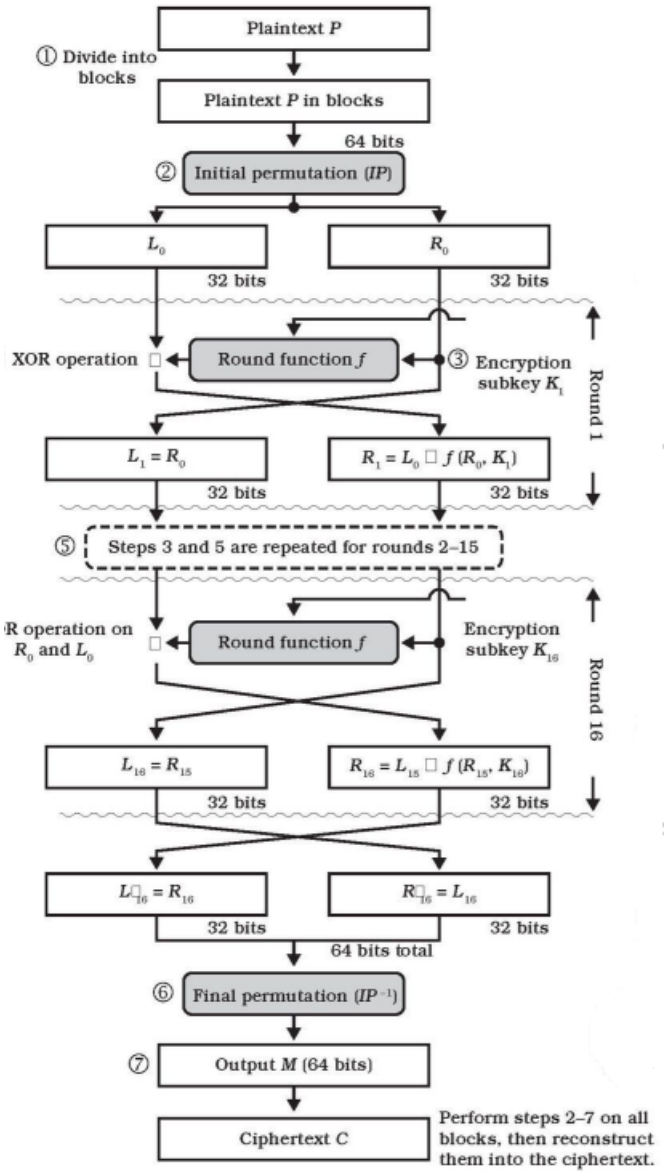
Assim como nas cifras manuais, a criptografia computadorizada pode utilizar, simultaneamente, a transposição e a substituição para torná-la mais segura. Além da segurança, a disseminação de computadores comerciais na década de 1960, apontaram a necessidade de um sistema civil de codificação padronizado. Como cita (SINGH, 2020, p.272), "uma empresa poderia usar um sistema particular de cifragem para garantir a segurança nas comunicações internas, mas não poderia enviar uma mensgem secreta para uma organização externa, a menos que o receptor usasse o mesmo sistema de cifragem". O primeiro deles foi o Padrão de Criptografia de Dados (DES), baseado no criptossistema Lúcifer criado por Horst Feistel que trabalhava com Don Coppersmith na International Business Machines Corporation (IBM) nos anos de 1970.

Lúcifer cifra mensagens da seguinte forma: inicialmente, a mensagem é traduzida em dígitos binários. Depois esse texto é dividido em bloco de 64 bits e é executada uma permutação inicial, usando um algoritmo para cada bloco de 64 bits que substitui e reorganiza esses bits, dividindo 32 bits a direita e 32 bits a esquerda. A seguir, é utilizada uma função que reorganiza e substitui cada bit em um bloco, o direito fica a esquerda e no da esquerda é aplicada uma operação por meio de um algoritmo para criar um novo bloco direito de 32 bits. Com isso, uma etapa chamada round é concluída e repete-se o processo descrito por 16 rounds até que o texto seja cifrado, conforme figura 1.7. Quando o destinatário recebe a mensagem cifrada, faz o processo inverso para ter acesso ao texto original.

Na época, esse sistema era um dos mais poderosos disponíveis comercialmente, mas a Agência de Segurança Nacional (NSA) interferiu no trabalho de Feistel, limitando o número de chaves para 56 bits. Provavelmente, porque não queria a adoção de uma cifra que estivesse além das suas capacidades de quebra. A versão aprovada pela NSA, foi oficialmente adotada em 23 de novembro de 1976, batizada como Padrão de Cifragem de Dados (DES).

Conforme apregoa Mitani et al. (2007), a criptografia DES tornou-se insegura a partir de 1990, devido ao avanço dos computadores. A exemplo de alguns métodos que podem quebrar essa cifra, esse autor cita: o algorítmo de pesquisa exaustiva (utiliza a força bruta para

Figura 1.7: Estrutura do Sistema Lúcifer



Fonte: Mitani et al. (2007, p. 73).

tentar as chaves possíveis), a Critptoanálise diferencial (procura vulnerabilidade na chave, correlações entre as entradas e saídas) e a criptoanálise linear (pesquisa vulnerabilidade na cifra, procurando por fraquezas matemáticas na sua estrutura).

Mitani et al. (2007) cita que em 1997, o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos fez uma convocação pública para que fosse apresentado um algorítmo melhor. Empresas e organizações enviaram suas submissões e dentre elas foi escolhido o algorítmo Rijndael, denominação derivada dos nomes de seus inventores: Joan Daemen e Vicent Rijmen. Renomeado, em 2000, para Padrão de Criptografia Avançado (AES) e publicado como Padrão Federal de Processamento de Informações (FIPS), apresenta três tamanhos possíveis de chaves: 128, 192 e 256 bits, sendo a força da criptografia

proporcional ao tamanho da chave. Essa cifra utiliza uma rede de substituição (por meio de uma operação XOR executada em cada bloco e subchave) e permutação (função que embaralha os bits de entrada), ambas são executadas simultaneamente por um número de rounds, assim como numa rede Feistel.

A criptografia DES e AES são simétricas, ou seja, o emissor e receptor comungam da mesma chave para cifragem e decifragem das mensagens. Por isso, também partilham o problema da distribuição de chaves, feita por meios eletrônicos e vulneráveis a interceptação de intrusos. Logo, as chaves precisavam ser compartilhadas e armazenadas de forma segura, mas esse tipo de criptografia não garante a identidade de quem enviou ou recebeu a mensagem. Cimino (2018, p. 182) cita que: "A única forma segura de distribuir a chave era por portador. Os mensageiros voavam pelo mundo com chaves da cifra DES trancadas em pastas acorrentadas ao pulso".

Com o desenvolvimento da internet surge, também, a necessidade de garantir ao público o direito a privacidade, o que exigia uma troca segura de chaves. Esse problema foi atacado por Whitfield Diffie, Martin Helman e Ralph Merkle que, a princípio, se viram num beco sem saída, pois todas as suas tentativas terminavam em fracasso. Após meses tentando achar uma solução, concentraram suas pesquisas nas funções matemáticas. Como cita Singh (2020),

> Uma função é qualquer operação matemática que transforma um número em outro. Por exemplo, "dobrar" é um tipo de função porque transforma o número 3 em 6 e o número 9 em 18. Além disso, nós podemos pensar em todas as formas de cifragem por computador como funções, porque elas transformam um número (o texto original) em outro (o texto cifrado) (SINGH, 2020, p. 285).

Com foco nas funções de mão única (funções fáceis de fazer, mas praticamente irreversíveis) e na aritmética modular (campo da matemática rico em funções de mão única), Hellman encontrou uma estratégia para resolver o problema da troca de chaves, provando que duas pessoas poderiam estabelecer uma chave sem se encontrar. "A ideia de Hellman dependia de uma função de mão única da forma $Y^x = (modP)$" (SINGH, 2020, p. 289), que pode ser explicada da seguinte forma: inicialmente, remetente e destinatário escolhem valores para Y e P. De regra, qualquer valor serve, mas existem restrições, como o valor de Y ser menor que P. Esses números não são secretos, podendo ser compartilhados até mesmo por telefone, pois mesmo que haja interceptação, eles escolheram uma função de mão única.

Esse esquema ficou conhecido como troca de chaves de Diffie-Helman-Merkle e foi publicado em 1976. Apesar de ser uma das grandes descobertas da criptografia, esse sistema ainda não era perfeito, pois para estabelecer uma comunicação era necessário que remetente e destinatário estivessem simultaneamente conectados. Esse embate começou a ser solucionado com a ideia da cifra assimétrica de Diffie com chaves diferentes para

codificação e decodificação, sendo a chave de codificação pública para que qualquer pessoa pudesse utilizá-la, porém a chave de decodificação seria privada e somente com ela alguém conseguiria ler a mensagem.

Com a publicação das ideias de Diffie, outros cientistas começaram a pesquisar uma função de mão única com base nos critérios exigidos para uma cifra assimétrica e, assim, três pesquisadores do Laboratório de Ciência e Computação do Instituto de Tecnologia de Massachusetts (MIT), os cientistas Ron Rivest e Adi Shamir e o matemático Leonardo Adleman obtiveram como resposta o criptossistema RSA (Rivest, Shamir, Adleman). Esse sistema tornou-se a cifra mais influente da critografia moderna, sendo explicado por Cimino (2018) da seguinte forma (Alice e Bob, citados pelo autor, são os personagens do processo comunicativo):

> ...Ele usa uma função de mão única, como antes, mas aqui Alice cria uma chave multiplicando dois números primos grandes "p" e "q": $p \times q = N$. Esses dois números são sua chave privada, e ela os guarda para si. O produto "N"faz parte da chave pública, que ela distribui a todo mundo junto com um número que chamaremos de "e".
>
> Num sistema computadorizado, o texto costuma ser codificado em ASCII ou alguma outra forma de código binário. Portanto, em essência o texto é um número. Chamaremos o texto original de número **M** e o texto cifrado, de número **C**. A função de mão única que usaremos é:
>
> $\mathbf{C} = \mathbf{M}^e \pmod{N}$
>
> Bob escolhe os números primos 17 como "p" e 11 como "q" e mantém ambos em segredo. mas divulga a chave pública N, que é $17 \times 11 = 187$, juntamente com $e = 7$, digamos. Digamos também que a mensagem de Alice e Bob seja simplesmente a letra inicial de seu nome, A, que é 65 em ASCII. Assim, ela codifica a mensagem:
>
> $\mathbf{C} = 65^7 \pmod{187} = 142$
>
> Para decifrar a menagem, Bob tem de descobrir sua chave de decodificação **d** usando a fórmula: $d = 1 \pmod{(p-1).(q-1))/e}$
>
> portanto,
>
> $d = 1 \pmod{16.10)/17} = 1 \pmod{160)/7} = 23$
>
> Para decodificar a mensagem de Alice, Bob usa a fórmula:
>
> $\mathbf{M} = \mathbf{C}^d \pmod{187}$
>
> $\mathbf{M} = 142^{23} \pmod{187}$
>
> $\mathbf{M} = 65$, ou seja, A em ASCII (CIMINO, 2018, p. 187).

Na realidade, os números escolhidos para "p" e "q" são enormes, de forma que é fácil multiplicá-los para gerar uma chave pública, mas fatorar esse produto para obter os números primos escolhidos é dificílimo, por isso a chave pública, na prática, continua indecifrável até descobrirem um atalho para a fatoração.

Embora os cientistas citados tenham levado crédito pelo criptossistema de chave pública, este já teria sido descoberto anteriormente pelo Quartel-General de Comunicações do Governo (GCHQ) em Cheltenham criado após a Segunda Guerra Mundial com remanescente de Bletchley Parq, mas foi mantido sob anonimato pelo governo. No GCHQ, a ideia da criptografia com chave pública foi idealizada por James Ellis, um dos maiores criadores de códigos do país, ainda na dácada de 60. Todavia, ele não era matemático, então revelou sua descoberta aos chefes e as mentes mais brilhantes da instituição esforçaram para encontrar uma função de mão única que atendesse as determinações de Ellis. Ao final de três anos de busca, o recém graduado Clifford Cocks foi incorporado a equipe e, seguindo os mesmos processos mentais de Rivest, Shamir e Adleman, solucionou o problema, descobrindo o sistema mais tarde denominado RSA.

Atualmente, a decodificação cabe a organizações sigilosas, como o GCHQ e a NSA, que se opõem a codificação forte temendo atos criminosos e terroristas, entretanto, sem esse tipo de codificação essas organizações conseguem ter acesso a qualquer transação feita pela internet. Diante disso, alguns criptólogos entraram na defesa do direito a privacidade, como o cientista da computação e ativista antinuclear Philip Zimmermann que criou o Algoritmo Internacional de Codificação de Dados (IDEA), uma cifra de bloco simétrica que apressa o uso do RSA num computador pessoal. No IDEA somente a chave seria cifrada com RSA que poderia ser transmitida em segurança através do programa Privacidade Bastante Boa (PGP), também desenvolvido por ele.

Na busca por mais segurança nas transações realizadas por meio da internet, Zimmermann acrescentou a assinatura eletrônica para garantir a legitimidade do remetente e evitar fraudes. Por exemplo, sem a assinatura digital, o banco recebe uma mensagem solicitando uma transferência para outra conta, mas não pode assegurar que a solicitação foi feita pelo titular da conta. Em decorrência disso, como cita Cimino (2018), Zimmermann incorporou ao seu programa um processo de codificação em dois estágios: primeiramente a mensagem era codificada com a chave do remetente e depois o resultado era codificado com a chave pública do destinatário, de forma que só este poderia decifrá-la usando sua chave privada e por fim, usaria a chave pública do remetente para decifrar o resultado, conferindo a legitimidade do remetente.

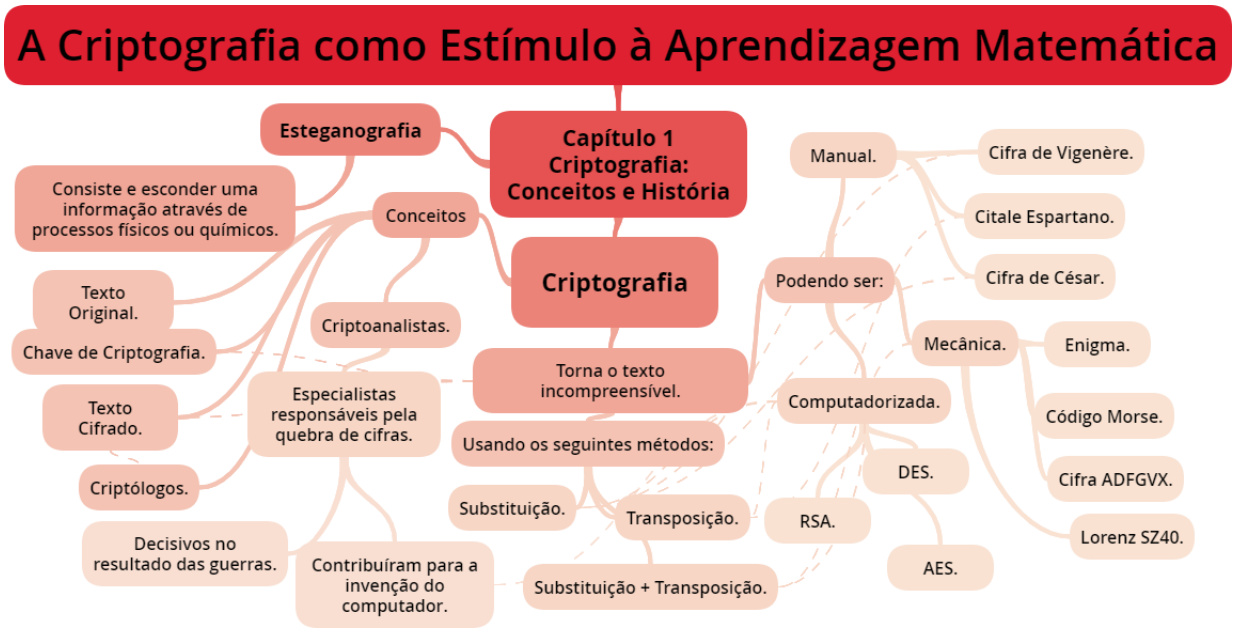
Para legalizar o PGP, Zimmermann teve que enfrentar o governo e perseguições do FBI, sendo acusado por tráfico de armas ao disponibilizar o PGP na internet. Singh (2020) cita que o ativista foi alvo de investigações por três anos, mas não conseguiram levá-lo a júri, arquivando o processo. Após fazer um acordo como a RSA, ele obteve uma licença, patenteando o PGP que foi vendido para a Network Associates, onde se tornou sócio majoritário.

Além da RSA, existem outras cifras modernas consideradas inquebráveis até o momento, mas, como foi visto, essas cifras são alvo da criptoanálise que sempre descobre uma forma de vencê-las, como aconteceu com a cifra de Vigenère e a Enigma. Porém, há séculos, os

matemáticos estão na busca, sem sucesso, por uma forma mais rápida de fatoração. Diante disso, os criptoanalistas investem esforços numa inovação tecnológica: o Computador Quântico, que seria bilhões de vezes mais rápido que um computador atual. Enquanto isso, os criptógrafos pensam um outro sistema de segurança, a criptografia quântica, a qual não será detalhada nesse trabalho, mas caso o leitor se interesse poderá recorrer a Singh (2020), apesar das informações ainda serem incipientes e provavelmente, guardadas em segredo.

De acordo com o que foi discutido neste capítulo, é inegável a importância da criptografia para garantia da privacidade de governos, organizações e civis, principalmente na era da internet. Também ficou evidente o quanto a batalha entre ciptógrafos e criptoanalistas contribuiram para o avanço dos sistemas criptógraficos, dentre os quais muitos não foram abordados neste texto, mas poderão ser alvo de pesquisas futuras. Por fim, segue o mapa mental representando os conhecimentos discutidos no capítulo.

Figura 1.8: Mapa Mental - Capítulo 1



Fonte: Elaboração da autora..

2 Análise de Pesquisas que Relacionam Criptografia e o Ensino de Matemática na Educação Básica

Neste capítulo, apresentaremos um levantamento bibliográfico relacionado com a temática: Criptografia e o Ensino da Matemática na Educação Básica que tem por objetivo adicionar o embasamento necessário para o desenvolvimento da pesquisa e direcionar intervenções diferenciadas para a sala de aula.

Inicialmente, fizemos uma busca no site da Biblioteca Brasileira de Teses e Dissertações (BDTD) e no catálogo da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) utilizando a frase: Criptografia e Matemática na Educação Básica, sendo encontrados quarenta e seis trabalhos. Após uma breve leitura do resumo e da aplicação prática selecionamos vinte e quatro deles tendo como base o objetivo da presente pesquisa: analisar o potencial da criptografia para estimular a aprendizagem do conceito de função nos 9º ano A e B do Colégio Municipal X. Utilizamos como limite temporal as dissertações defendidas entre os anos de 2013 e 2019, período com maior número de publicações. Na sua maioria, elas são do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) e na tabela 2.1 apresentaremos dados gerais: nome do autor, título, ano de publicação, conteúdo abordado e etapa da educação básica para a qual foi proposta e/ou aplicada e, em seguida, fizemos uma breve análise do conteúdo abordado ou indicado para sala de aula por cada uma delas.

Tabela 2.1: Dissertações de Mestrado que Relacionam Criptografia e Conteúdos de Matemática Básica

Autor	**Título**	**Instituição/ano**	**Conteúdos Trabalhados na Prática / Etapa da Educação Básica**

1- Henrique Augusto Schurmann	Criptografia matricial aplicada ao Ensino Médio.	Universidade Estadual de Londrina - PROFMAT/2013.	Matrizes / Ensino Médio.
2- Jaqueline de Moraes Rodrigues	Criptografia e conteúdos de matemática no Ensino Fundamental.	Universidade Federal de São Carlos - PROFMAT/2013.	Conceito de Função / Ensino fundamental.
3- José Luiz dos Santos	A arte de cifrar, criptografar, esconder e salvaguardar como fontes mediadoras para atividades de matemática básica.	Universidade Federal da Bahia - PROFMAT/2013.	Funções, análise combinatória e matrizes / Ensino Médio.
4- Reinaldo Donizete de Oliveira	Utilização de mensagens cripetografadas no ensino de matrizes.	Universidade Federal de São Carlos - PROFMAT/2013.	Matrizes / Ensino Médio.
5- Darci Dala Costa	A matemática e os códigos secretos: uma introdução a criptografia.	Universidade Estadual de Maringá - PROFMAT/2014.	Função inversa e criptografia / Ensino Médio.
6- Flávio Ornellas Loureiro	Tópicos de criptografia para o ensino médio.	Universidade Estadual do Norte Fluminense Darcy Ribeiro /2014.	Funções, funções de várias sentenças, matrizes e análise combinatória / Ensino Médio.
7- Márcia Shizue Matsumoto	Despertando o interesse do aluno pela matemática com a criptografia.	Universidade Federal da Grande Dourados /2014.	História da criptografia, Cifra de César, divisão euclidiana e análise de frequência / Ensino Fundamental (6º e 7º).

8- Waldizar Borges de Araújo França	A Utilização da criptografia para uma aprendizagem contextualizada e significativa.	Universidade de Brasília - PROFMAT/2014.	Funções, matrizes e análise combinatória e nº de subconjuntos / Ensino Médio.
9- Ana Paula Ganassoli e Fernanda Ricardo Schankoski	Criptografia e matemática.	Universidade Federal do Paraná - PROFMAT/2015.	Análise combinatória, matrizes, funções, divisão, aritmética modular e RSA / Ensino Fundamental e Ensino Médio.
10 - Dayane Silva dos Santos	Uso da criptografia como motivação para o ensino básico de matemática.	Universidade Federal de Sergipe - PROFMAT/2015.	Divisibilidade, congruência, função e matriz / Ensino Fundamental e Ensino Médio.
11 - Waldir Claudio de Castro Júnior	Criando mensagens secretas na escola básica utilizando a criptografia RSA.	Universidade Federal de São Carlos - PROFMAT/2015.	Criptografia RSA / Ensino Fundamental (9º ano) e Ensino Médio.
12- Igor Nascimento da Silva	Criptografia na Educação Básica: das escritas ocultas ao código RSA.	Pontifícia Universidade Católica do Rio de Janeiro /2016.	Aritmética modular, criptografia e sistema RSA / Ensino fundamental (8º e 9º ano).
13- Jean Mendes Jansen	Criptografia: uma abordagem para o ensino médio.	Universidade Federal do Maranhão - PROFMAT/2016.	Funções, matrizes e sistema RSA / Ensino Médio.

14- Beatriz Fernanda Litoldo	As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas a função afim.	Universidade Estadual Paulista /2016.	Função afim / Ensino Médio.
15- Leandro Rodrigues de Carvalho	O uso de elementos da criptografia como estímulo matemático na sala de aula.	Universidade Estadual Paulista - PROFMAT/2016.	Divisão euclidiana, criptografia e permutação / Ensino Médio.
16- Fabiana de Souza Bomfim	História da matemática e cinema: O caso da matemática na introdução do ensino da álgebra.	Universidade de São Paulo- PROFMAT/2017.	Criptografia / Ensino Fundamental (8º ano).
17- Paulo Francisco de Araújo	Aplicações de Criptografia no Ensino Médio.	Universidade Federal de Viçosa, MG - PROFMAT/2017.	Congruência, matrizes, Algoritmo de Euclides e logaritmos discretos/Ensino Médio.

18- Anderson Pinheiro Machado	Teoria dos números e criptografia RSA: uma proposta de ensino para alunos de matemática olímpica.	Universidade Federal de Santa Maria - PROFMAT/2018.	Criptografia, divisibilidade, números inteiros, MDC, MMC, números primos, Equações Diofantinas, aritmática modular, inversos multiplicativos, aritmética modular, Teorema Fundamental da Aritmética, Teorema de Euler / alunos medalhista do Ensino Fundamental (8º e 9º ano).
19- Cíntia Kohori Rosseto	Criptografia como recurso didático: uma proposta metodológica aos professores de matemática.	Universidade Estadual Paulista - PROFMAT/2018.	Funções e Cifra de César / Ensino Fundamental e Médio.
20- Maria Suzana Pinheiro	Criptografia RSA, números primos e uma sugestão de aplicação no Ensino Médio.	Universidade Estadual do Ceará - PROFMAT/2018.	Sistema RSA, Números Primos, Congruência, Teorema Fundamental da Aritmética e Pequeno Teorema de Fermat / Ensino Médio (3º ano).
21- Reginaldo Cristiano Griseli	Criptografia: uma proposta para a educação básica.	Universidade Federal da Fronteira do Sul - PROFMAT/2018.	Algorítmo da divisão e congruência / professores.

22- Evelyn Gomes da Silva	Criptografia RSA: da teoria à aplicação em sala de aula.	Universidade de São Paulo - PROFMAT/2019.	Matrizes e criptografia/ Ensino Médio.
23- Moisés de Oliveira Moura	A criptografia motivando o estudo das funções no 9º ano do ensino fundamental.	Universidade Federal do Tocantins - PROFMAT/2019.	Função afim / Ensino Fundamental (9º ano).
24- Solange Mariano da Silva Santos	Aprendizagem das funções polinomiais do 1º e 2º grau mediada pelo jogo "Trilha Matemática Criptografa": uma abordagem sob a perspectiva Vygotskyana.	Universidade Tecnológica do Paraná /2019.	Funções polinomiais do 1º e 2º grau / Ensino Médio).

Fonte: Elaboração da autora.

2.1 Análise da proposta prática das dissertações selecionadas

Nesta seção, descreveremos, brevemente, as atividades práticas das dissertações analisadas. Utilizamos como critério organizacional o conteúdo trabalhado em cada uma delas, por acreditar que essa possa ser a melhor forma para comparar metodologias, objetivos e resultados, além de auxiliar no desenvolvimento de outras propostas sobre criptografia e matemática. Assim, abordaremos os seguintes temas: Funções, Matrizes, Análise Combinatória, Aritmética Modular (Divisão Euclidiana, Congruência, Sistema RSA).

2.1.1 Funções

Dentre os trabalhos analisados, onze deles relacionam criptografia e funções. Partem da premissa que é necessário tornar as aulas de matemática mais contextualizadas e significativas e, em geral, têm o mesmo objetivo: motivar o ensino aprendizagem dessa disciplina por meio da criptografia. Dessa forma, espera-se que ao contextualizar o conteúdo com uma temática atual e utilizada cotidianamente, o estudante perceba a aplicabilidade do conteúdo e se interesse pelo saber matemático.

Rodrigues (2013), pesquisa 2, tem como ponto de partida as dificuldades dos alunos do 9º ano na aprendizagem de funções e apresenta uma proposta que tem como metodologia a engenharia didática. As atividades aplicadas relacionam criptografia e funções, nas quais, inicialmente, o professor explica que existem dois tipos de criptografia: simétrica e assimétrica e, em seguida, são apresentadas três atividades. A primeira usa a Cifra de Chiqueiro para codificar e decodificar mensagens entre os alunos e a segunda apresenta um criptograma, uma adição que os alunos deveriam descobrir quais números correspondiam a cada letra. A terceira atividade consistia em codificar o nome da escola seguindo os seguintes passos:

- Faz-se uma pré-codificação utilizando uma tabela em que cada letra corresponde a um número;
- Escreve-se os números sem deixar espaços e divide essa sequência em blocos de cinco e quatro dígitos, mas não podem começar com zero, pois pode causar problemas durante a codificação;
- Utiliza-se a função $f(x) = 2x + 5$ para codificar o nome da escola, substituindo $f(x)$ por cada um dos blocos.

Para decodificar a mensagem basta fazer as operações inversas. De acordo com a autora, os alunos já tinham conhecimentos prévios sobre funções, facilitando o desenvolvimento das atividades. Construíram empiricamente o conceito de função inversa, uma vez que esse conteúdo não faz parte do currículo do Ensino Fundamental.

A proposta apresentada por Litoldo (2016),pesquisa 14, tem por objetivo compreender como as atividades envolvendo problemas de criptografia podem auxiliar os alunos na exploração das ideias associadas à função afim. De acordo com a autora, o trabalho tem como relevância a busca por metodologias diversificadas para o ensino da matemática, a valorização dos conhecimentos prévios dos estudantes e a elaboração de atividades instigantes e desafiadoras que relacionam conhecimentos matemáticos e criptografia, pois estas são escassas.

A autora também discorre sobre o empoderamento da matemática, se fundamenta na Concepção Construtivista da Educação e na metodologia de resolução de problemas para elaborar uma sequência didática que foi aplicada com um grupo de sete alunos do primeiro ano do Ensino Médio. Essa sequência foi composta por oito atividades inspiradas em jogos de criptograma e palavras cruzadas, tendo como foco o conceito de função afim. Cada uma delas é composta por um conto com o Sherlock Holmes (personagem pelo qual a pesquisadora tem afeição), uma mensagem criptografada e uma ficha de perguntas.

As atividades desenvolvidas apresentam grau de complexidade crescente: a primeira teve por objetivo apresentar o tema criptografia, a segunda, terceira e quarta abordou o conceito de função afim e suas especificidades, a quinta e sexta trabalhou o gráfico da

referida função, a sétima a definição de função inversa e a oitava uma síntese do que foi desenvolvido.

Nesta pesquisa, os alunos se posicionaram como decifradores, investigando, explorando e desenvolvendo diferentes estratégias de resolução das mensagens criptografadas e dos problemas propostos. Litoldo (2016) avalia o trabalho como significativo para seu crescimento pessoal, além de permitir que os alunos aguçassem a criatividade, a iniciativa, o espírito explorador e a autonomia.

Outro trabalho que aborda o conceito de função afim é o de Moura (2019), pesquisa 23, que tem como tema: "A criptografia motivando o estudo das funções no 9º ano do ensino fundamental", sendo justificado pelo fato da criptografia estar presente no cotidiano dos alunos por meio de recursos digitais e, também, de favorecer conexões com outras áreas. Dessa maneira, a criptografia será o agente motivador para despertar no educando o interesse pela matemática. A aplicação das atividades aconteceu em seis encontros conforme quadro apresentado a seguir:

Tabela 2.2: Cronograma de Atividades Desenvolvidas

Data	Atividades Desenvolvidas
09/10/2018	Conversa informal com os participantes, para explicar a proposta da pesquisa e, a contribuição dos mesmos nesse processo; Aplicação do pré-teste (anexo A): atividade para verificação do conhecimento prévio sobre criptografia, função bijetora e função inversa.
16/10/2018	Exposição do tema criptografia e relatos de alguns fatos históricos envolvendo suas aplicações; Exemplos e atividades para mostrar a criptografia utilizada no bastão de Licurgo e na cifra de César.
23/10/2018	Exposição do tema funções: definição das funções afim, injetora, sobrejetora, bijetora e função inversa; Mostrar a relação entre criptografia e funções.
30/10/2018	Mostrar como codificar e decodificar mensagens usando as funções afins.
06/11/2018	Aplicação do pós-teste (anexo B): atividade para verificar se os participantes compreenderam os temas e atividades abordados nos encontros anteriores.
13/11/2018	Aplicação da atividade final (anexo C): atividade cuja intenção, era saber a opinião dos participantes em relação ao trabalho de um modo geral.

Fonte: Moura (2019, p. 53)

O pré-teste foi aplicado para sondar os conhecimentos dos alunos sobre o tema criptografia, funções bijetoras e a inversa de uma função. Após desenvolver as atividades, realizou-se um pós-teste que mostrou resultados positivos no processo ensino-aprendizagem de matemática.

> O pós-teste (anexo C) além de apresentar um resultado positivo quanto à aceitação da proposta da pesquisa em seu conjunto, também deixou explícito a satisfação dos participantes em relação

> ao método utilizado e aos conteúdos abordados. Com a análise dos dados coletados com a aplicação do anexo C, verifica-se que o objetivo foi alcançado. Assim, por meio desta análise, percebem-se novas possibilidades de aplicações da criptografia como motivação em estudos posteriores, uma vez que esse processo possibilita avanços satisfatórios, tanto no ensino quanto na aprendizagem (MOURA, 2019, p. 64).

Santos (2019), pesquisa 24, baseou-se na teoria Vigotskyana sobre os níveis de desenvolvimento e aprendizagem e na taxonomia de Bloom[1] para desenvolver uma proposta que trabalha com funções polinomiais do 1º e 2º grau, com alunos do Ensino Médio, por meio do jogo "Trilha Matemática Criptografada". Esse jogo consiste em um tabuleiro com cartas-perguntas criptografadas em forma de *QR CODES*, conforme figura 2.1 e explicação da autora:

> O jogo contém 20 cartas-perguntas criptografadas (vermelha), 20 cartas-respostas criptografadas (vermelha), 20 cartas-perguntas criptografadas (amarela), 20 cartas-respostas criptografadas (amarela),20 cartas-perguntas criptografadas (azul), 20 cartas-respostas criptografadas (azul), 01 dado, 02 carrinhos de cores diferentes, 01 tabuleiro , folhas rascunho e 01 Manual de Instruções (SANTOS, 2019, p. 40).

As cores das cartas relacionam-se com o tipo de questão e de jogo da seguinte forma:

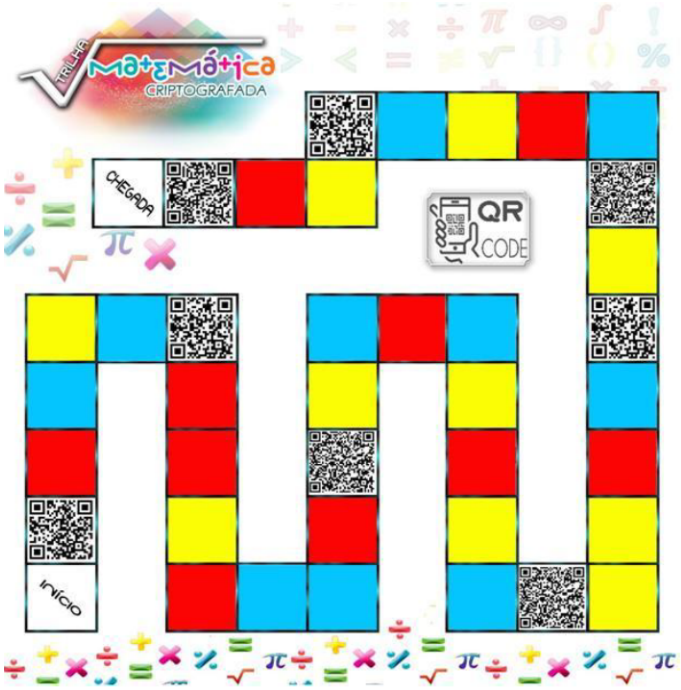
- Cartas Amarelas - Questões de fixação - Jogos de treinamento;
- Cartas azuis - Questões de análise e interpretação - jogos de treinamento e/ou aprofundamento;
- Cartas vermelhas - Questões com situações-problema mais elaboradas e contextualizadas - Jogos de aprofundamento.

Antes e depois do jogo, realiza-se uma atividade para verificar o nível de desenvolvimento real dos alunos em relação ao conteúdo já explicitado. De acordo com a pesquisadora, os alunos mostraram mais dificuldades nas resoluções das cartas com questões mais complexas dentro da hierarquização da taxonomia de Bloom. Também afirma que:

> O aspecto lúdico do jogo enfatiza o desenvolvimento afetivo e emocional, e para Vygotsky é imprescindível no processo de construção do conhecimento. Ainda, pelas falas dos alunos descritas na seção 5, é possível percebermos o interesse e envolvimento deles

[1] De acordo com Santos (2019), a Convenção Americana de Psicologia (APA) de 1948, realizada em Boston, reuniu um grupo de psicólogos que demonstraram interesse em discutir, definir e elaborar uma taxonomia dos objetivos dos processos educacionais. Liderados por Benjamim Bloom desenvolveram três deles: cognitivo, afetivo e psicomotor.

Figura 2.1: Tabuleiro do jogo Trilha Matemática Criptografada



Fonte: Santos (2019, p. 41).

> com o jogo, o que os auxilia no desejo em aprender Matemática, enfatizamos ainda, que a utilização de tecnologias (smartphones) e criptografias (QR CODE) também foi importante para a motivação dos estudantes e contribuiu para que o jogo ficasse mais instigante (SANTOS, 2019, p. 78).

A autora conclui explicitando que houve melhora no rendimento dos estudantes e que a utilização do jogo contribuiu para compreensão do conteúdo abordado, para formação de valores (como respeito, cooperação, iniciativa pessoal) e para proporcionar um ambiente mais agradável e motivador da aprendizagem matemática.

Na dissertação de Costa (2014), pesquisa 5, são apresentadas dicas de como trabalhar criptografia na Educação Básica e um plano de aula para alunos do 1º ano do Ensino Médio envolvendo funções, especialmente função inversa. Para a realização da atividade deve ser feita uma pré-codificação, associando cada letra do alfabeto a um número inteiro, iniciando pelo 11. Depois estabelece uma relação de substituição que associa cada x , valor da letra pré-codificada, a um y, valor da letra codificada. Após cifrar a mensagem, determina a inversa para encontrar a chave de decodificação.

Pesquisadores como Santos (2013), Ganassoli e Schankoski (2015), França (2014), Jansen (2016), Santos (2015) e Rosseto (2018), pesquisas 3, 9, 8, 13, 10 e 19 respectivamente, apesar de não terem o conteúdo como único foco, também apresentam atividades relacionadas com funções.

Na dissertação de Santos (2013) são citados exemplos que correlacionam matemática e criptografia, como os conceitos de função aplicados as técnicas de cifragem por substituição

e transposição. O autor faz uso da metodologia de resolução de problemas e propõe atividades para estudantes do Ensino Médio, tendo como base o conjunto de competências e habilidades definidas pela matriz de referência do Exame Nacional do Ensino Médio (ENEM). São descritas três atividades envolvendo funções.

Essas atividades exploram o conceito de função como uma transformação, o cálculo da imagem, a bijeção como condição para determinação da função inversa, o cálculo da pré-imagem e a análise de gráficos. A orientação é que os discentes estejam divididos em grupos com quatro componentes, cada um com funções bem definidas, enquanto o professor faz o papel de mediador, tirando dúvidas e enfatizando questões importantes. A primeira atividade parte da situação abaixo e são feitos uma série de questionamentos envolvendo cifragem, decifragem, domínio e imagem com um tempo de 1h30min para realização.

> Luiz deseja enviar uma mensagem sigilosa para José, a qual deverá ser cifrada substituindo-se cada letra por um número, conforme a tabela abaixo, aplicando o número correspondente na função $f(x) = 3x - 2$, obtendo a mensagem cifrada. Por exemplo, a letra m corresponde ao número 13, que é transformado pela função em $f(13) = 13 \times 13 - 2 = 37$, ou seja, a letra m é cifrada pelo número 37 ($m \mapsto 37$) (SANTOS, 2013, p. 52).

Tabela 2.3: Pré-codificação

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Santos (2013, p. 52)

A segunda atividade utiliza essa mesma tabela, mas os questionamentos são feitos a partir da função quadrática:$f(x) = x^2 - 8x + 17$, considerada função cifradora, e na terceira, os estudantes podem trabalhar em grupos ou individualmente para manipular funções cifradoras, estipular valores para todas as letras do alfabeto e determinar a função decifradora (a função inversa). Dessa forma, a proposta trabalha os diversos tipos de funções: afim, quadrática, modular, exponencial e logarítmica. Além disso, o autor apresenta todas as resoluções e comentários para professores em cada um dos ítens.

Com essa mesma abordagem, tanto em relação a metodologia quanto aos conteúdos, e com o objetivo de apresentar aos professores de matemática atividades didáticas que relacionam criptografia e conteúdos de matemática, França (2014) e Jansen (2016) propõem atividades envolvendo funções para discentes do Ensino Médio, tendo como base os Parâmetros Curriculares Nacionais. No caso do segundo, além de indicar as atividades no capítulo V, desenvolve no capítulo anterior uma série de exemplos similares. Uma diferença nas atividades propostas por Jansen (2016) são as tabelas para pré-codificação do alfabeto, nas quais os números nem sempre estão em sequência ou iniciam em 1.

As atividades desenvolvidas por Rosseto (2018), tiveram como origem uma enquete feita com estudantes do 9º ano para saber a opinião deles sobre a disciplina de Matemática. Os resultados apontaram que eles concordam sobre sua presença no cotidiano e que seus conteúdos são importantes, mas a maioria tem aversão, devido as dificuldades de aprendizagem. Ainda sugeriram o uso de dinâmicas, aplicações, jogos, filmes e atividades em grupo no desenvolvimento das aulas. Diante disso, a pesquisadora exibiu o filme: "O Jogo da Imitação", através do qual os alunos se mostraram mais entusiasmados, então, aproveitou-se a oportunidade para trabalhar a história e técnicas de criptografia, como a Cifra de César e as funções: $f(x) = 3x - 2$, $f(x) = 2x - 6$ e $f(x) = 2x + 3$ para codificar e decodificar palavras.

Nessa mesma perspectiva, Ganassoli e Schankoski (2015) e Santos (2015) propõem atividades para o Ensino Médio, com situações-problema do tipo: **"Cifre a mensagem que Carla escreveu para sua amiga Isabela: FESTA SURPRESA PARA A BIA, utilizando a seguinte regra: valor da letra +2"** (GANASSOLI; SCHANKOSKI, 2015, p. 41). Para resolver essa questão o estudante deve olhar os valores das letras da mensagem original numa tabela igual a tabela 2.7 e adiconar 2, ou seja, utilizando a fórmula: $y = x + 2$, x representa o valor da letra da mensagem inicial e y da letra cifrada. As demais perguntas seguem essa mesma organização, porém utilizando outras funções e aumentando gradativamente o grau de complexidade.

Nem todos os trabalhos analisados foram aplicados para verificar os resultados com os estudantes e/ou professores, mas todos avaliam as propostas de forma positiva,tendo em vista que podem tornar as aulas mais atrativas, instigando os estudantes a questionar, investigar e procurar soluções. Além disso, o uso da criptografia contextualiza, de forma histórica e prática, os conceitos matemáticos, como cita Santos (2013):

> A temática apresentada neste trabalho é naturalmente vocacionada a um contexto histórico do desenvolvimento da ciência e tecnologia, além de apropriar-se de conceitos matemáticos que podem ser desenvolvidos em atividades acessíveis aos estudantes do Ensino médio, retirando a matemática do isolamento didático que tradicionalmente se confina no contexto escolar (SANTOS, 2013, p. 78).

Somada a indicação das propostas práticas, nessas pesquisas há um referencial teórico que apresenta o contexto histórico da criptografia, técnicas de cifragem e, na maioria, uma explanação sobre funções. Assim, o docente pode se fundamentar para compreender melhor o tema e, dessa maneira, trabalhar com mais segurança as questões propostas e/ou elaborar novas atividades.

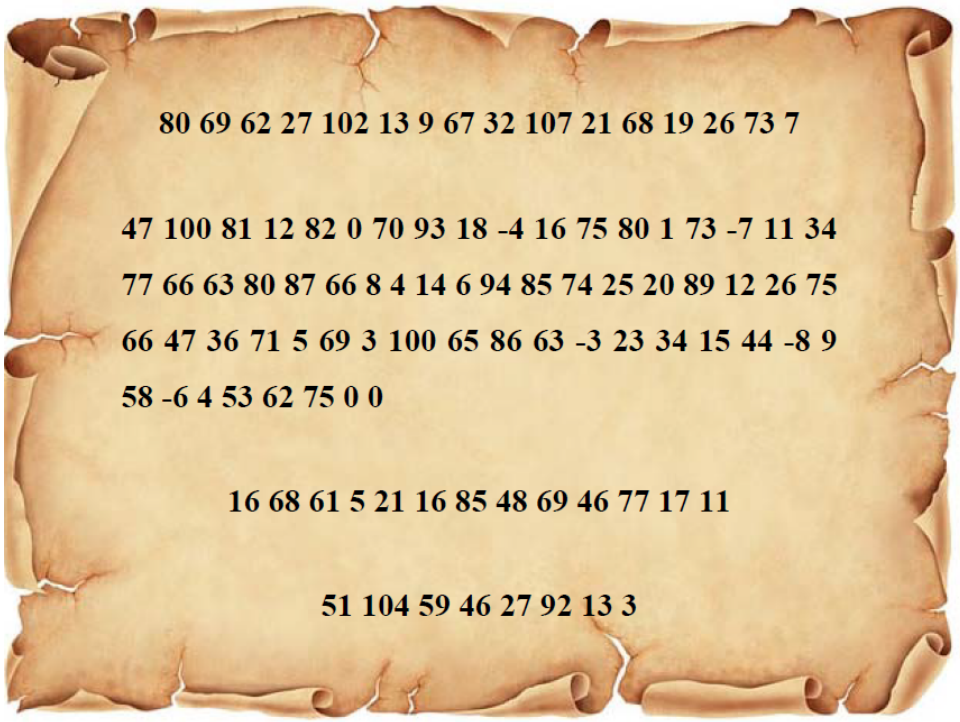
2.1.2 Matrizes

As pesquisas analisadas que relacionaram criptografia e matrizes, no total de dez trabalhos, também justificam a escolha do tema pela necessidade de contextualizar as aulas

de matemática, tornando a aprendizagem mais dinâmica e proporcionando a percepção da importância dos conteúdos trabalhados para a resolução de problemas reais, pois conforme Schurmann (2013), pesquisa 1, os conceitos de matrizes estão estruturados por meio de regras sem nenhuma conexão com o cotidiano dos alunos.

Desses trabalhos, dois deles tem como foco somente o ensino-aprendizagem de matrizes e apresentam propostas que podem favorecer a interdisciplinaridade com outras áreas, apesar delas não serem desenvolvidas nessa perspectiva. No caso de Schurmann (2013), a proposta pedagógica é desenvolvida a partir da releitura simplificada do drama Romeu e Julieta de Shakespeare feita pela escritora Silvia Regina Costa Lima. Apresenta-se o texto com as aventuras dos personagens e, em seguida, as trocas de mensagens entre eles são problematizadas por meio da criptografia matricial, a exemplo da figura 2.2. Assim, ao longo da narrativa, o autor elabora cinco atividades envolvendo criptografia que consistem em codificar ou decodificar mensagens usando números primos, matrizes, operações com matrizes, matriz transposta e matriz inversa.

Figura 2.2: Mensagem criptografada por Julieta



Fonte: Schurmann (2013, p. 37).

Para realizar a decodificação das mensagens, conforme a da figura 2.2, os estudantes são orientados a seguir os passos combinados entre os personagens, descritos aqui de forma resumida:

1 Faz a contagem de quantos números estão escritos na mensagem codificada, organiza numa tabela com número de linhas igual ao número de colunas e reescreve na forma

de uma matriz quadrada A. No caso da mensagem da figura 2.2 será uma matriz 10×10;

2 Escreve outra tabela de mesma dimensão da primeira, procedendo da seguinte forma: na primeira linha escreve números inteiros positivos em ordem crescente iniciando em 1 (na mensagem considerada será do 1 ao 10); Na segunda linha escreve os mesmos números inteiros positivos, mas em ordem decrescente (do 10 ao 1); na terceira linha escreve os números inteiros negativos em ordem decrescente, iniciando em -1 (-1 ao -10); e na quarta linha, escreve os mesmos números inteiros negativos em ordem crescente (-10 ao -1). Procede-se obedecendo as regras das quatro primeiras linhas até preencher toda a tabela e reescreve como a matriz B, também 10×10;

3 Realiza a operação $B - A$ para encontrar os valores numéricos originais usados por Julieta, obtendo outra matriz 10×10;

4 Troca os valores pelas letras e símbolos correspondentes utilizando a tabela 2.4, obtendo a mensagem da figura 2.3.

Tabela 2.4: Códigos Utilizados por Romeu e Julieta

	?	!	,	A	B	C	D	E	F	G	H	I	J	K
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47

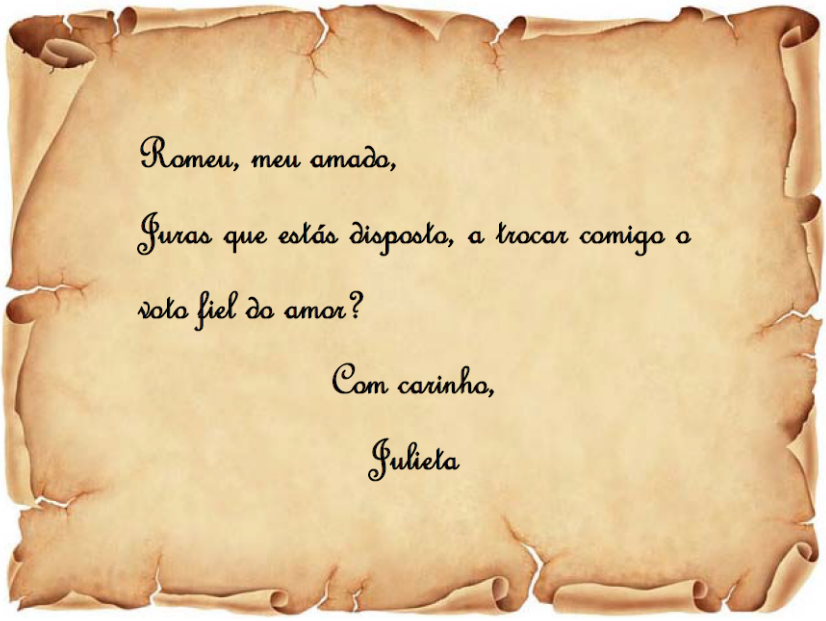
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113

Fonte: Schurmann (2013, 37).

Para decodificar mensagens deve ser feita uma pré-codificação usando a tabela 2.4, organizar os valores em uma tabela com o número de linhas igual ao de colunas, formando a matriz A que será somada com a matriz B. Nesse trabalho são propostas mais quatro atividades com essa mesma organização, nas quais os estudantes terão que desenvolver cálculos como adição, subtração e multiplicação de matrizes, além de determinar a matriz inversa.

A proposta de Oliveira (2013), pesquisa 4, tem como metodologia a engenharia didática e foi aplicada numa turma do 2º ano do Ensino Médio por um período de 100 minutos usando ditos populares criptografados para trabalhar matrizes. A aula foi iniciada com uma conversa sobre criptografia e seus usos, seguida de uma provocação para os alunos decifrarem as seguintes mensagens: **ASDQUNTEUNTADECERONA** e **AOFUFONARIZÇÃAA**. Apesar de nenhum aluno ter conseguido decifrar essas mensagens, o autor relata que o objetivo foi alcançado, pois conseguiu despertar o interesse dos educandos para outras atividades.

Figura 2.3: Mensagem Decodificada por Romeu



Fonte: Schurmann (2013, p. 41)

Para decodificar tais mensagens, o autor dispôs essas letras em tabelas que no primeiro caso poderia ser 1×20, 20×1, 2×10, 10×2, 4×5 ou 5×4) e no segundo (1×15, 15×1, 3×5 ou 5×3). As duas primeiras possibilidades são descartadas, pois não embaralha as letras. O estudante poderia escrever as letras obedecendo as outras organizações até conseguir decodificar as mensagens. Nesse caso, foram utilizadas as respectivas tabelas:

Tabela 2.5: ASDQUNTEUNTADECERONA

A	S	D	Q	U
N	T	E	U	N
T	A	D	E	C
E	R	O	N	A

Fonte: Adaptado de Oliveira (2013, p. 47).

Tabela 2.6: AOFUFONARIZÇÃAA

A	O	F
U	F	O
N	A	R
I	Z	Ç
Ã	A	A

Fonte: Adaptado de Oliveira (2013, p. 47).

Fazendo a leitura na vertical ou escrevendo a matriz transposta, temos as mensagens:

ANTES TARDE DO QUE NUNCA e A UNIÃO FAZ A FORÇA, respectivamente. Após explicar como foi feita essa decodificação e fazer uma explanação sobre o conteúdo, o pesquisador propôs a decodificação e codificação de outros ditos populares.

Uma das atividades propostas por Santos (2013), pesquisa 3, também explora a multiplicação de matrizes, matrizes invertíveis e cálculo da inversa de uma matriz 2×2. A pré-codificação das letras do alfabeto é feita conforme tabela 2.3. Para cifrar mensagens, utiliza-se uma matriz A, 2×2, que será a chave da cifra e a matriz $M_{2\times n}$ preenchendo as colunas de cima para baixo e da esquerda para a direita com as letras da mensagem. Assim, a mensagem cifrada é dada por: $C = A \times M$ e para decifrar utiliza-se a expressão: $M = A^{-1} \times C$. Utilizando esses mesmos passos, França (2014), Ganassoli e Schankoski (2015), Santos (2015), Jansen (2016)e Silva (2019) também propõem questões para serem aplicadas com alunos do Ensino Médio envolvendo a cifragem e decifragem de mensagens, por meio de matrizes.

Loureiro (2014) e Araujo (2017) também apresentam questões para estudantes do Ensino Médio que envolvem multiplicação de matrizes, cálculo da matriz inversa e cálculo do determinante, mas sob a abordagem da Cifra de Hill. Por exemplo, na atividade proposta por Loureiro (2014),pesquisa 6, no ítem **a** solicita a codificação da palavra **MATEMÁTICA** utilizando a cifra de Hill e a chave:

$$\mathbf{K} = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$$

Como a chave é uma matriz de ordem 2, a palavra é dividida em blocos de duas letras que serão substituídas pelos valores posicionais em ordem crescente, tomando A=0. Esses valores serão escritos na forma de uma matriz coluna da seguinte forma:

$$\mathbf{P_1} = \begin{pmatrix} 12 \\ 0 \end{pmatrix}, \mathbf{P_2} = \begin{pmatrix} 10 \\ 4 \end{pmatrix}, \mathbf{P_3} = \begin{pmatrix} 12 \\ 0 \end{pmatrix}, \mathbf{P_4} = \begin{pmatrix} 19 \\ 8 \end{pmatrix} e\ \mathbf{P_5} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

Cada uma dessas colunas será multiplicada pela chave:

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \times \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 60 \\ 24 \end{pmatrix} mod\ 26 = \begin{pmatrix} 8 \\ 24 \end{pmatrix} = \begin{pmatrix} I \\ Y \end{pmatrix}$$

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \times \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 119 \\ 50 \end{pmatrix} mod\ 26 = \begin{pmatrix} 15 \\ 24 \end{pmatrix} = \begin{pmatrix} P \\ Y \end{pmatrix}$$

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \times \begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 143 \\ 62 \end{pmatrix} mod\ 26 = \begin{pmatrix} 13 \\ 10 \end{pmatrix} = \begin{pmatrix} N \\ K \end{pmatrix}$$

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \times \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 10 \\ 4 \end{pmatrix} = \begin{pmatrix} K \\ E \end{pmatrix}$$

Então, a mensagem cifrada é IYPYNKKE. Para decifrar uma mensagem, segue-se o mesmo processo, mas utlizando a matriz K^{-1}. Na dissertação, talvez por engano, o autor utilizou a matriz:

$$\mathbf{K} = \begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}$$

para fazer a cifragem, dado que ele questiona no item c se esta matriz seria uma boa escolha para o ítem a, porém não tem como calcular a sua inversa, pois seu determinante é zero. Logo, não teria como fazer a decodificação, não sendo uma boa escolha.

Dentre os autores citados nesta subseção, Oliveira (2013), pesquisa 4, foi um dos pesquisadores que aplicou as atividades com estudantes do 2º ano do Ensino Médio e sua análise posteriori mostrou que eles foram atraídos pelo exercício e se empenharam na resolução dos enigmas, após compreenderem que seriam solucionados por meio de matrizes. O autor afirma que a experiência ocorreu conforme planejado, mesmo que alguns dos discentes não tenham se envolvido com a atividade e isso aconteceu por motivos como: cansaço em relação as metodologias tradicionais e falta de objetivos com os estudos.

2.1.3 Análise combinatória

Dos trabalhos analisados, nenhum deles focou exclusivamente em conteúdos de análise combinatória, mas quatro apresentam atividades que relacionam tal saber com criptografia.

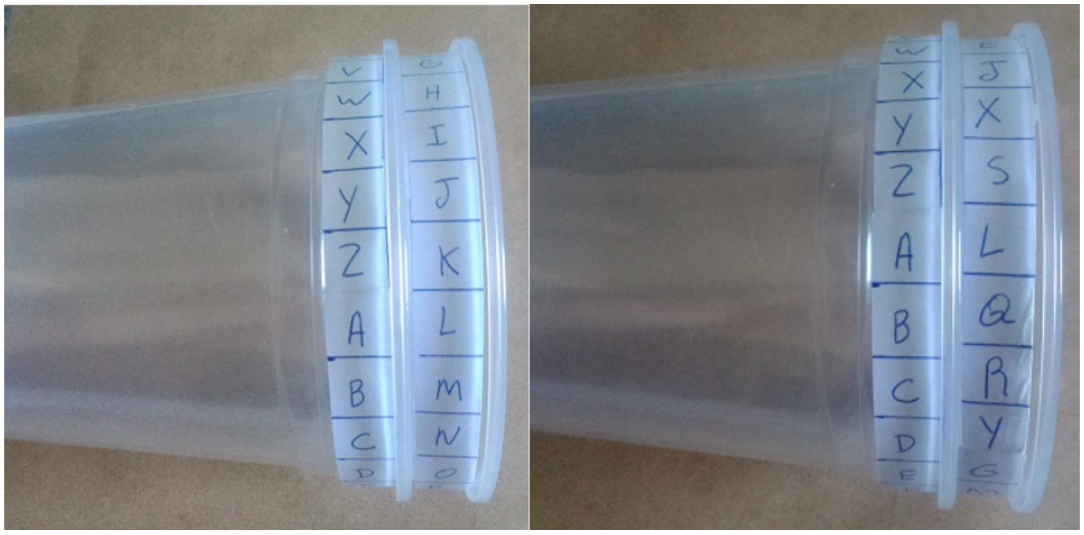
A atividade desenvolvida por Loureiro (2014),pesquisa 6, envolveu uma versão simples da cifra ADFGVX, utilizada no final da 1ª Guerra Mundial para elaborar uma questão sobre permutação, na qual ele solicita a quantidade de chaves da cifra ADFGVX. Como há 36 símbolos distintos, há 36! possibilidades para a chave.

Matsumoto (2014), pesquisa 7, apresenta atividades relacionadas a cifra de César, uma delas envolve análise de frequência das letras do alfabeto na língua portuguesa que, segundo a autora, consiste num método para decodificar mensagens, uma vez que as letras, em geral, sempre aparecem com a mesma frequência nos textos. A proposta envolve a análise de frequência das letras na música Aquarela de Toquinho e a decifragem de um texto utilizando esse método. Dessa forma, os participantes precisam contar as letras para descobrir as que mais aparecem e relacionar com a frequência aproximada das letras em português para definir a função utilizada para cifrar o texto e, assim, por meio do disco construído anteriormente decodificam as demais letras.

Na proposta de Carvalho (2016), pesquisa 15, o conceito de permutação pode ser trabalhado por meio de um kit de encriptação e descriptação que, segundo o autor, tem como base um vídeo do *Youtube* do Massachusetts Institute of Techonogy, conforme figura 2.4 . O kit usa dois copos descartáveis, um dentro do outro e duas tiras de papel, uma em cada copo, que num primeiro momento contém as 26 letras do alfabeto na sequência. O professor explica a Cifra de César e como utilizar o kit, enquanto os alunos

em grupo, utilizam o *Whatsapp* para a troca de mensagens que são criptografadas por meio do deslocamento das letras escrtitas nas tiras de papel. Ao final dessa etapa, os estudantes devem perceber que não é tão difícil decifrar a mensagem secreta, porque só há 26 possibilidades. Na sequência, uma das tiras é substituída por outra com o alfabeto escrito de forma aleatória e após criptografar e descriptografar mensagens espera-se que os alunos percebam que o processo ficou mais difícil, pois com o novo kit há 26! possibilidades.

Figura 2.4: Kit para Criptografar e Descriptografar Mensagens



Fonte: Carvalho (2016, p. 70-74).

2.1.4 Aritmética modular

A aritmética modular não faz parte do currículo da Educação Básica, mas segundo os autores abordados nessa subseção, as sugestões de atividades levaram em consideração o nível dos alunos e têm como obetivo atrelar conceitos como divisão euclidiana, congruência e criptografia, tendo em vista uma aprendizagem matemática mais significativa e contextualizada.

Dessa forma, o trabalho de Griseli (2018), pesquisa 21, tem por objetivo motivar os professores e, por meio deles, os alunos para o estudo da criptografia relacionada a aritmética. Tem como sujeitos da pesquisa, professores da Educação Básica e se apoia na problemática de que as dificuldades dos alunos decorrem, entre outros fatores, da falta de contextualização do conteúdo abordado. Nesse caso, a criptografia é concebida como ferramenta motivadora para trabalhar conceitos de aritmética com alunos do 6º ao 9º ano.

Na prática, a pesquisa consistiu na realização de uma oficina com professores para que estes pudessem se apossar do material, verificando sua aplicabilidade com estudantes do 6º ao 9º ano do Ensino Fundamental. De acordo com o autor, a sequência de sete atividades apresenta um aumento gradativo no grau de dificuldade e aborda a história da criptografia, faz conexões entre criptografia e conceitos matemáticos, considera o conhecimento prévio

do aluno e estimula o raciocínio lógico e a aprendizagem.

Nas duas primeiras atividades trabalhou-se a cifra de transposição e de substituição, nas quais, além da parte teórica, os professores construíram uma cítala caseira e o kit de encriptação e descriptação já citado no trabalho de Carvalho (2016). Em seguida, nas atividades 3 a 7 foi trabalhado conceitos aritméticos como o algoritmo da divisão, uso de relógio para calcular o resto da divisão e abordar congruência e os conceitos aritméticos para codificação e decodificação da critptografia RSA. Griseli (2018) conclui afirmando que a oficina foi aceita de forma satisfatória pelos docentes que citam como desafios para sua implementação a quantidade de alunos por turma e a heterogeneidade.

Araujo (2017), pesquisa 17, cita que a maioria dos livros didáticos privilegiam a conceituação e não a aplicação de conteúdos e, com isso, utilizam muitas fórmulas distantes do contexto do estudante que, consequentemente, demonstra desinteresse e dificuldades em aprender, levando o ensino da matemática ao fracasso. Assim, a pesquisa do referido autor, teve por objetivo:

> Aplicar de forma contextualizada e integrada a outros conhecimentos alguns métodos criptográficos, de tal forma que ofereça ao professor uma ferramenta de trabalho que o possibilite desenvolver alguns conceitos abordados no ensino médio, de forma mais eficaz, oferecendo assim aos alunos, a oportunidade de uma aprendizagem significativa destes temas (ARAUJO, 2017, p. 4).

A proposta é direcionada para alunos do segundo ano do Ensino Médio e dentre os conteúdos trabalhados, aborda-se congruência, algoritmo de Euclides e criptografia RSA que também envolve números primos, fatoração, aritmética modular, algoritmo de Euclides e Fermat. As atividades são estruturadas com uma questão e o passo a passo para solucioná-la. Em algumas delas há sugestão para trabalhar em grupo e uma das atividades sobre a criptografia ElGamal há indicação de uma calculadora online para o cálculo de logaritmos discretos.

Araujo (2017) não aplica as atividades na prática, mas conclui afirmando que a criptografia faz parte do cotidiano dos alunos e pode ser eficaz e motivador para que alunos do Ensino Fundamental e Médio desenvolvam conceitos matemáticos. Comungando dessa mesma ideia, Silva (2016), pesquisa 12, aplicou uma sequência de atividades com alunos do 8º e 9º ano do Ensino Fundamental, onde ele apresentou a aritmética modular com suas definições básicas, proposições, exercícios de fixação e questões de concursos de nível fundamental; o contexto histórico da criptografia; e o Sistema RSA como aplicação da aritmética modular.

Consoante esse autor, a abordagem de tópicos que não constam no currículo da Educação Básica, a exemplo da aritmética modular, são pertinentes e viáveis para dar significado ao estudo de conteúdos como: sistema de numeração, divisibilidade, números primos e resolução de equações. Ao final do trabalho, os alunos responderam um questionário

avaliando a prática e, os resultados evidenciaram que os estudantes nunca tinham ouvido falar ou nem imaginavam que havia relação entre matemática e criptografia, além disso os relatos mostraram que eles se interessaram pelo tema.

Uma proposta similar para o 3º ano do Ensino Médio é descrita por Pinheiro (2018), pesquisa 20, por meio de uma sequência de sete aulas de cinquenta minutos, distribuídas em quatro planos de aula. Inicialmente, ela propõe a instalação do *software* MAXIMA nos *notebooks* ou do aplicativo Maxima on Android. Os conteúdos estão distribuídos da seguinte forma:

- Plano 1 (2 aulas): a importância da criptografia RSA na atualidade, números primos, trocas de mensagem;
- Plano 2 (2 aulas): congruência e inversos modulares;
- Pano 3 (2 aulas): Princípio da Indução Finita, Teorema Fundamental da Aritmética e Pequeno Teorema de Fermat;
- Plano 4 (1 aula): Sistema RSA.

Nos planos, ainda há sugestão dos vídeos sobre aritmética do Portal Matemático da OBMEP. Por fim, a autora cita que essa proposta didática visa a aplicação, em sala de aula, dos conceitos estudados na dissertação, cujo intuito é despertar o interesse em aprender matemática, debatendo um tema atual por meio da experimentação. Nos apendices e anexos, também apresenta orientações para a troca de mensagens secretas e sugestões de atividades para trabalhar os conteúdos em sala de aula.

Ao contrário dos outros pesquisadores, o trabalho de Machado (2018), pesquisa 18, foi aplicado com alunos do 8º e 9º ano do Ensino Fundamental de um colégio militar que já apresentavam bons resultados em matemática. Eles fazem parte de um Clube de Matemática e grande parte são medalhistas nas olimpíadas de matemática. No entanto, apesar da facilidade em aprender os conteúdos, questionavam sobre a aplicabilidade de temas envolvendo Números Primos e Aritmética Modular. Diante disso, foi criada uma sequência de 13 planos, cada um com duas aulas, sobre Criptografia RSA.

A proposta levou em consideração o nível dos alunos e foi aplicada em forma de um minicurso com o título: "Criptografia RSA e Teoria dos Números". Sendo utilizados como metodologias: apresentações no *powerpoint*, uso de aplicativos para *smartphone*, como o Decrypto que criptografa e descriptografa mensagens em várias cifras, o Módulo Calculator, o *software Microsoft Excel*, exercícios diversos (inclusive com questões da OBEMP e OBM) e discussão das questões.

De acordo com o autor, os alunos trabalharam em duplas e não demonstraram dificuldades na resolução das questões e se mostraram entusiasmados pelo tema, principalmente ao atrelar criptografia e os recursos tecnológicos. Cita também, que por trabalhar com um

público especial, houve demanda de um planejamento mais complexo e indica melhorias para a proposta como, diminuir o número de aulas, focar mais no método RSA e melhorar o conteúdo da apostila.

Castro (2015), pesquisa 11, aplicou uma pesquisa com estudantes do Ensino Fundamental (9ºano) e Médio de uma escola particular com o objetivo de mostrar aos alunos o quão simples e elegantes podem ser algumas teorias, como os conceitos relacionados a Criptografia RSA, trabalhados de forma compatível com o nível dos alunos e com aplicações utilizadas no cotidiano.

A metodologia utilizada foi a Engenharia Didática que se "baseia na concepção, realização, observação e análise da sequência de ensino, confrontando análises a priori e análises posteriori" (CASTRO, 2015, p. 38). As atividades foram aplicadas em dois dias com carga horária de 3 horas, com os seguintes passos: exposição de um material teórico sobre criptografia primitiva, expondo seus problemas e fragilidades, além da abordagem histórica do sistema RSA; explicação das bases do RSA, indicando o passo a passo para os alunos criarem chaves públicas e privadas; em grupos, os alunos recebem dois números primos distintos para determinar chaves públicas e privadas para criptografar a palavra CÓDIGO.

Na pesquisa 13, Jansen (2016) aborda-se conceitos de aritmética nas atividades 7 e 8 ao solicitar a codificação da palavra MATEMÁTICA por meio do RSA e decodificação da mensagem 6355-4947 codificada pelo método RSA utilizando $n = 7597$, $e = 4947$ e $\varphi(n) = 7420$.

A partir de atividades com a Cifra de César, Matsumoto (2014), pesquisa 7, aborda ideias de congruência, divisibilidade e MDC, por meio de diversas transformações com a expressão: $ax + b$ para verificar quais expressões podem ser usadas para criptografar. Como os números de 0 a 25 correspondiam as letras de A a Z, as transformações eram feitas da seguinte forma: se o número obtido com a expressão do tipo $ax + b$ fosse maior que 25, dividia esse número por 26 e considerava o resto ($*ax + b \, mod \, 26$), conforme exemplos a seguir, nos quais verifica-se que é possível criptografar mensagens com a expressão $5x$, mas o mesmo não acontece para $6x + 1$, pois letras diferentes levam ao mesmo resultado.

Tabela 2.7: Correspondência Alfabeto - Números

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Elaboração da autora.

Tabela 2.8: Transformações com as Expressões $5x$ e $6x + 1$

$5x$	*		$6x + 1$	*	
0	0	A	1	1	B
5	5	F	7	7	H
10	10	K	13	13	N
15	15	P	19	19	T
20	20	U	25	25	Z
25	25	Z	31	5	F
30	4	E	37	11	L
35	9	J	43	17	R
40	14	O	49	23	X
45	19	T	55	3	D
50	24	Y	61	9	J
55	3	D	67	15	P
60	8	I	73	21	V
65	13	N	79	1	B
70	18	S	85	7	H
75	23	X	91	13	N
80	2	C	97	19	T
85	7	H	103	25	T
90	12	M	109	5	F
95	17	R	115	11	L
100	22	W	121	17	R
105	1	B	127	23	X
110	6	G	133	3	D
115	11	L	139	9	J
120	16	Q	145	15	P
125	21	V	151	21	V

Fonte: Elaboração da autora.

Após discorrer sobre congruência, algoritmo de Euclides e o Teorema de Femat, Ganassoli e Schankoski (2015), pesquisa 9, propõem atividades para o Ensino Fundamental e médio envolvendo esses conteúdos. O primeiro nível tem como uma das situações: "O relógio está marcando 8:00, e ainda é de manhã, minha mãe me avisou que daqui a 9 horas tenho consulta médica" (GANASSOLI; SCHANKOSKI, 2015, p. 55), para questionar sobre o horário da consulta, sobre o horário se o relógio contasse de 12 em 12 horas e sobre a relação estabelecida no algoritmo da divisão. São propostas mais questões envolvendo esse algoritmo, congruência, além da cifragem e decifragem de mensagens utilizando tais conteúdos, como no exemplo a seguir:

7- Cifre NÚMERO, sendo o quociente 2, o divisor é 26 e o resto é o

valor de cada letra da palavra, e o dividendo é a cifra. Substituição: 13 - 20 - 12 - 4 - 17 - 14 Processo:

$$\text{dividendo} = 2.26 + 13 \longrightarrow \text{dividendo} = 65$$

$$\text{dividendo} = 2.26 + 20 \longrightarrow \text{dividendo} = 72$$

$$\text{dividendo} = 2.26 + 12 \longrightarrow \text{dividendo} = 64$$

$$\text{dividendo} = 2.26 + 4 \longrightarrow \text{dividendo} = 56$$

$$\text{dividendo} = 2.26 + 17 \longrightarrow \text{dividendo} = 69$$

$$\text{dividendo} = 2.26 + 14 \longrightarrow \text{dividendo} = 66$$

Mensagem Cifrada: 65 - 72 - 64 - 56 - 69 - 66 (GANASSOLI; SCHANKOSKI, 2015, p. 58).

Para o nível II (Ensino Médio), inicialmente, são propostos vários cálculos de divisões e sua representação por meio do algorítmo de Euclides e, na sequência, diversos problemas envolvendo tal conhecimento, além da cifragem e decifragem de mensagens com mais complexidade do que o exemplo citado anteriormente, pois há introdução das fórmulas: $C \equiv a.P + k \mod 26$ para cifrar e $P \equiv \overline{a}.(C - k) \mod 26$ para decifrar, sendo:

- P- número da letra original
- C - número da letra cifrada
- a - número inteiro tal que $(a, 26) = 1$
- k - número positivo
- $\overline{a}$ - inverso de a, ou seja, $a.\overline{a} = 1 \mod 26$

As pesquisadoras também apresentam atividades envolvendo o sistema RSA, mas alertam que é um método mais complexo e só deve ser trabalhado se o professor perceber que os alunos têm preparação para compreenderem o processo de cifragem e decifragem. No entanto, deve ser mostrada aos estudantes do Ensino Médio, objetivando a percepção da importância de pesquisas matemáticas para o cotidiano.

2.1.5 Considerações sobre a análise dos trabalhos

Os trabalhos analisados, em geral, apresentam o contexto histórico da criptografia e o embasamento teórico dos conteúdos abordados que poderão servir como material de estudo para os professores ou demais interessados no assunto. Também indicam sugestões de atividades relacionando conhecimentos matemáticos e criptografia que podem ser adaptadas de acordo com a realidade de cada turma, além de servir como apoio para elaboração de atividades similares.

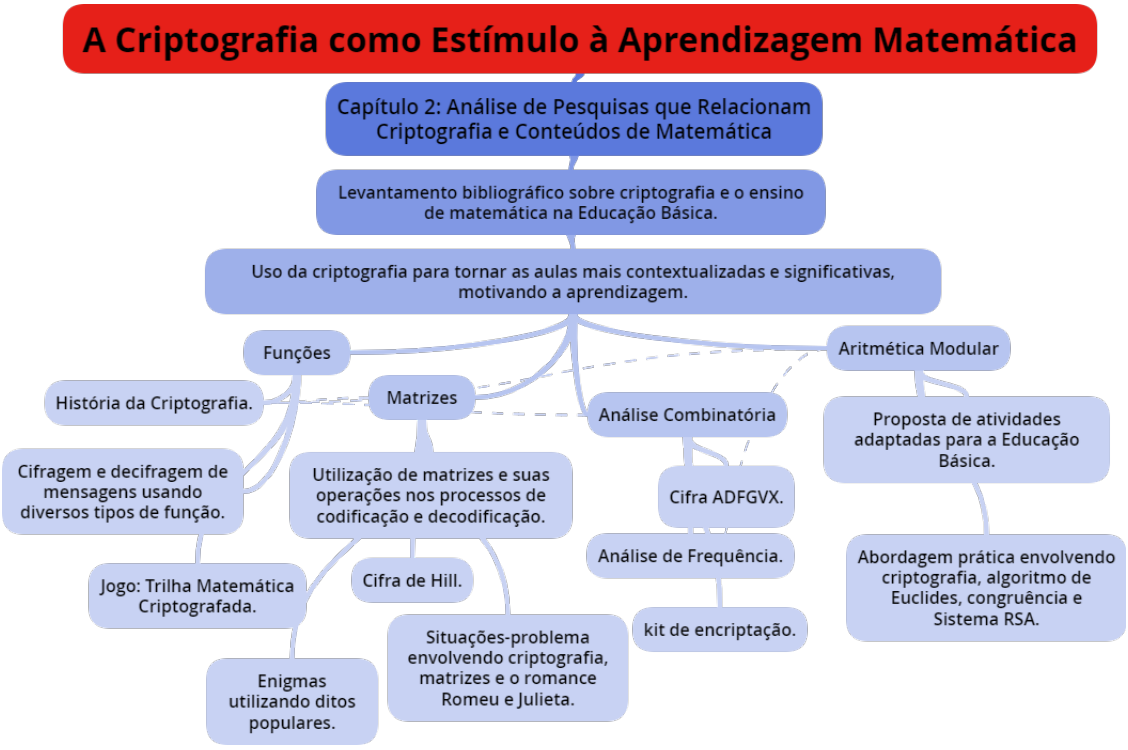
A pesquisa 16, de Bomfim (2017), tem por objetivo "refletir sobre a própria prática e buscar uma transformação no ensino aprendizagem para se proporcionar uma aprendizagem mais significativa na introdução do ensino da álgebra" (BOMFIM, 2017, p. 4). Mas,

são descritas apenas as atividades envolvendo técnicas de criptografia que também são interessantes para trabalhar em sala de aula. A autora escolhe o cinema e a história da matemática como organizadores prévios para uma sequência didática que, de início, os estudantes foram instigados a descobrir uma mensagem secreta num bilhete entregue a cada um deles. Nas outras atividades, trabalhou o conceito de criptografia, o filme O Jogo da Imitação, cifras de transposição, de substituição e a enigma.

Essa autora avaliou a aplicação da sequência de forma positiva, pois segundo ela o filme aproximou o aluno do conteúdo, permitindo a problematização, a investigação e a interpretação de fatos, de modo que os alunos foram protagonistas na construção do conhecimento. Também cita, assim como as demais pesquisas aqui analisadas, que a história da matemática pode inspirar a elaboração de atividades mais contextualizadas, propiciando discussões mais amplas, a conexão com outras disciplinas e, consequentemente, aprendizagens mais significativas.

Pode-se concluir que as pesquisas analisadas, com exceção a de Machado (2018), partem de problemáticas como as dificuldades dos estudantes em matemática, o uso de metodologias tradiconais que não contribuem para a contextualização do conteúdo, tornando-o estanque e sem significado para o estudante que acaba se sentindo desmotivado. Assim, as atividades propostas tem como tema criptografia com o intuito de motivar a aprendizagem dos conteúdos matemáticos, possibilitando o diálogo entre esses saberes e sua construção histórica, como também o reconhecimento de sua importância para a sociedade. Na sequência, há um mapa mental com as principais abordagens desse capítulo.

Figura 2.5: Mapa Mental - Capítulo 2



Fonte: Elaboração da autora.

3 Criptografia e Matemática

Este capítulo versa sobre conceitos matemáticos necessários para a compreensão de métodos criptográficos abordados no capítulo I: cifra monoalfabética, como a de Júlio César e o código RSA. Assim, apresentaremos alguns resultados da Teoria dos Números, tendo como referências Coutinho (2005), Hefez (2005) e Shokranian (2012).

3.1 Representação de um número inteiro

Os conjuntos dos Números Naturais e Inteiros são denotados, respectivamente, por:

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

e

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

.

Para escrever números inteiros utiliza-se o sistema de numeração posicional, no qual o valor de cada algarismo depende da posição ocupada. Usualmente, são representados por meio do sistema de numeração decimal que emprega os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 ou 9. Como são dez caracteres, diz-se que é um sistema de base 10. No entanto, há outras bases de numeração utilizadas, como a binária que é muito útil para a linguagem computacional e só utiliza dois dígitos, o zero e um.

Teorema 3.1 (Representação na base b)**.** Sejam a,$b \in \mathbb{N}$ e $b > 1$. Se $a \neq 0$, então existem números naturais r_0,$r_1, \cdots, r_n$ menores que b, univocamente determinados, tais que $a = r_n b^n + r_{n-1} b^{n-1} + \ldots + r_2 b^2 + r_1 b + r_0$.

Em particular, dado um número $a = n_1, n_2, \ldots, n_k$, na base decimal, ele pode ser escrito da seguinte forma:

$$a = n_1 \times 10^{k-1} + n_2 \times 10^{k-2} + \ldots + n_k \times 10^{k-k}$$

$$a = n_1 \times 10^{k-1} + n_2 \times 10^{k-2} + \ldots + n_k$$

Exemplo 3.1.1. Considere $a = 52345$, então k = 5 é a quantidade de algarismos deste

número, cuja representação decimal é a seguinte:

$$52345 = 5 \times 10^4 + 2 \times 10^3 + 3 \times 10^2 + 4 \times 10^1 + 5 \times 10^0$$

$$52345 = 50000 + 2000 + 300 + 40 + 5$$

Exemplo 3.1.2. Agora tome o número binário $a = 1101$. Sua representação na base 2 é feita da mesma forma dos números decimais, porém considerando o 2 ao invés do 10.

$$a = 1101 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

Logo, na base decimal esse número corresponde ao 13. Isso significa que é possível escrever um número decimal em binário e vice-versa. Para compreender melhor a expansão de qualquer número numa base b será necessário conhecimento sobre divisibilidade e alguns teoremas relacionados com esse conteúdo, como a Divisão Euclidiana.

3.2 Divisibilidade

Sejam $a, b \in \mathbb{Z}$ e $b \neq 0$, b divide a quando existe um inteiro c tal que $a = bc$. Escreve-se $b \mid a$ e diz-se que a é divisível por b. Caso b não divida a, escreve-se $b \nmid a$. Por exemplo, $(-5) \mid 10$, pois, existe $c = -2$, tal que $10 = (-5)(-2)$.

Considerando a um número natural, dizemos que seus divisores são todos os inteiros positivos b e c. Assim, os divisores de 30 são 1, 2, 3, 5, 6, 10, 15 e 30. Dessa forma, o número zero é divisível por qualquer inteiro não nulo, enquanto o 1 só possui um divisor, ele próprio.

Quando um número natural maior que 1 possui como divisores apenas o 1 e ele próprio, é chamado de primo. Do contrário, se possuir mais de dois divisores, ele é composto. Por exemplo, o 13 é primo, pois só se divide por 1 e 13 e o 12 é composto, pois se divide por 1, 2, 3, 4, 6 e 12.

Teorema 3.2. Sejam a, a', b, números inteiros.

i) Se $b \mid a$ e $b \mid a'$, então $b \mid (a + a')$, $b \mid (a - a')$, $b \mid (a' - a)$, $b \mid (aa')$,

ii) Se $k \mid b$ e $b \mid a$, então $k \mid a$ $k \in \mathbb{Z}$.

iii) Se $b \mid a$, então $b \mid at$, $t \in \mathbb{Z}$.

Demonstração. i) Como $b \mid a$ e $b \mid a'$, então $\exists$ c e $c' \in \mathbb{Z}$, tal que $a = bc$ e $a' = bc'$. Assim, $a + a' = b(c + c')$. Logo, $b \mid (a + a')$. Analogamente, prova-se as demais propriedades desse item.

ii) Como $k \mid b$ e $b \mid a$, então $\exists$ d e $c \in \mathbb{Z}$, tais que $b = kd$ e $a = bc$. Dessa forma, $a = (kd)c = k(cd)$. Logo, $k \mid a$.

iii) Se $b \mid a$, então $a = bc$, $(c \in \mathbb{Z})$. Tome $t \in \mathbb{Z}$, multiplicando os dois lados dessa igualdade por esse número. Assim, $at = bct$. Segue que $at = b(ct)$. Portanto, $b \mid at$.

□

Quando $b \nmid a$, sendo a e b números inteiros e $b \neq 0$, é sempre possível a divisão de a por b com resto r. Esse resultado é enunciado pelo Teorema abaixo, cuja demonstração pode ser encontrada em Hefez (2005).

Teorema 3.3 (Divisão Euclidiana)**.** Sejam a e b dois números inteiros com $b \neq 0$. Existem somente dois números, q e $r \in \mathbb{Z}$, tais que

$$a = bq + r, \text{ com } 0 \leq r < |b|.$$

Veja os exemplos:

Exemplo 3.2.1. O quociente e o resto da divisão de 13 por 2 são $q = 6$ e $r = 1$, ou seja, $13 = 2 \times 6 + 1$.

Exemplo 3.2.2. O quociente e o resto da divisão de -17 por 5 são $q = -4$ e $r = 3$, ou seja, $-17 = 5 \times (-4) + 3$.

Com essa compreensão, pode-se determinar a expansão de um número qualquer relativamente a base b por meio do algoritmo a seguir, o qual consiste em aplicar, sucessivamente, a divisão euclidiana, conforme explica Hefez (2005) :

$$a = bq_0 + r_0,\ r_0 < b,$$
$$q_0 = bq_1 + r_1,\ r_1 < b,$$
$$q_1 = bq_2 + r_2,\ r_2 < b,$$

e assim por diante. Como $a > q_0 > q_1 > ...$, deveremos, em certo ponto, ter $q_{n-1} < b$ e portanto, de

$$q_{n-1} = bq_n + r_n,$$

decorre que $q_n = 0$, o que implica $0 = q_n = q_{n+1} = q_{n+2} = ...$, e, portanto, $0 = r_{n+1} = r_{n+2} = ...$

Temos, então, que

$$a = r_0 + r_1 b + ... + r_n b^n \text{ (HEFEZ, 2005, p. 60).}$$

Exemplo 3.2.3. Representar o número 13 na base 2:

$13 = 6 \times 2 + 1$,

$6 = 3 \times 2 + 0$,

$3 = 1 \times 2 + 1$,

$1 = 0 \times 2 + 1$

Portanto, $13 = 1 + 0 \times 2 + 1 \times 2^2 + 1 \times 2^3$. Consequentemente, $13 = [1101]_2$.

Exemplo 3.2.4. Representar o número 827 na base 5:

$827 = 165 \times 5 + 2$

$165 = 33 \times 5 + 0$

$33 = 6 \times 5 + 3$

$6 = 1 \times 5 + 1$

$1 = 0 \times 5 + 1$

Logo, $827 = 2 + 0 \times 5 + 3 \times 5^2 + 1 \times 5^3 + 1 \times 5^4$, e assim, $827 = [11302]_5$.

Outro teorema importante para o estudo da criptografia diz que todo número composto pode ser escrito de forma única como produto de números primos. Chamado de Fatoração Única, será descrito a seguir e sua demonstração pode ser encontrada detalhadamente em Coutinho (2005, p. 35).

Teorema 3.4 (Fatoração Única)**.** Dado um inteiro positivo $n \leq 2$ podemos sempre escrevê-lo de forma única, como:

$$n = p_1^{e_1} \dots p_k^{e_k}$$

onde $1 < p_1 < p_2 < \cdots < p_k$ são números primos e $e_1, \dots, e_k$ são números inteiros positivos.

Existem alguns algoritmos para decompor um número composto em fatores primos e o mais usado na Educação Básica é descrito por Coutinho (2005) da seguinte maneira:

> **Algoritmo da fatoração**.
>
> **Entrada:** Inteiro positivo n.
>
> **Saída:** inteiro positivo f que é o menor fator primo de n ou uma mensagem indicando que ele é primo.
> **Etapa 1:** Comece fazendo $F = 2$.
>
> **Etapa 2:** Se n/F é inteiro escreva 'F é fator de n' e pare; senão vá para a etapa 3.
>
> **Etapa 3:** Incremente F de uma unidade e vá para a Etapa 4.
>
> **Etapa 4:** Se $F > \sqrt{n}$ escreva n é primo e pare; Senão volte a etapa 2 Coutinho (2005, p. 35).

Exemplo 3.2.5. Fatoração completa do número 792.

Aplicando o algoritmo, tem-se que o menor fator desse número é o 2. Em seguida, aplica-se o algoritmo novamente ao co-fator de 2 em 792 que é $792/2 = 396$, que tem o 2 como menor fator. Assim, $396/2 = 198$. Feito isso descobre-se que 2 também é fator de 198. Então, $198/2 = 99$. Logo, 2^3 é fator de 792 e ao aplicar o algoritmo mais três vezes, encontra-se 3^2 e 11 cujo co-fator é 1. Portanto, a forma fatorada do número dado é $792 = 2^3 \times 3^2 \times 11$.

Esse algoritmo é lento e, por isso, ineficiente para a fatoração de números muito grandes. De acordo com Coutinho (2005), a eficiência dos algoritmos depende do tipo de fator do número a ser fatorado, sendo importante o entendimento que não há um algoritmo que funcione bem em todos os inteiros e disto depende a segurança do método RSA.

3.3 Congruências

O entendimento de congruência também é essencial para o estudo da criptografia, a exemplo do sitema RSA. Recebe outras denominações como Aritmética dos Restos por Hefez (2005), operação módulo m por Shokranian (2012) e aritmética modular por Coutinho (2005).

Dois inteiros, a e b são congruentes módulo m se, e somente se,

$$m \mid (a - b)$$

Se $m \mid (a - b)$, diz-se que a e b são congruentes módulo m. Quando a e b forem congruentes módulo m, escreve-se:

$$a \equiv b \pmod{m}$$

Existem infinitos inteiros a congruentes ao inteiro b módulo m .

Exemplo 3.3.1. Tome $m = 7$ e $b = 1$, então a pode ser:

$$\ldots, -20, -13, -6, 1, 8, 15, \ldots$$

No geral, escreve-se os inteiros a congruentes com 1 módulo 7 da seguintes forma:

$$a = 1 + 7k, k \in \mathbb{Z}$$

Ou seja, a são todos os inteiros, em que o resto da divisão por 7 é 1. Dessa maneira, aplicando a divisão de Euclides, pode-se determinar um inteiro x para que o número dado a seja congruente com x módulo m.

Exemplo 3.3.2. Supondo $a = 457893$ e $m = 135$. Assim, $457893 \equiv b \pmod{135}$. Para encontrar o valor de b basta encontrar o valor de r na identidade $a = bq + r$. Logo,

$$457893 = 135 \times 3391 + 108,$$
$$457893 - 108 = 135 \times 3391.$$

Que pode ser reescrita como:

$$457893 \equiv 108 \pmod{135}$$

Portanto, b é o resto da divisão de a por m e, com isso, obtem-se o seguinte resultado:

Teorema 3.5. Dados a, $m \in \mathbb{Z}$, existe um único inteiro positivo x com $0 \leq x < m$ tal que

$$a \equiv x \pmod{m}$$

De acordo com Shokranian (2012, p. 10), "A cada inteiro positivo b, podemos associar um subconjunto infinito dos inteiros a ser chamado classes de b módulo m ou números $b \pmod m$". Logo, a classe do número b é o conjunto dos inteiros congruentes com b módulo m.

Dadas duas classes, $b \pmod m$ e $d \pmod m$, elas são iguais se, e somente se, $m \mid (b-d)$, ou seja,

$$b \pmod m = d \pmod m \Leftrightarrow b - d = 0 \pmod m.$$

No conjunto de classes módulo m é possível realizar as operações aritméticas da soma, multiplicação e divisão. As duas primeiras são mais fáceis de serem definidas. Considerando $b \pmod m$ e $d \pmod m$, tem-se:

$b \pmod m + d \pmod m = b + d \pmod m$.

Exemplo 3.3.3. Ex. $1 \pmod 5 + 3 \pmod 5 = 4 \pmod 5$.

Temos também, $b \pmod m \times d \pmod m = bd \pmod m$.

Exemplo 3.3.4. $3 \pmod 5 \times 4 \pmod 5 = 2 \pmod 5$.

Em relação a divisão, no conjunto de números módulo m, Shokranian (2012) cita que, em princípio, é melhor definir a inversão.

Sejam $b \pmod m$ e $d \pmod m$, se $b \pmod m \times d \pmod m = 1 \pmod m$, então $d \pmod m$ é a inversa de $b \pmod m$. Para compreender classe inversa, é válido recordar o conceito de máximo divisor comum mdc entre dois inteiros a e b e duas proposições mencionadas por Shokranian (2012).

Como leciona Hefez (2005), dado um inteiro $d > 0$ é o mdc de a e b se possuir as seguintes propriedades:

i) d é divisor comum de a e b.

ii) d é divisível por todo divisor comum de a e b .

Proposição 3.1. Sejam a, b, $c \in \mathbb{Z}$. Então, existem inteiros x, y, tal que:

$$ax + by = c$$

se e somente se, $\text{mdc}\,(a, b) \mid c$.

Exemplo 3.3.5. Tome $a = 6$, $b = 8$ e $c = 2$, então existe x, $y \in \mathbb{Z}$, tais que $6x + 8y = 2$, pois $\text{mdc}\,(6, 8) = 2$ e $2 \mid 2$.

Proposição 3.2. Seja $b \neq 0$, um número inteiro, então a classe $b \pmod m$ tem inversa se, e somente se, $\text{mdc}\,(b, m) = 1$.

A demonstração para tal proposição pode ser encontrada em Shokranian (2012, 12 e 13) e, como o $\text{mdc}\,(b, m) = 1$ diz-se que os números são primos entre si ou coprimos.

3.3.1 Congruências Lineares

Congruência linear, denominada por Shokranian (2012) de equação afim e por Coutinho (2005) de equações lineares, é toda expressão do tipo:

$$ax \equiv b \pmod{m}, a,\ b,\ m \in \mathbb{Z}, m > 1.$$

Proposição 3.3. Dados $a,\ b,\ m \in \mathbb{Z}, m > 1$, a congruência $ax \equiv b \pmod{m}$ tem solução se, e somente se, o $\text{mdc}\,(a, m) \mid b$.

Demonstração. Suponha que a congruência $ax \equiv b \pmod{m}$ tenha solução, então existe $x_0 \in \mathbb{Z}$, tal que $ax_0 \equiv b \pmod{m}$, ou seja, $ax_0 + ym = b$, com $\in \mathbb{Z}$. Pela proposição 3.1, temos que $\text{mdc}\,(a,m) \mid b$.
Reciprocamente, considere que $\text{mdc}\,(a,m) \mid b$. A equação dada pode ser escrita como: $ax + (-y)m = b$, concluindo que $\text{mdc}\,(a, m) \mid b$ e, portanto, a congruência tem solução. □

Exemplo 3.3.6. A congruência $3x \equiv 6 \pmod{9}$ tem solução, pois $\text{mdc}\,(3, 9) = 3$ e $3 \mid 6$.

Com o objetivo de determinar o conjunto das soluções de uma congruência, Hefez (2005) enuncia o seguinte teorema:

Teorema 3.6. Sejam $a,\ b,\ m \in \mathbb{Z},\ m > 1$ e $\text{mdc}\,(a,m) \mid b$. Se x_0 é uma solução da congruência $ax \equiv b \pmod{m}$, então $x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$, onde $d = \text{mdc}\,(a,m)$, formam um sistema completo de soluções da congruência, duas a duas incongruentes módulo m.

Demonstração. Ver Hefez (2005, p. 213). □

Considere o exemplo dado anteriormente: $3x \equiv 6 \pmod{9}$. Como $d = \text{mdc}\,(3,9) = 3$ e $3 \mid 6$, a congruência tem $d = 3$ soluções módulo 9.

Por tentativa e erro, obtem-se $x_0 = 5$. Portanto, as soluções módulo a são: $5, 5 + \frac{9}{3}, 5 + 2\frac{9}{3} = 5,\ 8,\ 11$.

Corolário 3.1. Se $\text{mdc}\,(a,m) = 1$, então a congruência $ax \equiv b \pmod{m}$ tem apenas uma solução módulo m.

Assim, a congruência $ax \equiv 1 \pmod{m}$, sendo $\text{mdc}\,(a,m) = 1$ tem somente uma solução módulo m que será chamada de inverso multiplicativo módulo m.

De acordo com Hefez (2005):

> Uma solução da congruência $aX \equiv 1 \pmod{m}$ determina e é determinada por qualquer outra solução. Se considerarmos que

> duas soluções congruentes módulo m são, essencialmente, a mesma, temos a unicidade da solução da congruência $aX \equiv 1\ mod\ m$.
>
> Um sistema reduzido de resíduos módulo m é um conjunto de números inteiros $r_1, \ldots, r_s$ tais que
>
> a) $(r_i,\ m) = 1$, para todo $i = 1, \ldots, s$;
>
> b) $r_i \not\equiv r_j \pmod m$, se $i \neq j$;
>
> c) Para cada $n \in \mathbb{Z}$ tal que $(n,\ m) = 1$, existe i tal que $n \equiv r_i \pmod m$ (HEFEZ, 2005, p. 194).

Esse conjunto é denominado por Shokranian (2012) de números módulo m, sendo denotado por $\mathbb{Z}/m\mathbb{Z}$, então,

$$\mathbb{Z}/m\mathbb{Z} = \{0,\ 1,\ 2, \ldots, m-2, m-1\}$$

Daí obtem-se o subconjunto $(\mathbb{Z}/m\mathbb{Z})^*$ formado por todos os números coprimos com m, ou seja,

$$(\mathbb{Z}/m\mathbb{Z})^* = \{x \in \mathbb{Z}/m\mathbb{Z} \mid \text{mdc}\,(x, m) = 1\}.$$

Designa-se por $\varphi(m)$ a quantidade de inteiros $1 \leq x \leq m-1$ que são coprimos com m. Fazendo $\varphi(1) = 1$ define-se a função $\varphi : \mathbb{N} \to \mathbb{N}$, chamada função fi de Euler. Nesta função, $\varphi(m) \leq m-1$, para todo $m \leq 2$. Se m for um número primo, então $\varphi(m) = m-1$.

Exemplo 3.3.7. $\varphi(7) = 6$, pois 1, 2, 3, 4, 5, 6 forma um sistema reduzido de resíduos módulo 7.

Do contrário, se m for composto, possui um fator f, tal que $1 < f \leq n-1$. Assim, $\text{mdc}\,(f, m) > 1$. portanto, se m é composto, $\varphi(m) < m-1$. Shokranian (2012) enuncia um algoritmo para o cálculo de $\varphi(m)$ através do seguinte teorema:

> O número de elementos do conjunto $(\mathbb{Z}/m\mathbb{Z})^*$ é dado pela função φ de Euler, e esse número é igual a
>
> $$\varphi(m) = m \prod_{p|m} (1 - \tfrac{1}{p})$$
>
> na qual os números p representam os divisores primos de m contados sem repetição (SHOKRANIAN, 2012, p. 17-18).

Exemplo 3.3.8. Considere $m = 26$, o qual possui dois divisores primos $p = 2$ e $p = 13$. Logo,

$\varphi(26) = 26 \prod_{p|26} (1 - \frac{1}{p})$
$\varphi(26) = 26(1 - \frac{1}{2})(1 - \frac{1}{13})$
$\varphi(26) = 26 \times (\frac{1}{2}) \times (\frac{12}{13})$
$\varphi(26) = 12$

Dessa forma, há 12 números coprimos de 26 e, portanto, são invertíveis módulo 26 e a tabela a seguir mostra seus inversos.

Tabela 3.1: Inversos dos coprimos de 26

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Fonte: Elaboração da autora.

Teorema 3.7. Dados dois números inteiros positivos n e m, primos entre si, isto é, $\text{mdc}\,(n, m) = 1$, existe um elemento $x \in (\mathbb{Z}/m\mathbb{Z})^*$ tal que $\text{mdc}\,(x, m) = 1$ e $n \equiv x \pmod{m}$.

Demonstração. Como os possíveis restos da divisão de n por m são os elementos de $x \in (\mathbb{Z}/m\mathbb{Z})$, pela divisão euclidiana $n = mq + r$, sendo $q \in \mathbb{Z}$ e $r \in (\mathbb{Z}/m\mathbb{Z})$. Considerando, $\text{mdc}\,(r, m) \neq 1$, então $\text{mdc}\,(n, m) \neq 1$, o que é uma contradição. Logo, $\text{mdc}\,(x, m) = 1$ e $n \equiv x \pmod{m}$. □

Teorema 3.8. Sejam x, m, a, $b \in \mathbb{Z}$ e $m > 0$. Se $\text{mdc}\,(x, m) = 1$, então $ax \equiv bx \pmod{m} \Longrightarrow a \equiv b \pmod{m}$.

Demonstração. Por suposição $m \mid x(a-b)$, mas m e x só tem um divisor comum que é o número 1. Portanto, $m \nmid x$ e deve dividir $a-b$. Isso implica que $a \equiv b \pmod{m}$). □

Para entender o sistema RSA, ainda serão necessários mais alguns resultados da teoria dos números, como o Teorema de Euler e o Pequeno Teorema de Fermat, os quais são descritos, demonstrados e/ou exemplificados por Hefez (2005), Shokranian (2012) e Coutinho (2005).

Teorema 3.9 (Teorema de Euler)**.** Sejam a, m inteiros com $m > 0$ tal que $\text{mdc}\,(a, m) = 1$. Então,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Sejam $r_1, r_2, \ldots, r_{\varphi(m)}$ os elementos de $(\mathbb{Z}/m\mathbb{Z})^*$. Nesse conjunto temos os elementos 1 e $m-1 \in (\mathbb{Z}/m\mathbb{Z})^*$. Tome $r_1 = 1$ e $r_{\varphi(m)} = m-1$. Agora, considere o conjunto $j = \{ar_1,\ ar_2, ..., ar_{\varphi(m)}\}$, cujos elementos são dois a dois incongruentes módulo m. Pelo teorema 3.7, pode-se escrever:

$$\begin{gathered} ar_1 \equiv r_i \pmod{m} \\ ar_2 \equiv r_j \pmod{m} \\ \cdots \equiv \ldots \\ ar_{\varphi(m)} \equiv r_k \pmod{m} \end{gathered}$$

em que $r_i, r_j, \ldots, r_k$ são elementos de $(\mathbb{Z}/m\mathbb{Z})^*$. Fazendo o produto de ambos os lados dessa congruência, obtêm-se:

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod{m}.$$

Como todos os elementos $r_1,\ r_2, \dots, r_{\varphi(m)}$ são coprimos com m, então o produto $r_1 r_2 \dots r_{\varphi(m)}$ também é coprimo com m. Assim, pode-se cancelar $r_1,\ r_2, \dots, r_{\varphi(m)}$ de ambos os lados da última congruência, obtendo $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Teorema 3.10 (Pequeno Teorema de Fermat)**.** Seja p um número primo. Se a é um inteiro tal que $\text{mdc}\,(p, a) = 1$, então

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração. Esse teorema é consequência direta do teorema 3.9, basta supor que $m = p$. Por outro lado, $\varphi(p) = p - 1$. Logo, o teorema de Euler fornece:

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Do Pequeno Teorema de Fermat há vários resultados importantes, como o corolário e o teorema que serão apresentados a seguir, cujas demonstrações podem ser encontradas em Shokranian (2012, 44 e 45).

Corolário 3.2. Sejam p e q dois números primos distintos. Seja $m = pq$. Supondo que exista um inteiro r tal que

$$r \equiv 1 \pmod{p-1} \text{ e } r \equiv 1 \pmod{q-1}.$$

Então, para todo inteiro a obtem-se:

$$a^r \equiv a \pmod{m}.$$

Teorema 3.11. Sejam p e q dois números primos distintos e $a \in \mathbb{Z}$ tal que

$$a \not\equiv 0 \pmod{p},\ a \not\equiv 0 \pmod{q}.$$

Então,

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Diante da teoria exposta, compreende-se melhor o teorema relacionado com o Sistema RSA, o qual é citado com base em Shokranian (2012).

Teorema 3.12. Sejam:

1) p e q primos distintos;

2) $e \in \mathbb{N}$ tal que $mdc\big(e,(p-1)(q-1)\big)=1$;

3) $T \in \mathbb{Z}$ tal que $T \not\equiv 0 \pmod{p}$ e $T \not\equiv 0 \pmod{q}$;

4) $C \in \mathbb{Z}$ definido por $C \equiv T^e \pmod{pq}$;

5) $d \in \mathbb{Z}$ definido pelas duas condições:

$$ed \equiv 1 \pmod{(p-1)(q-1)},\ 1 \leq d < (p-1)(q-1).$$

Então,

$$T \equiv C^d \pmod{pq}.$$

Demonstração. Considerando a condição (4), obtem-se:

$$C^d \equiv (T^e)^d \pmod{pq}.$$

Então,

$$C^d \equiv T^{ed} \pmod{pq}.$$

Mas, $ed \equiv 1 \pmod{(p-1)(q-1)}$. Portanto, tomando $l \in \mathbb{N}$,

$$ed = l(p-1)(q-1)+1,$$

Assim,

$$C^d \equiv T^{ed} \equiv T^{l(p-1)(q-1)+1} \pmod{pq}.$$

O teorema 3.11 diz que:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Portanto,

$$C^d \equiv T^{l(p-1)(q-1)+1} \equiv T^{(p-1)l} \times T \equiv 1^l \times T \equiv T \pmod{pq}.$$

Ou seja,

$$T \equiv C^d \pmod{pq}.$$

□

3.4 A cifra de César no contexto das congruências

A cifra de César já foi abordada no capítulo 1 e neste tópico pretende-se descrevê-la no contexto das congruências. Inicialmente, considere a tabela 3.1 :

Tabela 3.2: Alfabeto Texto e Alfabeto Cifra

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	F	G	H	I	J	K	L	M	N	O	P	Q	R

O	P	Q	R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A	B	C	D

Fonte: Elaboração da autora.

Na primeira e terceira linha, está escrito o alfabeto normal que corresponde ao texto, desconsiderando letras com acento. Enquanto na terceira e quarta linha estão as mesmas letras, mas com uma troca de posição por 4 letras, trata-se da cifra. Para enviar uma mensagem criptografada, o remetente usa o alfabeto cifra que deve ser decodificado pelo destinatário utilizando essa mesma tabela. Tome como exemplo a mensagem cifrada:

I W P A I W P E Y W

Que resulta em MATEMÁTICA ao ser decifrada. Trocando as letras por decimais do 0 ao 25, obtem-se a tabela 3.3. Assim, essa mesma mensagem poderia ser enviada na forma digital: 16042308160423120604. No caso de frases, podem ser agrupadas em blocos de letras, como no exemplo a seguir, cujas letras foram arrajandas em blocos com no máximo quatro números e corresponde ao texto: VIDA DE ESTUDANTE.

25120704 07080822 23240704 172308

Tabela 3.3: Alfabeto Texto e Cifra em Números

A	B	C	D	E	F	G	H	I	J	K	L	M	N
04	05	06	07	08	09	10	11	12	13	14	15	16	17

O	P	Q	R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	00	01	02	03

Fonte: Elaboração da autora.

Dessa forma, na Cifra de César, a posição das letras do texto e as cifras obedecem a congruência:

$$C \equiv T + k \pmod{26},$$

denominada por Shokranian (2012) de cifra JC generalizada, sendo C o texto cifrado, T é o texto normal, k é a chave, tal que $0 \leq k \leq 25$, e 26 é a quantidade de letras do alfabeto. Na cifra considerada anteriormente, $k = 4$. Shokranian (2012) chama de cifra afim a expressão:

$$C \equiv aT + b \pmod{26}.$$

que pode ser escrita como:

$$aT \equiv C - b \pmod{26}.$$

Nessa congruência, a, b são chamados chaves da cifra, tais que $0 \leq a$, $b \leq 25$ e $mdc\ (a, 26) = 1$. Assim, um texto escrito nessa cifra pode ser decifrado calculando o valor de T. Como $mdc\ (a,\ 26) = 1$, pela proposição 3.2, existe a^{-1} módulo 26. Multiplicando ambos os lados da última congruência por a^{-1} obtem-se:

$$T \equiv a^{-1}(C - b) \pmod{26}.$$

Com essa congruência determina-se o conteúdo de uma mensagem criptografada. Se $a = 1$ a cifra afim corresponde a cifra de César, havendo 26 cifras JC generalizadas, porque há somente 26 possibilidades para a escolha de k. De acordo com Shokranian (2012), existem 312 cifras afins, pois $mdc\ (a,\ b) = 1$, há $\varphi(26) = 12$ possibilidades para escolher a e 26 para b. Logo, há $12 \times 26 = 312$ formas para escolher a e b.

3.5 Algoritmo do sistema RSA

Conforme visto no capítulo 1, com o advento dos computadores surge a necessidade de uniformização nos procedimentos de privacidade e segurança na troca de informações. Assim, todas as informações foram transformadas em códigos binários, surgindo a partir de 1960, o Código Padrão para o Intercâmbio de Informações (ASCII). Veja parte desses códigos na figura 3.1, mas este não é um método de cifragem e sim uma pré-codificação. De acordo Andrade e Silva (2012),

> A tabela original trabalhava com 7 bits, representando 128 caracteres, inicialmente para língua inglesa que não possui caracteres acentuados, e ela foi estendida a 8 bits para contemplar outros idiomas. Atualmente utilizam-se ASCII ESTENDIDA, com o nome ASCII, com 256 caracteres correspondendo ao alfabeto latino, com letras maiúsculas, minúsculas, letras acentuadas, pontuação e outros símbolos (ANDRADE; SILVA, 2012, p. 442).

Para uniformizar o uso dos sistemas criptográficos, em 1973, o National Bureau of Standards escolheu o Data Encryption Standard (DES) como padrão, o qual era complexo e funcionava com chaves simétricas, isto é, as partes envolvidas no processo combinavam

Figura 3.1: Parte da Tabela ASCII com 256 Caracteres

ASCII printable characters

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
32	20h	espacio	64	40h	@	96	60h	`
33	21h	!	65	41h	A	97	61h	a
34	22h	"	66	42h	B	98	62h	b
35	23h	#	67	43h	C	99	63h	c
36	24h	$	68	44h	D	100	64h	d
37	25h	%	69	45h	E	101	65h	e
38	26h	&	70	46h	F	102	66h	f
39	27h	'	71	47h	G	103	67h	g
40	28h	(	72	48h	H	104	68h	h
41	29h	)	73	49h	I	105	69h	i
42	2Ah	*	74	4Ah	J	106	6Ah	j
43	2Bh	+	75	4Bh	K	107	6Bh	k
44	2Ch	,	76	4Ch	L	108	6Ch	l
45	2Dh	-	77	4Dh	M	109	6Dh	m
46	2Eh	.	78	4Eh	N	110	6Eh	n
47	2Fh	/	79	4Fh	O	111	6Fh	o
48	30h	0	80	50h	P	112	70h	p
49	31h	1	81	51h	Q	113	71h	q
50	32h	2	82	52h	R	114	72h	r
51	33h	3	83	53h	S	115	73h	s
52	34h	4	84	54h	T	116	74h	t
53	35h	5	85	55h	U	117	75h	u
54	36h	6	86	56h	V	118	76h	v
55	37h	7	87	57h	W	119	77h	w
56	38h	8	88	58h	X	120	78h	x
57	39h	9	89	59h	Y	121	79h	y
58	3Ah	:	90	5Ah	Z	122	7Ah	z
59	3Bh	;	91	5Bh	[	123	7Bh	{
60	3Ch	<	92	5Ch	\	124	7Ch	|
61	3Dh	=	93	5Dh	]	125	7Dh	}
62	3Eh	>	94	5Eh	^	126	7Eh	~
63	3Fh	?	95	5Fh	_			

theASCIIcode.com.ar

Fonte:<https://www.ufrgs.br/wiki-r/index.php?title=Raw>.

parâmetros para a função cifragem que era a mesma para a decifragem. Diante disso, surgiu a necessidade de resolver a questão da troca de chaves entre os correspondentes, surgindo o Sistema RSA, assimétrico, já abordado de forma histórica no capítulo 1 e baseado matematicamente na Teoria dos números.

Andrade e Silva (2012) explica que:

> A ideia do algoritmo RSA concentra-se no fato de que, embora seja fácil encontrar dois números primos de grandes dimensões (mais do que 100 dígitos), o tempo estimado para fatorar números, por exemplo, de 308 dígitos, com os algoritmos clássicos é de aproximadamente 100 mil anos (OLIVEIRA et al, 2003). De fato, ele mostra-se computacionalmente inquebrável com números de tais dimensões, e a sua força é geralmente quantificada com o número de bits utilizados para descrever tais números. Para um número de 100 dígitos são necessários cerca de 350 bits, e as implementações atuais superam os 512 e mesmo os 1024 bits (ANDRADE; SILVA, 2012, p. 444 e 445).

O funcionamento desse algoritmo foi descrito pelo Teorema 3.12, mas pode ser explicado de forma mais didática da seguinte forma:

1) Seleciona dois números primos extensos: p e q, no mínimo, da ordem de 10^{100};

2) Calcula-se $n = p \times q$;

3) Escolhe-se um número inteiro e de forma que $1 < e < \varphi(n)$, sendo e e $\varphi(n)$ coprimos;

4) Computa-se d obedecendo a relação: $e \times d \equiv 1 \pmod{(p-1)(q-1)}$;

O par (n, e) corresponde a chave pública que pode ser compartilhada com qualquer pessoa, enquanto p, q e d constituem a chave privada e devem ser mantidos em sigilo. Se n for um número muito pequeno será fácil deduzir os outros valores por meio da fatoração, mas do contrário, se for extenso, até o momento, é uma tarefa quase impossível, pois como já foi citado, os algoritmos de fatoração são lentos.

5) Para cifrar e decifrar uma mensagem são utilizadas as seguintes congruências: $C \equiv T^e \pmod{n}$ e $T \equiv C^d \pmod{n}$), respectivamente. Dessa forma, C equivale ao texto cifrado e T ao texto original. Antes de cifrar a mensagem é feita a pré-codificação através de algum código como o ASCII.

Para entender melhor esse processo, tome como exemplo, uma mulher chamada Ana que deseja fazer uma compra online em determinado site. Mesmo que não conheça a criptografia, a comunicação entre ela e o site é protegida por meio de algum sistema. Supondo que seja o RSA, os procedimentos serão os descritos a seguir.

O destinatário, site de compras, escolhe dois primos grandes. No entanto, para facilitar os cálculos, serão utilizados dois primos pequenos, $p = 17$ e $q = 23$. Calcula-se $n = 17 \times 23 = 391$ e $\varphi(n) = (p-1)(q-1) = 352$. Daí, escolhe e que satisfaça $1 < e < \varphi(n)$, sendo e e $\varphi(n)$ coprimos. Para facilitar a codificação será escolhido o $e = 3$. Na sequência, encontra-se o número d que satisfaça: $e \times d \equiv 1 \pmod{(p-1)(q-1)}$, neste exemplo, $3 \times d \equiv 1 \pmod{352}$. Logo, $d = 235$, pois $3 \times 235 \equiv 1 \pmod{352}$.

O site de compras disponibilizará para Ana os números $n = 391$ e $e = 3$ para que seja feita a criptografia dos seus dados, como o nome **SILVA** que se encontra no cartão de Crédito. Inicialmente, é feita a pré-codificação por meio da tabela de códigos ASCII, figura 3.1, obtendo:

$$083\ 073\ 076\ 086\ 065$$

Cada um desses blocos será denotado por T e utiliza-se a fórmula: $C \equiv T^e \pmod{n}$ para que seja feita a codificação de cada um deles. Veja:

$$C \equiv 083^3 \pmod{391} \Longrightarrow C \equiv 145 \pmod{391}.$$
$$C \equiv 073^3 \pmod{391} \Longrightarrow C \equiv 363 \pmod{391}.$$
$$C \equiv 076^3 \pmod{391} \Longrightarrow C \equiv 274 \pmod{391}.$$
$$C \equiv 086^3 \pmod{391} \Longrightarrow C \equiv 290 \pmod{391}$$
$$C \equiv 065^3 \pmod{391} \Longrightarrow C \equiv 143 \pmod{391}.$$

Portanto, o site receberá a mensagem:

$$145\ 363\ 274\ 290\ 145.$$

Para decodificá-la deverá utilizar a fórmula: $T \equiv C^d \pmod{n}$, obtendo:

$$T \equiv 145^{235} \pmod{391} \Longrightarrow T \equiv 83 \pmod{391}$$

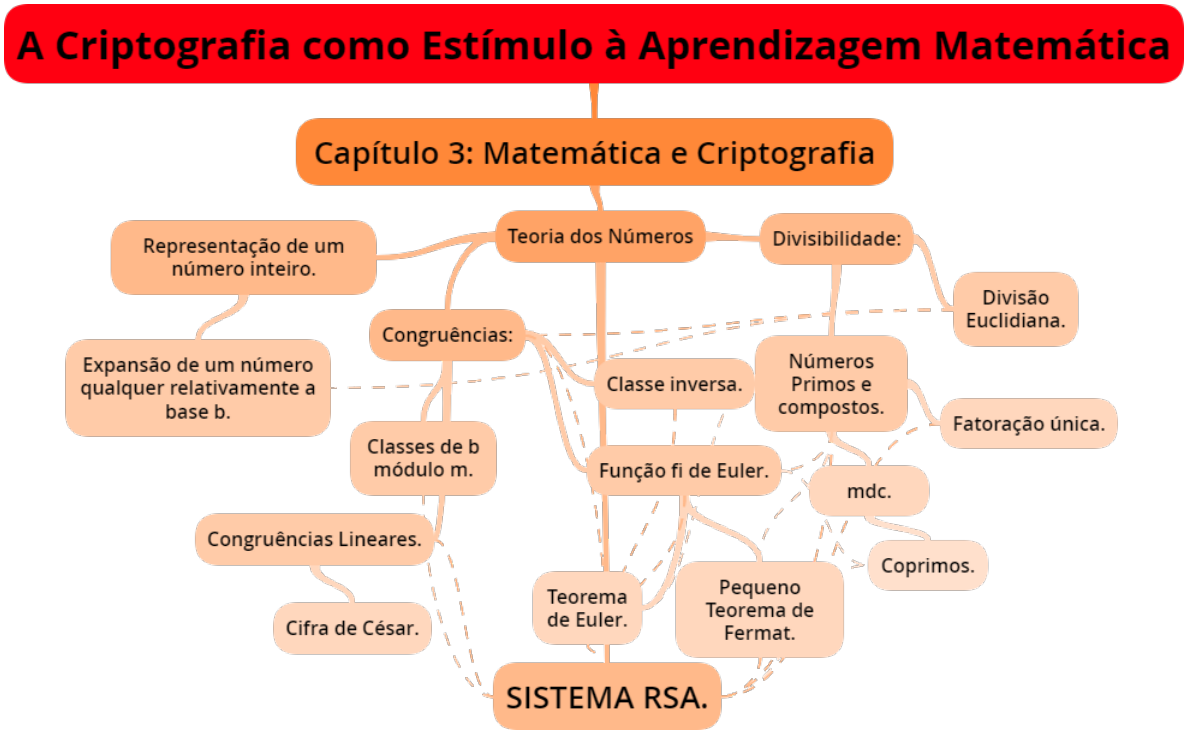
Fazendo esse processo em todos os blocos, obtem-se a mensagem pré-codificada que, ao ser comparada com a tabela ASCII, encontra-se a mensagem original.

Com esse exemplo, percebe-se que são muitas as operações envolvidas no processo e a segurança do RSA, de acordo com Hefez (2005), reside na dificuldade de descobrir os números p, q e d conhecendo apenas os dados públicos: n e e. Realmente, dado $x \in \mathbb{N}$, não é uma tarefa difícil calcular o resto da divisão de x^e por n, mas não é fácil fazer o contrário, ou seja, dado $y \in \mathbb{N}$ não é fácil encontrar $x \in \mathbb{N}$, tal que y é o resto da divisão de x^e por n, pois os valores de x na equação $x^e \equiv y \pmod{m}$ pode variar. Logo, é necessário construir a tabela dos valores da função: $\mathbb{N} \to \mathbb{Z}_m$, $x \to [x^e]$. No entanto, se p e q forem bem escolhidos, isso é computacionalmente inviável.

Conforme já foi citado no capítulo 1, existem outras cifras históricas já superadas, mas também há Cifras modernas que ainda são inquebráveis. Todavia, decidiu-se por uma maior ênfase na Cifra de César e no RSA, devido a popularidade e o desejo da pesquisadora em entender melhor o algoritmo do último método, afim de desenvolver atividades que possam ser aplicadas na Educação Básica.

Para concluir este capítulo, segue o mapa mental com os principais conceitos que foram apresentados.

Figura 3.2: Mapa Mental - Capítulo 3



Fonte: Elaboração da autora.

4 A Metodologia e Procedimentos da Pesquisa

Neste capítulo apresentaremos a metologia de pesquisa e a de ensino, bem como propostas de atividades envolvendo criptografia e matemática, compondo uma sequência de cinco planos de aula que explicitam o processo de intervenção realizado.

4.1 Metodologia da pesquisa

A pesquisa aqui apresentada teve como objetivo analisar o potencial da criptografia para motivar a aprendizagem do conceito de função nos 9º ano A e B do Colégio Municipal X. Para isso, foram utilizados como instrumentos para coleta de dados: questionários contendo questões abertas e fechadas, as observações da pesquisadora e um conjunto de atividades envolvendo criptografia e matemática. Assim, a pesquisa pode ser caracterizada como qualitativa, pois "preocupa-se em analisar e interpretar aspectos mais profundos, descrevendo a complexidade do comportamento humano, fornece análise mais detalhada sobre investigações, hábitos, atitudes, tendências de comportamento, etc." (MARCONI; LAKATOS, 2007, p. 269).

Sobre o papel do pesquisador, Ludke e Andre (2015) explica que ele deve estabelecer uma relação de confiança com os sujeitos da pesquisa, agindo com responsabilidade e imparcialidade, buscando envolvimento de todos, sem priorizar grupos ou participantes. Além de definir e apontar as estratégias mais prováveis para alcançar os objetivos propostos, ser capaz de compreender e analisar os dados coletados para apresentá-los de forma sistêmica.

4.2 Lócus e sujeitos da pesquisa

A pesquisa foi desenvolvida durante a pandemia da COVID-19 (Coronavirus Disease 2019). De acordo com Schuchmann et al. (2020), é uma infecção respiratória provocada pelo Coronavírus da Síndrome Respiratória Aguda Grave 2 (SARS-CoV-2). Os primeiros casos da doença foram identificados em Wuhan, na China. Devido a alta taxa de transmissão do vírus e seu alastramento por diversas partes do globo, foi declarada como pandemia, em 11 de março de 2020, pela Organização Mundial da Saúde (OMS). No Brasil, o primeiro caso foi confirmado em 26 de fevereiro de 2020 e, após casos de transmissão comunitária em São

Paulo e Rio de Janeiro, começaram a ser adotadas medidas para conter a contaminação. No dia 18 de março de 2020 o país decretou estado de calamidade pública, recomendando medidas de isolamento social para toda a população brasileira. Sobre essa realidade Alves (2020) cita:

> A pandemia afeta a saúde pública de forma agressiva, tirando a vida não apenas dos idosos, considerados inicialmente como o principal grupo de risco, mas crianças, jovens e adultos, também têm sido afetados pela doença. As medidas de isolamento e distanciamento social adotadas por todos países, por meio do confinamento com regras nem sempre rígidas, para manter a população em casa, tencionam a economia dos países, refletindo na paralisação de distintos serviços e atividades, dentre eles o processo de ensino-aprendizagem (ALVES, 2020, p. 350).

As aulas na Bahia foram suspensas a partir do dia 17 de março de 2020 e, de acordo com a autora supracitada, desde o dia 18 de março o Ministério da Educação começou a publicar Portarias suspendendo as aulas presenciais e indicando, em caráter emergencial, a Educação remota. E no dia 28 de abril de 2020, o Conselho Nacional de Educação (CNE) orientou as atividades não presenciais em todos os níveis de ensino da Educação Infantil até o Ensino Superior, durante a pandemia da COVID-19.

Com essas orientações, o município em que a pesquisa foi realizada, também publicou decretos e portarias determinando a suspensão das aulas e as orientações para o ensino remoto a partir de junho de 2020. No entanto, assim como ocorreu em muitas escolas do Brasil, os educadores não foram preparados para esse tipo de ensino e tiveram que se reinventar, utilizando plataformas gratuitas e o celular como principal meio para chegar até o aluno, unindo esforços para dar continuidade ao processo de ensino e aprendizagem.

A escola pesquisada organizou um horário de aulas, através do *Google Meet*, para atender os alunos com acesso a *internet* e disponibilizou atividades impressas para aqueles que não tivessem recursos tecnológico (computador ou celular) e/ou *internet*. Os professores usavam os grupos de *Whatsapp* para interagir com os estudantes, postar material e atividades, receber trabalhos resolvidos e dar *feedback*. Alguns profissionais com mais habilidade, também começaram a utilizar o google sala de aula, com a mesma função do *Whatsapp*.

A pesquisa foi desenvolvida em um colégio municipal X , numa cidade do interior baiano, localizada na mesorregião do Centro-Sul. Ocupa uma área de $1431km^2$ e, de acordo com o IBGE, sua população em 2018 era de 21520 habitantes. A instituição oferece os anos finais (8^{o} e 9^{o}) do Ensino Fundamental no diurno e Educação de Jovens e Adultos no noturno. Recebe estudantes de diversos bairros e da zona rural. Em geral, os da sede estão matriculados do turno matutino e os da zona rural no turno vespertino, devido a necessidade de transporte escolar. Em relação ao desempenho, há alunos com interesse pelos estudos e facilidade para desenvolver as atividades discentes, outros que frequentam,

prestam atenção às explanações dos professores, mas compreendem pouco e resolvem as atividades com dificuldade, mas também há aqueles que são desatentos e não cumprem as tarefas.

Apesar do empenho da equipe gestora e dos docentes, os resultados apresentados pelo Índice de Desenvolvimento da Educação Básica (IDEB) não são satisfatórios, pois houve queda nos dois últimos anos e em 2019 não conseguiu atingir a meta projetada, conforme mostra a tabela 4.1.

Tabela 4.1: IDEB - Resultados e Metas

IDEB Observado			Metas Projetadas		
2015	2017	2019	2015	2017	2019
4.8	4.5	4.5	4.1	4.3	4.6

Fonte: Elaborado pela pesquisadora com base em <http://ideb.inep.gov.br/resultado/>.

Os sujeitos participantes da pesquisa são trinta e três alunos, que compõem duas turmas do 9º ano do turno matutino no referido colégio. A maioria é oriunda da área urbana de classe média e baixa. Todos eles possuíam aparelhos celulares e/ou computadores e apenas dois deles não tinham acesso a internet em suas residências, mas se dirigiam à escola para assistirem as aulas *online* durante o período da pandemia da COVID-19.

Esses alunos estão participando e fazendo atividades de forma remota desde o início da suspensão das aulas, em março de 2020. A grande parte demonstra pouca motivação nos estudos remotos, quase não participam dos encontros síncronos e fazem as tarefas propostas, porque são cobrados constantemente e no caso de matemática, todas as atividades são pontuadas. Uma pequena parcela participa ativamente, respondendo a questionamentos e tirando dúvidas.

Durante esse período pandêmico, a escola mantém contato com as famílias através de grupos no *Whatsapp* e, apesar da dificuldade em firmar parcerias, percebe-se que nas duas turmas pesquisadas, há um certo estímulo por parte da maioria dos responsáveis por estes estudantes, pois acompanham o trabalho desenvolvido na instituição e o desempenho dos alunos.

Diante do contexto apresentado, a intervenção foi realizada por meio de uma sequência de cinco planos de aula com uma carga horária prevista de 20 horas, distribuída em atividades síncronas e assíncronas com o uso de tecnologias digitais.

4.3 Proposta prática para o ensino aprendizagem do conceito de função no contexto da criptografia

A proposta teve como foco o estudo do conceito de função motivado pela criptografia. A escolha por tal conteúdo se deu pelo fato de estar relacionado com os algoritmos de alguns

sistemas criptográficos e ser definido pela Base Nacional Comum Curricular (BNCC), como um dos objetos de conhecimento para o 9º ano do Ensino Fundamental. Esse conteúdo está relacionado com a habilidade EF09MA06, "Compreender as funções como relações de dependência unívoca entre duas variáveis e suas representações numérica, algébrica e gráfica e utilizar esse conceito para analisar situações que envolvam relações funcionais entre duas variáveis" (BRASIL, 2017, p. 316).

Além do conceito de função, na atividade inicial foi proposta a solução de problemas envolvendo equação do 1º grau para fazer uma conexão entre o conteúdo que estava sendo estudado e o que se pretendia desenvolver. Como as Cifras de César e o RSA estão embasadas na Aritmética modular, foi feita uma breve abordagem sobre congruências, levando em consideração o nível dos estudantes. Apesar desse conteúdo não fazer parte do currículo da educação básica, é possível relacioná-lo com situações cotidianas e com algumas habilidades definidas pela BNCC, para os anos finais do Ensino Fundamental, como a realização de cálculos envolvendo números naturais e inteiros e problemas sobre divisibilidade.

4.3.1 A Sala de Aula Invertida como metodologia de ensino

Para aproveitar melhor o tempo nos encontros síncronos para as discussões e atividades em grupos e, ainda, tornar o trabalho mais dinâmico, optamos pela metodologia a Sala de Aula Invertida (SAI), pois pode permitir que os alunos apropriem do conteúdo antecipadamente e participem mais ativamente dos encontros pelo *Google Meet*. Neste sentido, Sant'ana (2021) cita:

> Vale destacar a grande distinção da sala de aula do ensino tradicional, no qual o professor transmite as informações ao aluno durante a aula, e em casa, realizar o estudo referente ao material abordado e realizar as atividades (tarefas) de avaliação solitariamente, para assimilação do conteúdo. Já na SAI o estudante recebe orientação on-line para o estudo prévio, ficando a abordagem na sala de aula o lugar de aprendizagem ativa, onde há perguntas, discussões, trabalhos em equipe e atividades práticas (SANT'ANA, 2021, p. 228).

De acordo com esta autora, a SAI é uma ferramenta que tem suas origens no Ensino Híbrido, o qual significa misturado, mesclado, combinado, sendo desenvolvido a partir de experiências *e-learning*. Esta forma de ensinar e aprender ainda é muito discutida, principalmente no cenário das atividades remotas, tem defensores no Brasil e utiliza as tecnologias com foco num processo educacional mais personalizado. No entanto, além de inverter a sala de aula, é necessário que o docente incorpore quatro pilares que podem ser resumidos pela sigla "F-L-I-P" que significa: F-*flexible environments* (ambiente flexível); L-*Learning culture* (cultura de aprendizagem); I-*intentional teaching actions* (conteúdo dirigido); P-*Professional Educator* (educador profissional).

Dessa forma, a metodologia da Sala de Aula Invertida orienta que o ambiente precisa ser flexível, tendo em vista diversos modos de ensinar e aprender, a compreensão e a acomodação dos diferentes tempos de aprendizagem dos estudantes. Assim, o aprender precisa estar centrado no educando e na sua relação com o outro. O professor assume o papel de mediador, responsável pelo planejamento de ações que tenham intencionalidade e sejam contextualizadas para dar significado ao que está sendo aprendido. Também precisa avaliar e prover *feedback* regular aos educandos, refletindo constantemente sobre a sua prática (SANT'ANA, 2021).

Nesta perspectiva, Sant'ana (2021) lista, como exemplo, diversas atividades que podem ser desenvolvidas na SAI pré-classe *(pré-class)* e sala de aula *(in class)*. Seguindo esses encaminhamentos, neste trabalho, as atividades pré-classe foram elaboradas por meio de palestras com vídeos curtos, leituras de resumos e história em quadrinho, questionários e jogos *online*, vídeos explicativos do *Youtube* e um filme. Todo esse material foi disponibilizado em uma turma, do google sala de aula, criada para que os participantes pudessem acessar os materiais de estudo, atividades e interagir com os colegas e a pesquisadora, que utilizou esse mesmo espaço para dar *feedback* nas produções dos alunos.

Nos encontros *online*, realizados por meio do *Google Meet*, foram feitas discussões do que os alunos deviam estudar pré-classe, esclarecimento de dúvidas, exercícios individuais e colaborativos de resolução de problemas e uma gincana criptográfica, realizada em grupos com provas individuais e coletivas, tendo por objetivo avaliar, de forma dinâmica, o conteúdo abordado. Também, foram aplicados questionários, no início, para verificar os conhecimentos prévios dos estudantes sobre criptografia e sua relação com a matemática, e no final da intervenção, para que eles pudessem avaliar as atividades desenvolvidas.

A intervenção, portanto, foi realizada de forma remota, ou seja, a prática pedagógica foi mediada por plataformas digitais: *Google Meet* e Google Sala de Aula, propondo atividades que pudessem desafiar a participação, interação e produção dos sujeitos. Sobre a educação remota, Alves (2020) denuncia que predomina a adaptação de metodologias usadas no ensino presencial, como a exposição do conteúdo pelo professor e correção de atividades nos horários normais de aula. Ao se questionar sobre como engajar os estudantes, responde:

> Uma certeza nós temos, não é passando e corrigindo tarefas, usando uma plataforma como o Google Meet, por exemplo, que vamos motivar os nossos estudantes neste momento de confusão e incerteza. As atividades devem desafiar os alunos para que possam criar, se autorizar, participar e interagir com seus professores e pares, pensando e discutindo o momento que estão vivendo, escutando-os (ALVES, 2020, p. 360).

Portanto, os recursos tecnológicos precisam de uma abordadem além da instrumental, isto é, "ir além de recursos didáticos que fazem transposição entre o que era feito sem a mediação do digital e da web" (ALVES, 2016, p. 576). Com esse entendimento, pretende-se utilizar os recursos tecnológicos em conformidade com a competência geral de número

cinco definida pela BNCC, segundo a qual, ao longo da Educação Básica, o estudante seja capaz de:

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva (BRASIL, 2017, p. 9).

Somando as plataformas citadas, foram utilizados:

- Grupos de *Whatsapp* para interação entre os envolvidos e envio de informações referente a pesquisa.
- O *Google Forms* para elaboração de questionários online.
- As plataformas do *Wordwall* e o *Kahoot*, para criação de jogos e competições que tiveram o objetivo de motivar a aprendizagem e promover a avaliação formativa.
- O *Youtube* para o compartilhamento de vídeos e interação entre os participantes.
- O *Powerpoint* para exibição de slides e gravações de tela.
- O *FlashBack Express Recorde* para gravações de tela.
- O *YouCut* para edição de vídeos.
- Calculadoras online que auxiliaram nos cálculos do processo de encriptação pelo Sistema RSA.
- O *Qr Code* Generator para elaboração da primeira atividade.
- Leitores de *Qr Codes*, aplicativos e/ou câmera do celular que os estudantes utilizaram para ter acesso ao problema que deveriam resolver para descobrirem a mensagem secreta.

Todos estes recursos foram selecionados, porque são gratuitos, possuem interfaces intuitivas e úteis e, a maioria, já são utilizados pelos participantes no cotidiano, dentro e fora do espaço escolar. Em relação aos jogos digitais e a gincana criptográfica, realizados em momentos assíncronos e síncronos, como citado, tiveram o objetivo de tornar o processo mais dinâmico, motivar a aprendizagem e promover a avaliação, pois no caso dos jogos digitais, são gerados relatórios sobre o desempenho de cada jogador.

4.3.2 Apresentação da proposta

Devido a pandemia da COVID-19, como já foi explicado, as atividades escolares ainda estavam acontecendo de forma remota quando se iniciou a intervenção. Na escola pesquisada, as aulas estavam organizadas em três horas de encontros síncronos, por meio do *Google Meet* e atividades assíncronos disponibilizadas no Google Sala de Aula e/ou nos grupos de *Whatsapp* das turmas.

Diante disso, a equipe gestora ficou receosa ao receber a solicitação para aplicação da pesquisa, pois enquanto professora de matemática da turma, a pesquisadora ainda precisaria trabalhar muitas habilidades consideradas essenciais para a etapa e revisar os descritores avaliados na prova externa do Sistema de Avaliação da Educação Básica (SAEB) que seria aplicada no ano em curso. No entanto, foram apresentados os planos de aula para os cinco encontros, ressaltando que seria abordado o conceito de função, conteúdo considerado essencial para o 9º ano do Ensino Fundamental, conforme a BNCC, além de uma abordagem interdisciplinar, na qual também seriam realizadas leituras, análises de filmes e reflexões sobre contextos históricos.

Com os argumentos apresentados, foram pensadas alternativas para a aplicação do projeto, de forma que não comprometesse somente as aulas de matemática. Então, ficou combinado que seriam concedidas todas as aulas, durante uma semana, para realização da pesquisa. Foi cogitado desenvolver o projeto no turno oposto, mas os estudantes poderiam ficar sobrecarregados, comprometendo os resultados tanto pesquisa quanto das aulas normais.

Com essa decisão, a pesquisadora, direção e coordenação, reuniram com os alunos e responsáveis, de forma presencial, para apresentar a pesquisa: objetivos, metodologia e duração. Para cumprir com os aspectos éticos, definidos pelas diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos, foi solicitado que os participantes e seus responsáveis assinassem um Termo de Consentimento e Livre Esclarecido e um Termo de Autorização de Imagens. Na oportunidade, foram entregues aos estudantes um kit de encriptação (dois copos descartáveis transparentes com uma fita contendo as vinte e seis letras do alfabeto e coladas na borda, conforme figura 4.1) que seria utilizado no segundo encontro.

Com as autorizações necessárias, a proposta foi colocada em prática na semana seguinte com um planejamento sistematizado em cinco planos de aula estruturados com base na metodologia da Sala de Aula Invertida e no modelo apresentado por Silveira Júnior (2020). Em cada um deles, há uma estimativa para a duração de cada atividade, articuladas entre espaços e tempos *online* síncronos e assíncronos e com a definição do papel do aluno e do professor.

Com excessão do pimeiro encontro, que foi uma conversa sobre a proposta para esclarecer possíveis dúvidas e do último, no qual o estudo foi apresentado em forma de

Figura 4.1: Kit de Encriptação

Fonte: Elaboração da autora.

vídeo, todos os outros foram planejados com uma conversa inicial para que os participantes apresentassem um resumo do que estudaram, as dúvidas e discutissem o conteúdo com a mediação da professora.

No primeiro encontro, foi solicitado que respondessem um questionário online para investigar os conhecimentos prévios dos alunos sobre criptografia e sua relação com a disciplina de matemática. No último, foi aplicado outro questionário *online* para avaliarem as atividades desenvolvidas. Também foram formados seis grupos, sendo três com seis alunos e três com cinco alunos, para realizarem as tarefas conjuntas, pelo *Google Meet* e grupos de *Whatsapp*, durante os cinco encontros. Nesse sentido, é importante que as "atividades durante a aula, busque o envolvimento do estudante, o trabalho em equipe, a valorização do aprendizado, a mediação dos estudantes" (SILVEIRA JÚNIOR, 2020, p. 20).

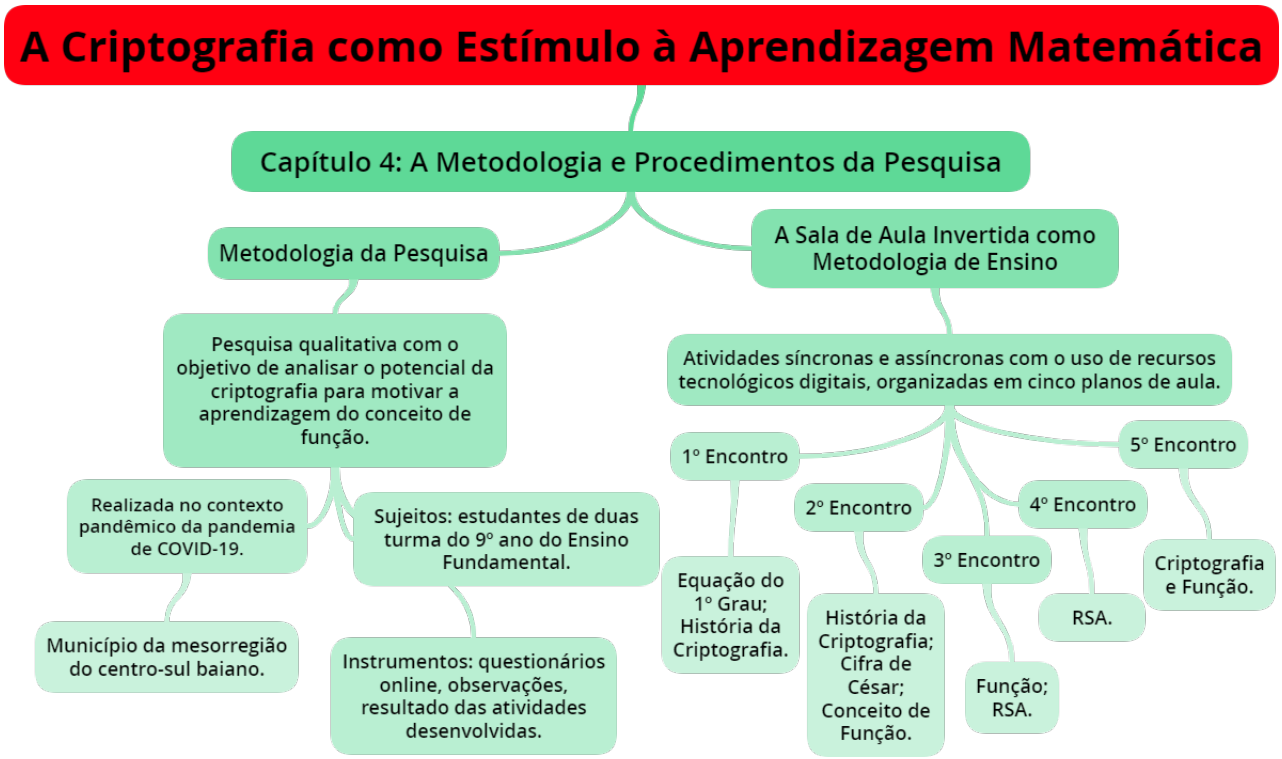
Após cada atividade em grupo, foi feita uma roda de conversa para que os alunos pudessem expor seus resultados e indicarem, oralmente, pontos positivos e negativos do que foi proposto. De acordo com (SILVEIRA JÚNIOR, 2020, p. 20), "ao elaborar o planejamento, considere que ele pode ser ajustado conforme o feedback que terá após a realização de cada aula". Nesse momento, também eram orientados os estudos que deveriam fazer em casa: leituras, assistir vídeos produzidos pela pesquisadora ou compartilhados no *Youtube* e filme, fazendo as devidas anotações e realização de jogos para verificar, de forma dinâmica e divertida, a compreensão sobre o conteúdo.

Em relação a avaliação, segundo Silveira Júnior (2020), no método tradicional, geralmente, o aluno é avaliado por meio de provas e trabalhos escritos e seminários em grupos. Porém, é atribuído um peso maior à avaliação escrita, fazendo com que o estudante concentre mais nesta atividade. Por outro lado, na Sala de Aula Invertida tudo é avaliado e cabe ao professor atribuir o peso de cada atividade, tendo em vista os objetivos de aprendizagem.

Os planos de aula seguem nos apêndices, juntamente com as atividades planejadas em cada um deles. Após a realização de todos os encontros, ficou evidente que esse planejamento

poderia ser melhorado, principalmente em relação a duração prevista para cada uma das atividades, pois houve necessidade de ampliar devido as dificuldades apresentadas por alguns grupos e pelo fato das orientações remotas demandarem mais tempo. No entanto, isso não foi feito neste trabalho, pois entendemos a flexibilidade deste instrumento e que as adaptações e mudanças serão necessárias para atender as particularidades de cada turma e/ou aluno. Por fim, para resumir o que foi exposto neste capítulo, segue o mapa mental da figura 4.2

Figura 4.2: Mapa Mental - Capítulo 4



Fonte: Elaboração da autora.

5 Análise e Discussão dos Resultados

Neste capítulo, apresentaremos o perfil dos estudantes por meio da análise das observações e de um questionário aplicado, de forma online, no primeiro encontro da intervenção. Na sequência, faremos um relato das atividades desenvolvidas, expondo trechos das produções dos participantes que serão identificados como A1, A2, ..., A33 para manter o sigilo quanto a identidade e respostas apresentadas. Por fim, expomos a análise de um questionário que os participantes responderam após a realização das atividades planejadas, avaliando as ações ao longo dos cinco encontro.

5.1 Perfil dos Estudantes

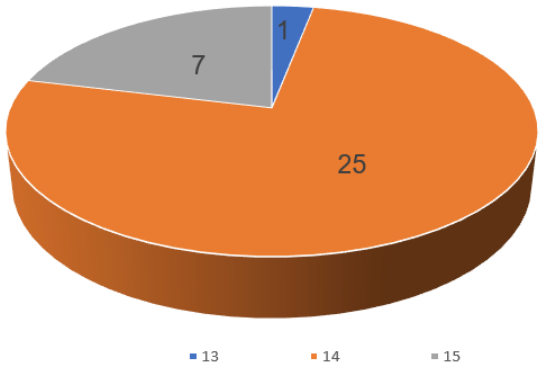
Como já citamos os sujeitos participantes dessa pesquisa foram trinta e três alunos das turmas do 9º A e B que frequentam a escola pesquisada, no turno matutino. Eles são heterogêneos em muitos pontos: são oriundos do meio urbano e rural e de diferentes situações econômicas, alguns trabalham no turno oposto ou cuidam dos irmãos para os pais trabalharem; possuem níveis de conhecimento distintos, não participam da mesma forma das discussões, enquanto alguns gostam de emitir opiniões e fazer questionamentos, outros demonstram timidez, falando somente o necessário e quando solicitado; apesar da família ser bastante presente, ainda há aqueles que carecem do acompanhamento dos responsáveis no seu processo educacional.

Após a conversa inicial sobre a proposta que seria desenvolvida, solicitamos que os participantes respondessem um questionário online elaborado no google forms e disponibilizado no Google Sala de Aula, composto por dez questões, sendo as três primeiras de identificação (nome, idade e turma). Os participantes da pesquisa são estudantes de duas turmas de um Colégio Municipal com idade entre 13 e 15 anos, conforme o gráfico 5.1.

A quarta pergunta refere-se ao gosto pela disciplina de matemática. Era aberta e solicitava uma justificativa. O objetivo era investigar a relação dos estudantes com a matemática. As respostas para esse questionamento foram tabuladas no gráfico da 5.2

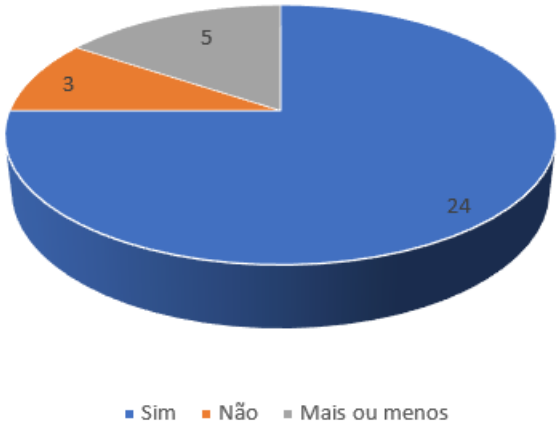
Conforme observamos no gráfico 5.2, 75% dos participantes que responderam a questão, dizem gostar de matemática. Ficamos surpresos com o resultado, pois apesar de não ter convivido presencialmente com as turmas, muitos reclamam da dificuldade em compreender os conteúdos que estão sendo trabalhados remotamente. No entanto, consideramos um dado positivo para avançar no processo de ensino e aprendizagem e ajudá-los a aumentar

Gráfico 5.1: Idade dos Participantes da Pesquisa



Fonte: Elaborado com dados da pesquisa.

Gráfico 5.2: Respostas dos alunos para a questão: "Você gosta de estudar matemática?"



Fonte: Elaborado com dados da pesquisa.

o nível de proficiência na disciplina. Esse gosto foi justificado de várias formas:

A32: "A Matemática ajuda em todas as disciplinas, até mesmo no Português! Ajuda na concentração."

A6: "Eu gosto de estudar matemática sim! Mas depende do assunto porque tem alguns que eu não consigo fazer as atividades direito. E respondendo a pergunta, eu gosto de estudar matemática porque é necessário hoje em dia a matemática está ligada à TUDO compras, valores, construções, medidas, história, geografia etc.. É por isso, porque é necessário."

A5: "Sim, pois ela me ajuda muito a desenvolver o raciocínio lógico e situação do cotidiano."

Diante do que estes alunos escreveram, percebemos que eles relacionam o gosto pela disciplina a funcionalidade e pragmatismo do conhecimento matemático presente nas mais diversas atividades sociais e do qual, as outras ciências também se apropriam como

ferramenta para modelar e explicar fenômenos. Somente cinco participantes justificaram de outra forma.

A24: "Minha disciplina favorita desde que eu era criança,"

A23: "Pra mim matemática e quase uma diversão, não estudo por obrigação, estudo pra testar os meus limites."

A13: "Pois acho divertido resolver problemas que estimulem o raciocínio logico e etc..."

Nesse caso, por um lado, esses estudantes parecem relacionar o gostar com a facilidade que possuem para compreenderem conteúdos e procedimentos da área. Por outro, consideram divertido o desafio de resolver problemas, chegando a demonstrar que se interessam em estudar matemática além dos muros da escola. Nas nossas observações, esses alunos, apresentaram um bom rendimento nas atividades desenvolvidas, evidenciando que essa afinidade colabora para o êxito do processo educativo.

As respostas "mais ou menos"e "não", foram justificadas, principalmente, pela dificuldade de aprendizagem e pela disciplina envolver muitas regras e cálculos. Apesar desta parcela dizer não gostar de estudar matemática, 100% dos alunos afirmam que considera importante o estudo desta disciplina e que percebem sua presença no cotidiano, citando vários exemplos:

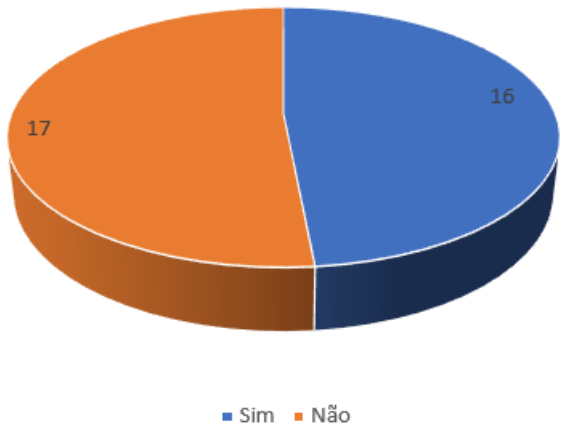
A3: "Ir às compras, preparar uma receita, contar tempo no relógio..."

A13: "Nas horas, número de celular de calçados, no calendário, na música, dinheiro entre varias outras coisas."

A6: "Como eu trabalho em um salão de cabeleireiro aqui a gente sempre toca no assunto de dinheiro, quando vem cliente pagar, ou fazer um cabelo ela sempre pergunta o valor, e se pode dividir etc... compras, valores, vendas, construções, medidas etc..."

A oitava questão tinha por objetivo verificar se os participantes apresentavam alguma familiaridade com a criptografia e as respostas foram organizadas no gráfico 5.3.

Gráfico 5.3: Respostas dos alunos para a questão: "Você já ouviu falar sobre criptografia?



Fonte: Elaborado com dados da pesquisa.

Na sequência, solicitamos que os estudantes descrevessem onde ou como já ouviram

falar sobre criptografia, caso a resposta para a questão anterior tivesse sido positiva. De acordo com o gráfico da figura 5.3, menos da metade afirmou já ter ouvido falar sobre criptografia. Mas se este questionamento tivesse sido feito antes da apresentação do projeto de pesquisa, esse número seria bem menor, porque ao justificarem a resposta positiva, alguns afirmaram que foi na aula de matemática e outros já teriam pesquisado sobre o tema para ver o que iriam estudar.

A25: "Eu ouvir falar sobre nas aulas de matemática."

A23: "A professora falou sobre‘."

A29: "Estava estudando antes para compreender melhor o que iria estudar."

Outras situações apresentadas foram no celular, *Whatsapp*, aplicativos, anúncio no *Youtube*, séries, *doramas* sul coreanos e na programação.

A17: " Eu ouvi falar em séries, *doramas* sul-coreanos, filmes e até no próprio *whatsapp* e entre outros apps, também vi em vídeos comentando sobre isso envolvendo coisas de *hackers* e tudo mais..."

A9: "Na programação e em *apps*."

Ao serem questionados sobre a utilidade da criptografia, cerca de 39% dos participantes tentaram responder, mas alguns mostraram insegurança no que estavam escrevendo, conforme se verifica nas respostas abaixo. No entanto, é perceptível que já conseguem associar a criptografia com a questão da segurança de dados.

A7: "Não muito bem, mas pelo que sei trata-se de uma escrita codificada."

A23: "Pelo o que eu vi e como se fosse senhas, com números primos e quase impossível decifrar sem computação gráfica e mais algumas coisas que não me lembro mais."

A12: "Serve para proteger algo."

A17: "Eu não sei exatamente se é isso mesmo mas creio que é coisa de quem mexe em computador, tipo a criptografia de um site ou app pra proteger que é tipo um código cheio de números e letras que serve na maioria das vezes pra proteger algo, tipo senhas, um exemplo é a criptografia do *WhatsApp* que protege sua privacidade. "

Conforme citamos, muitos participantes ouviram falar sobre ciptografia pela primeira vez na reunião para a apresentação da pesquisa, na qual foi necessário fazer uma pequena explanação sobre o tema, devido a curiosidade de alguns presentes. Vários deles lembraram que já tinham visto algo sobre criptografia no aplicativo *Whatsapp*, mas não sabiam qual a utilidade. Porém, esperávamos respostas positivas como estas, pois existem alunos com uma curiosidade mais aguçada em relação ao meio tecnológico, inclusive aluno com um pouco de conhecimento em programação.

Diante da análise das respostas a este questionário inicial, constatamos que a maioria dos participante desta pesquisa dizem gostar de matemática, e percebem a sua presença no cotidiano, todavia com base nos dados coletados e nas observações, muitos deles têm dificuldades de aprendizagem. Em relação a criptografia, menos da metade demonstra alguma familiaridade com o termo, um quantitativo maior do que esperado, mas que

nos deixou satisfeitos, visto que muitos deles se interessaram em investigar sobre o tema, quando a pesquisadora comentou sobre a proposta durante aulas e reunião que antecederam a realização da intervenção.

5.2 Relato do caminho trilhado e análise das produções dos estudantes

As pesquisas, no âmbito educacional, sofrem influências das ciências humanas e sociais, por esse motivo, o estudo dos fenômenos educacionais estão sujeitos a sistuações incontroláveis, uma vez que, "[...] as coisas na educação acontecem de maneira tão inextricável que fica difícil isolar as variáveis envolvidas e, mais ainda, apontar claramente quais são as responsáveis por determinado efeito" (LÜDKE e ANDRÉ, 2015, p.4). Diante disso, antes de relatar as atividades desenvolvidas, ressaltamos alguns aspectos que precisam ser considerados para compreensão do resultado final deste trabalho.

A intervenção foi realizada remotamente, por causa do contexto pandêmico, dificultando a identificação do estágio inicial e a definição da estratégia de intervenção, além de impedir observações mais precisas sobre o desempenho dos alunos. Esses estudantes apresentam dificuldades de aprendizagem que, em parte, são atribuídas ao processo de educação remota a que foram submetidos durante a pandemia da COVID-19. Sobre a implantação dessa proposta na Bahia, Alves (2020), tece várias críticas: a maioria dos estudantes são de classes sociais mais baixas, sem acesso a recursos tecnológicos digitais e espaços de estudo apropriados; dificuldades dos responsáveis na orientação dos estudos; falta de preparo do corpo docente para assumir suas atividades por intermédio de plataformas digitais, entre outros. Todavia, a educação remota foi implantada na escola pesquisada, impondo ao corpo docente, aos discentes e aos responsáveis outra forma de conduzir o processo educacional.

Na unidade escolar havia cinco turmas de nono ano. A professora pesquisadora lecionava matemática em duas delas, 9ºA e 9ºB, com 38 alunos, porém somente 33 deles participaram da pesquisa, visto que os demais estavam realizando atividades impressas, em virtude dos obstáculos já citados.

Citados os aspectos que julgamos mais relevantes, faremos alguns esclarecimentos. Aplicamos o questionário inicial no dia 13 de setembro de 2021, após uma conversa inicial para elucidar possíveis dúvidas que os participantes tivessem sobre a pesquisa. Nesse mesmo dia, iniciamos as atividades planejadas por meio da metodologia SAI, seguindo as orientações de Silveira Júnior (2020) e as reflexões de Sant'ana (2021). Foi necessário uma carga horária maior que a prevista, sendo utilizadas mais duas horas para o encerramento do que foi planejado. Sendo assim, a intervenção foi realizada por meio dos cinco encontros presumidos, mais duas horas, com atividades síncronas e assíncronas.

As atividades síncronas (conversas e exercícios colaborativos) foram realizadas por meio

do *Google Meet*. Seguindo a metodologia SAI, os participantes deveriam estudar o conteúdo que seria abordado no encontro seguinte, acessando o material que disponibilizamos no *Classroom* criado para a pesquisa. Para motivá-los elaboramos jogos na plataforma do *Wordwall*, figura 5.1, que deveriam ser acessados após o estudo. De posse dos relatórios dos resultados de tais jogos, identificamos os alunos que acessaram o material de estudo, as dificuldades apresentadas e o que conseguiram compreender. Tudo isso, orientava a conversa sobre o conteúdo, no encontro síncrono do dia seguinte.

Figura 5.1: Jogos Elaborados no *Wordwall*

Fonte: Dados da pesquisa.

Para as tarefas colaborativas de todos os encontros, foram formados seis grupos, com cinco ou seis alunos, utilizando a afinidade entre eles. Esse critério foi uma opção dos participantes e, a princípio, ficamos receosos, temendo que sobrassem alunos e que sentissem excluídos. No entanto, foram escrevendo no *chat* os grupos que estavam sendo compostos e as vagas disponíveis. Em menos de cinco minutos, todos os grupos foram instituídos.

5.2.1 Primeiro encontro

Iniciamos o primeiro encontro de forma síncrona através do *Google Meet*. Os estudantes receberam o *link* de acesso através do *google agenda* e do grupo de *Whatsapp*. De início, conversamos sobre a pesquisa, elucidando algumas dúvidas sobre as atividades que seriam desenvolvidas, o tempo necessário para realização, a metodologia que seria utilizada e a forma de avaliação (seriam atribuídas notas de 0 a 10 em cada atividade, tendo em vista o compromisso, a autonomia, o desempenho e a interação entre os estudantes e entre os estudantes e a professora).

Enviamos o *link* do *Classroom*, para que pudessem ter acesso as atividades e materiais de estudo, entregassem as resoluções e interagissem com a pesquisadora. A primeira atividade foi o questionário inicial, cujo objetivo e resultados foram apresentados na seção

5.1. Na sequência, foram formados os grupos, como citamos, esclarecemos que deveriam trabalhar de forma colaborativa e orientamos na escolha de um líder para coordenar as discussões e criar a reunião no *Google Meet*, enviando o *link* para os colegas do grupo e professora.

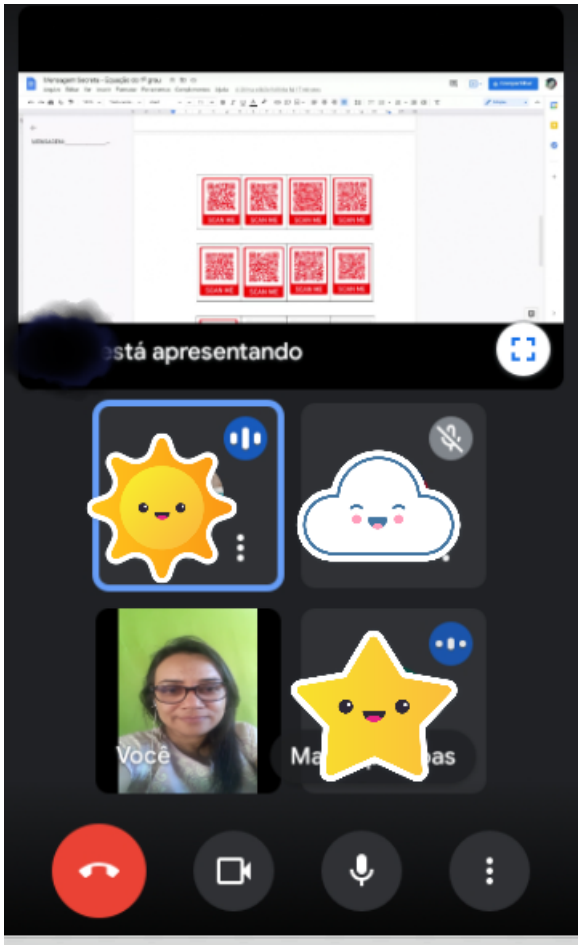
Dadas essas orientações, os grupos se reuniram para responder a atividade: "Mensagem Secreta com *QR Codes* (resolução de problemas envolvendo equação do 1º grau)" que teve por objetivo iniciar as discussões sobre criptografia, revisando o conteúdo que estava sendo estudado anteriormente. Foi elaborada com base nas ideias de Santos (2019), que desenvolveu sua pesquisa mediada pelo jogo: "Trilha Matemática Criptografada", descrita no capítulo 2. Entretanto, sua intervenção utilizou os *QR codes* com problemas envolvendo funções para montar o jogo, enquanto, neste trabalho, consistiu numa sequência de 17 *QR codes*, contendo dez situações problemas envolvendo equações, visto que sete deles eram iguais. Os estudantes deveriam fazer a leitura das imagens utilizando aplicativos do celular, solucionar os problemas e associar o número encontrado em cada um deles a uma letra, do alfabeto dado, para descobrir a mensagem secreta.

Acessamos o *link* de cada grupo, a exemplo da figura 5.2, para orientá-los, em caso de dúvidas, e incentivar a interação entre eles. Percebemos que estavam bastante envolvidos com a atividade e curiosos para descobrir a mensagem secreta. A maioria, utilizou a seguinte tática: um dos integrantes fez a leitura e enviou as informações contidas nos *QR codes* no *chat* do *Google Meet*, dividiram os problemas e no final analisaram as respostas encontradas, desvendando a mensagem secreta. Houve alguns equívocos na transcrição das situações para a linguagem matemática, demonstrando dificuldades na interpretação do enunciado. Todavia, somente um dos grupos demonstrou maiores dificuldades na condução da reunião e na interpretação das situações propostas, necessitando de acompanhamento constante. Por fim, todos necessitaram de mais tempo além do previsto para concluírem o exercício.

Na figura 5.3 apresentamos a resolução do grupo 5 e podemos perceber que cada componente ficou responsável por uma ou mais questões, revelando o envolvimento de todos e os recursos que utilizaram, alguns digitaram, outros entregaram a foto com os cálculos que foram organizados pelo líder do grupo, expondo a mensagem secreta: "CRIPTOGRAFIA É ARTE". Apesar dos *QR Codes* estarem na ordem das letras que formariam esta frase, dois grupos julgaram que seria apenas, "CRIPTOGRAFIA", talvez por causa da repetição das letras.

Como atividade pré-classe, eles deveriam fazer a leitura do prólogo do mangá: *The Manga Guide to Cryptography* de Mitani et al. (2007), apêndice A, que foi traduzido para português e assistir ao vídeo gravado pela professora/pesquisadora sobre a história e fundamentos da criptografia, cujo *link*: <https://www.youtube.com/watch?v=V2V9v089eng> foi disponibilizado no *Classroom*. Orientamos que fizessem as anotações que considerassem importantes para o encontro seguinte. Em seguida, deveriam acessar o jogo, Perseguição

Figura 5.2: Mensagem Secreta com *QR Codes* - Trabalho em Grupo

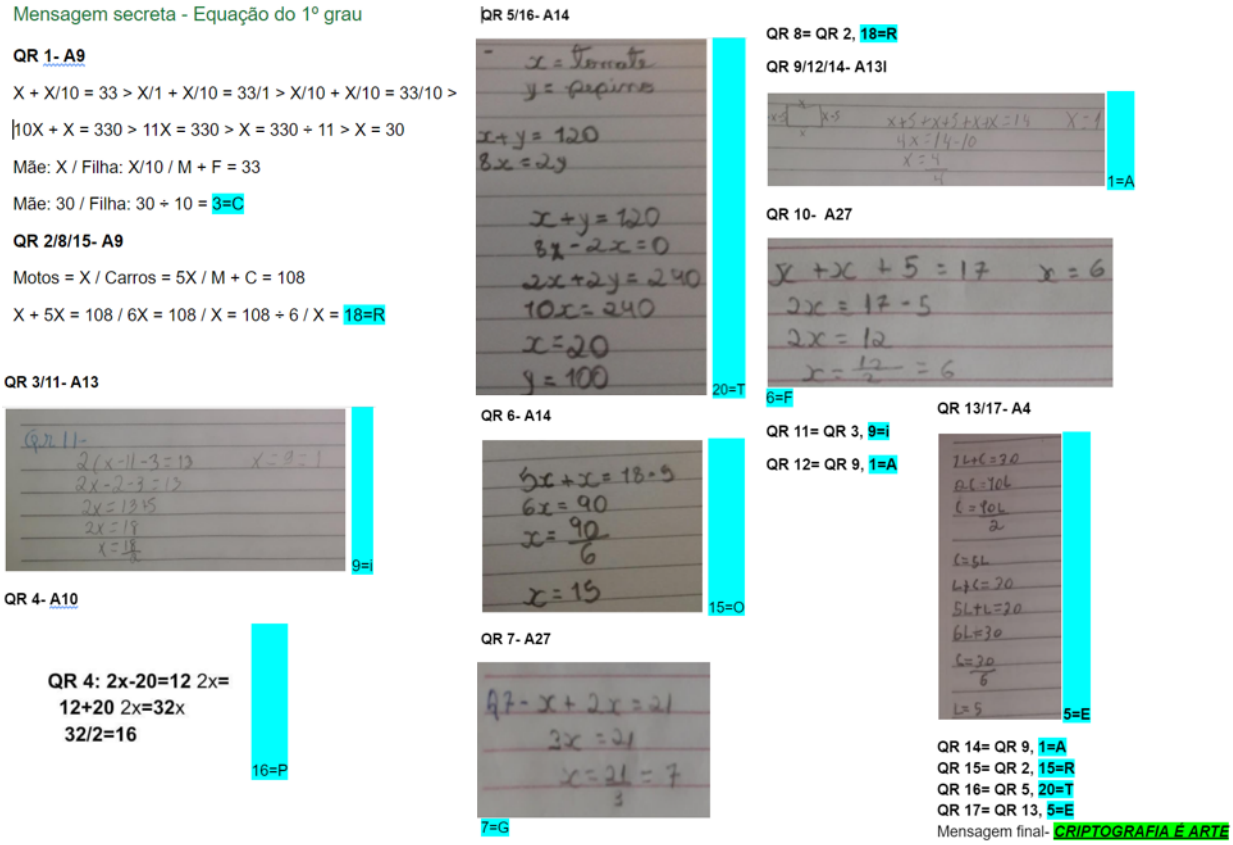


Fonte: Dados da pesquisa.

do labirinto, disponível no *link*: <https://wordwall.net/play/21137/642/319>, testando os conhecimentos abordados no mangá e no vídeo. Neste jogo, como mostrado na figura 5.4, os estudantes deveriam se dirigir para a resposta correta, tomando cuidado com os inimigos. Ao chocar com um inimigo, perdiam vidas e em cada jogada, só teriam direito a três vidas. Entretanto, com os *feedbacks* dos alunos sobre as dificuldades com o jogo, no que diz respeito a fuga dos inimigos para as respostas corretas, mudamos as configurações de três para dez vidas.

Analisando os relatórios do desempenho dos jogadores, verificamos o quantitativo de estudantes que acessaram o material de estudo, assim como a pontuação de cada um, questões que mais acertaram ou erraram, auxiliando no processo de avaliação e na retomada do conteúdo. Percebemos que os melhores desempenhos foram de participantes que convivem no universo dos jogos, uma vez que, mesmo com apenas três vidas, conseguiram pontuação total e quando questionamos como conseguiram, responderam que o jogo era moleza e que já estavam acostumados. Por outro lado, outros relataram que ficaram estressados, porque sabiam a resposta correta, porém perderam todas as vidas por não conseguir fugir dos inimigos.

Figura 5.3: Mensagem Secreta - Resolução do grupo 5



Fonte: Dados da pesquisa.

Neste primeiro plano, os estudantes também deveriam assistir ao filme "O Jogo da Imitação" e responderem um questionário sobre o mesmo, contudo, para não haver sobrecarga, decidimos que cada um escolheria o melhor momento para assistirem, contanto que fosse até o quarto encontro.

Podemos concluir que os resultados das atividades planejadas para esse encontro foram positivos, dado que os objetivos: resolver problemas envolvendo equação do 1º grau e conhecer a história da criptografia, compreendendo alguns conceitos básicos, foram alcançados. Na conversa, após a atividade que utilizou os Qr codes, os alunos afirmaram a questão da interação nos grupos como um dos pontos mais positivos, uma vez que nas reuniões com as duas turmas juntas, nem todos participam e relataram algumas dificuldades referentes a leitura dos *QR Codes* e na interpretação das situações problemas.

5.2.2 Segundo Encontro

Iniciamos o segundo encontro pelo *Google Meet*, com uma conversa sobre a história da ciptografia, a partir dos registros que fizeram sobre a leitura do mangá, do vídeo que assistiram e dos resultados do jogo: Perseguição no Labirinto. Ao serem questionados sobre os pontos que acharam mais interessantes, não houve muito consenso e acabaram citando

Figura 5.4: Perseguição do Labirinto - Jogando com a História da Criptografia

Fonte: Dados da pesquisa.

a esteganografia e todas as cifras citadas no vídeo. Dessa forma, debatemos brevemente sobre os fundamentos da criptografia, esteganografia, citale espartano, Cifras de César, Viginère e ADFGVX, Enigma, RSA, criptografia simétrica e assimétrica. Um dos alunos quis saber mais sobre o sistema RSA, então ressaltamos que seria conteúdo abordado no quarto encontro.

Planejamos a construção de um *kit* de criptografia, conforme o citado por Carvalho (2016), mas como as atividades foram desenvolvidas de forma remota, o *kit* da figura 4.1 foi entregue pronto a cada estudante na reunião para apresentação da pesquisa, conforme já comentamos.

Neste *kit* um dos alfabetos ficaria fixo, combinamos que seria o azul, enquanto o outro seria deslocado de acordo com um dado número x, que representava a chave da criptografia.

Como exemplo, consideremos x=3, então giramos o copo rosa, "pulando" três letras. Dessa maneira, o A ficaria alinhado com o D, o B com o E e assim por diante. Criptografando a palavra ESCOLA com x=3, obtemos: HVFROD.

Explicamos através de exemplos práticos, como o *kit* seria utilizado para cifrar e decifrar mensagens de acordo com o código de César. Logo após, os grupos se reuniram através do *Google Meet* para a realização da atividade que também fez uma breve abordagem sobre congruências. Isso foi explanado através da codificação da palavra PAZ, usando a cifra de César e um deslocamento igual a 3. De acordo com o alfabeto dado, somamos o número correspondente a cada letra com o 3:

P=15+3=18, que correpondia a letra S.

A=0+3=03, que correpondia a letra D.

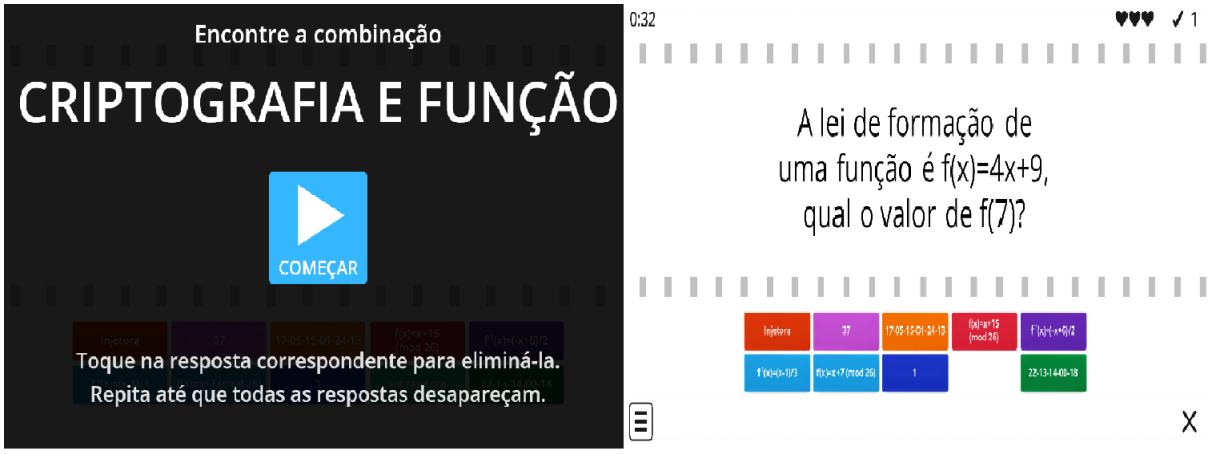
Z=25+3=28, aqui, questionamos a que letra correspondia o 28, sendo que no alfabeto dado (conforme tabela 2.7), as letras estavam numeradas de 0 a 25. Alguns deram a resposta por meio do *kit* de encriptação, então perguntamos o que fariam se não tivessem esse instrumento. Com as discussões, eles perceberam que deveriam contar conjuntos de 26 letras e registrar o resto quando o resultado da soma que estavam efetuando fosse superior a 25. Assim, o 28 seria dividido por 26 e considerariam o resto 2, cuja letra correspondente seria o C. Logo, 18-03-02 ou SDC correspondia a codificação da palavra PAZ. Para uma melhor compreensão, aplicamos esse mesmo raciocínio nas horas de um relógio, no qual temos um conjunto de 12 horas. Tomamos como exemplo, às 13h que corresponde a 1h: 13 dividido por 12, deixa resto 1. Dados esses e outros exemplos, representamo-los na linguagem das congruências: $28 \equiv 2 \pmod{26}$, $13 \equiv 1 \pmod{12}$, e solicitamos que assistissem ao vídeo: "Aritmética - Aula 42 -7+6=1. Aritmética modular"do Programa de Iniciação Científica da OBMEP acessando o *link*: <https://www.youtube.com/channel/UC5azyx8w7Y5qzASuxDSseO>.

Durante a atividade, um dos grupos demonstrou uma certa confusão quando utilizaram os copos para fazer o deslocamento das letras, não conseguiam diferenciar entre o alfabeto que representava a mensagem original e o que seria usado para cifragem. No entanto, na reunião com o grupo, pelo *Google Meet*, conseguimos elucidar as dúvidas e todos conseguiram concluir o exercício. Logo após, conversamos sobre as questões propostas, dificuldades, pontos positivos e negativos. Avaliaram positivamente a atividade e, no questionário final, analisado na seção 5.4, apontaram como a mais interessante de toda a intervenção.

Como atividade pré-classe, solicitamos que os participantes assistissem ao vídeo gravado pela professora e disponibilizado no google sala de aula através do link: <https://www.youtube.com/watch?v=cI08HSYIzwM>. Nele, partimos da cifra de César e abordamos a ideia de função, lei de formação, valor de $f(x)$, Função Injetora, Sobrejetora, Bijetora e Inversa. Também, foi disponibilizado o texto que baseamos para elaboração do vídeo, a fim de que pudessem fazer a leitura e rever os exemplos dados. Orientamos

que fizessem as anotações necessárias para participar do próximo encontro e para que responder ao *quiz* elaborado no *Wordwall*: <https://wordwall.net/play/21138/567/227> em forma de jogo de combinação, figura 5.5, envolvendo função e a Cifra de César.

Figura 5.5: Jogo de Combinação: Criptografia e Função



Fonte: Dados da pesquisa.

Os resultados deste jogo mostraram que os discentes compreenderam que a função seria o algoritmo utilizado para cifrar mensagens e já demonstravam um certa noção de congruência, visto que, dada as transformações $f(x) = x+13(mod26)$ e $f(x) = 5x(mod26)$, cerca de 72% deles conseguiram responder corretamente, como ficariam a cifragem das palavras ESCOLA e UNIÃO, respectivamente, por meio dessas expressões. No entanto, 50% se equivocaram ao identificar as funções que correspondiam a codificação das palavras ESTUDO e COLEGA, demonstrando dificuldade em associar uma dada situação a linguagem algébrica, nesse caso, a lei de formação da função. Diante disso, preparamos mais exemplos para serem discutidos no encontro seguinte.

Nas questões que abordaram o cálculo de $f(x)$, a classificação da função em injetora ou sobrejetora e função inversa, o nível de acertos foi superior a 81%, revelando que os discentes podem ter se apropriado do material de estudo com uma certa dedicação, pois como se tratava da introdução de conceitos, seria compreensível um percentual maior de erros. Outro ponto a ser ressaltado é que as questões eram objetivas, então, é possível que tenham "chutado" respostas, por isso, foram elaboradas perguntas abertas para a atividade colaborativa que seria aplicada na etapa posterior.

5.2.3 Terceiro Encontro

Neste encontro, inicialmente, conversamos sobre função a partir das anotações que fizeram do vídeo e das análises dos resultados do jogo realizado na atividade pré-classe. Gastamos mais tempo do que o previsto para elucidar as dúvidas, uma vez que questionaram sobre quase todos os pontos abordados no vídeo. Dessa forma, explicamos outros exemplos, focando nas dificuldades observadas, principalmente na lei de formação e injetividade.

Na sequência, orientamos que os grupos se reunissem para resolução da atividade: "Usando Funções Para Cifrar e Decifrar Mensagens". As questões foram elaboradas com base na proposta de Ganassoli e Schankoski (2015), Rodrigues (2013) e Costa (2014), citadas na seção 2.1.1, tendo em vista a realidade da turma. Os estudantes deveriam considerar o alfabeto da tabela 2.7 para responder aos questionamentos. No primeiro deles, apresentamos a seguinte situação:

1- Clara deseja enviar uma mensagem codificada para Bia. Sabendo que o conteúdo da mensagem será: ENCONTRE-ME NA PRAÇA DAS ARTES e que a regra será: valor da letra +9, ajude Clara nesta missão.

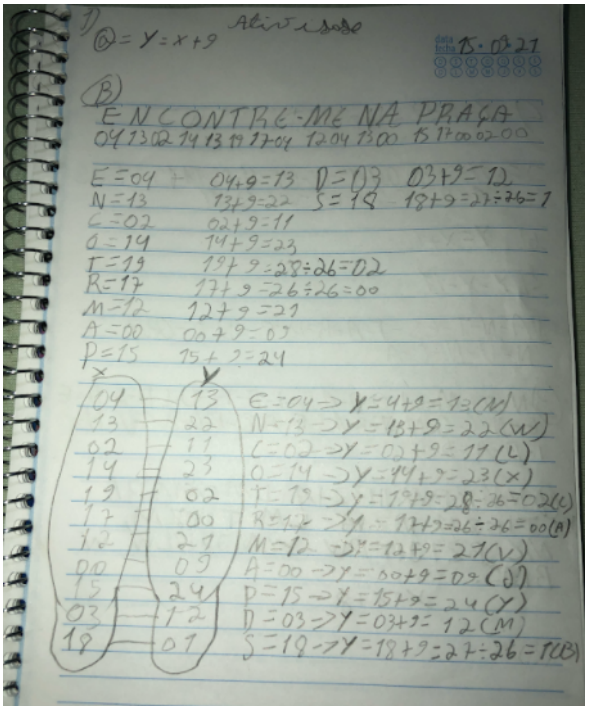
a) Reescreva a regra na linguagem matemática, atribuindo ao valor da letra da mensagem original a variável x e ao valor da letra cifrada, y .

b) Utilizando o valor de cada letra na tabela acima, cifre a mensagem.

c) Encontre a função inversa que Bia deverá utilizar para decifrar a mensagem de Clara.

Vejamos, na figura 5.6 algumas respostas obtidas:

Figura 5.6: Resposta do Grupo 4 para a 1º Questão da Atividade: Usando Funções para Cifrar e Decifrar Mensagens



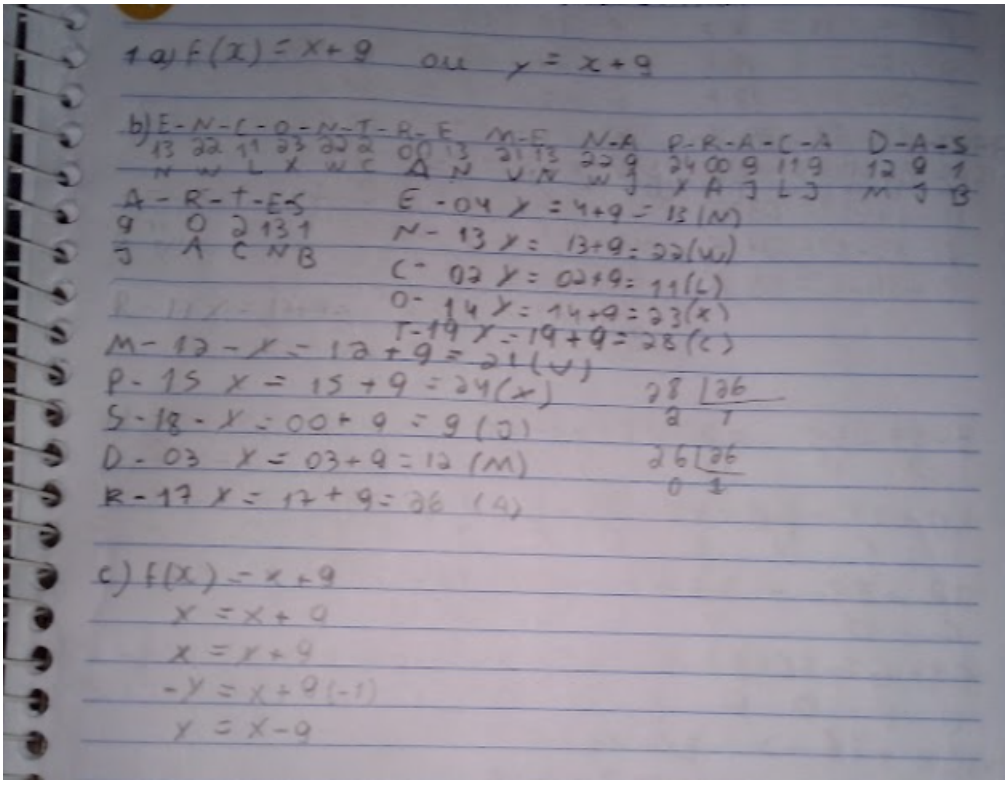
Fonte: Dados da pesquisa.

Nesta resposta, entregue pelo grupo 4, percebemos que, apesar de não ter colocado a frase completa, foi coerente nos cálculos, desenharam a relação no diagrama de *venn* e conseguiram aplicar os conhecimentos sobre congruência ao cifrarem as letras T, R e S. O item c foi respondido na página seguinte como $y = x - 9$.

A próxima resposta, figura 5.7, foi do grupo 3, que também demonstrou ter compreendido os conceitos estudados, escreveram a notação de função como $f(x)$ e, diferente do

grupo anterior, expôs como fizeram para encontrar a função inversa.

Figura 5.7: Resposta do Grupo 3 para a 1º Questão da Atividade: Usando Funções para Cifrar e Decifrar Mensagens



Fonte: Dados da pesquisa.

Dois grupos responderam a atividade de forma incompleta, não apresentaram todos os cálculos e cometeram equívocos em relação a função inversa, como podemos observar nas respostas no grupo 6, figura 5.8.

Provavelmente, estes alunos não compreenderam tal conceito e tentaram se basear no exemplo que demos a partir da função $f(x) = 2x + 5$, cuja inversa é $f^{-1}(x) = \frac{x-5}{2}$, porém não conseguimos identificar a lógica utilizada. Diante disso, tentamos orientar esses estudantes por meio do *Google Meet*, *Classroom* e *Whatsapp*, como mostra o diálogo com A29:

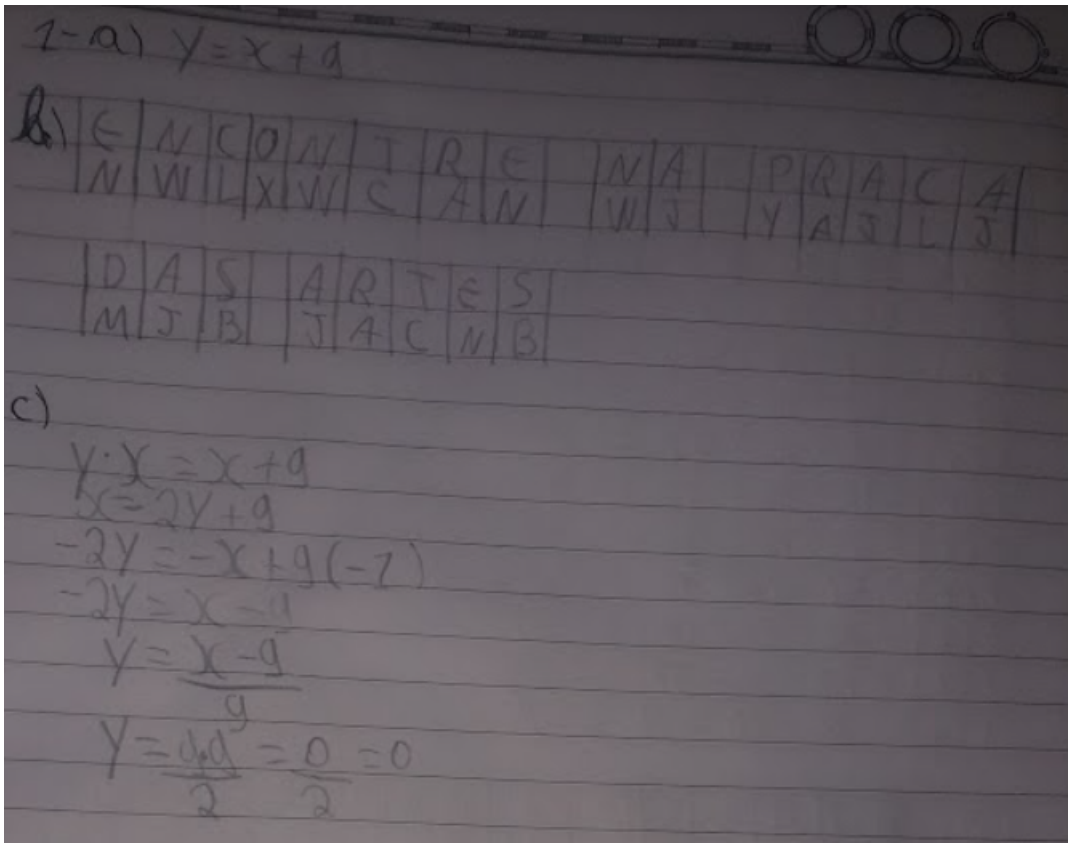
Pesquisadora: "Na letra c do 1 é a inversa da função que escreveu na letra a. Observe também a letra c do 2; A questão 3 está correta, mas precisamos melhorar a notação, exemplo: F(55)= (55-16)/3."

A29: "Pró, a senhora poderia me orientar na letra c da 1, veja se o que fiz está correto?"(enviou os cálculos no *Whatsapp*, mas como a imagem não estava muita nítida, faremos a transcrição).

$y = x + 9 > x = y + 9 > -y = -x + 9(-1) > y = x + 9 > y = \frac{x+9}{y}$

Pesquisadora: " Por que o 9 continuou positivo ao ser multiplicado por (-1)? De onde saiu o denominador y na resposta final?"

Figura 5.8: Resposta do Grupo 6 para a 1º Questão da Atividade: Usando Funções para Cifrar e Decifrar Mensagens



Fonte: Dados da pesquisa.

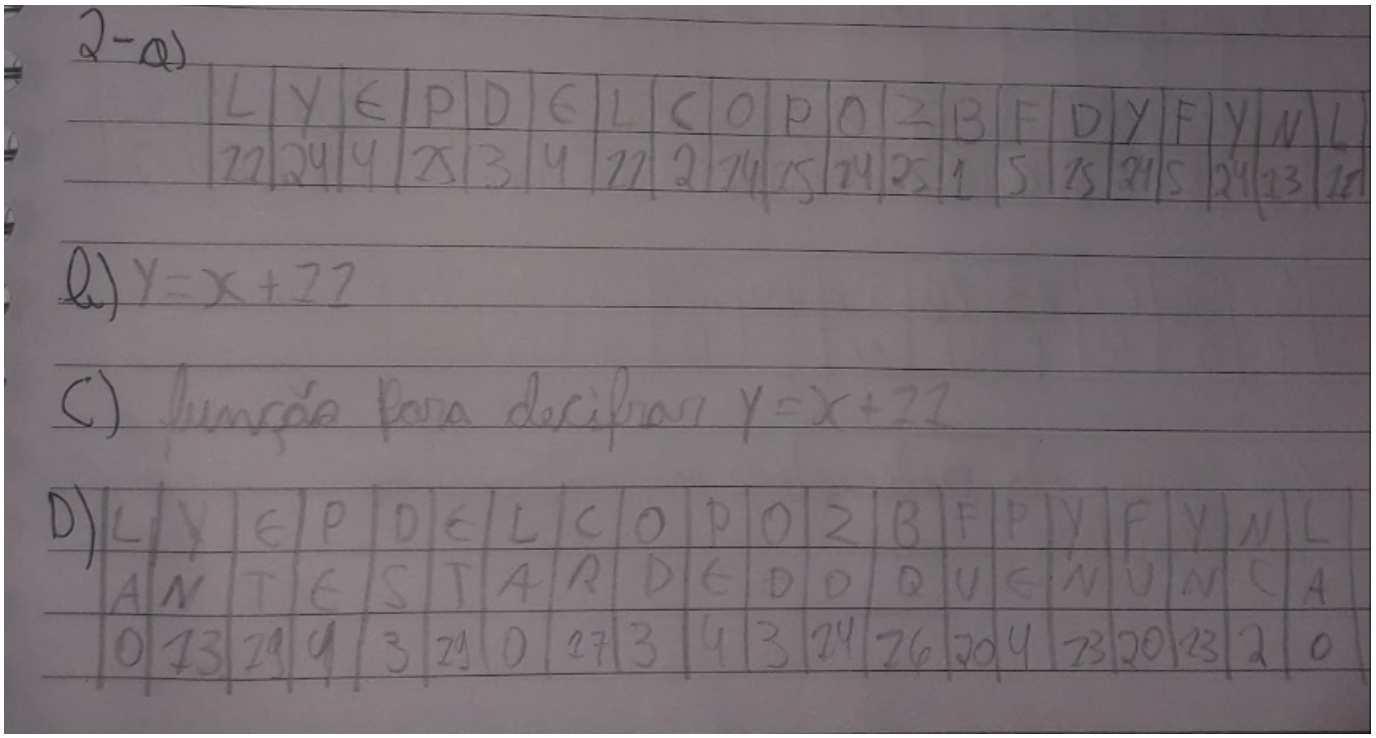
Parece que na compreensão deles, a função inversa, obrigatoriamente, precisava ser escrita com denominador, seguindo o exemplo dado no vídeo. Mas, através dos *feedbacks*, conseguimos auxiliar aqueles que se dispuseram a refazer a atividade, uma vez que um dos grupos não demonstrou interesse.

Na letra c da questão 2 o grupo 6 cometeu o mesmo equívoco, quando solicitamos que escrevessem a função para decifrar a mensagem, ou seja, a função inversa. Todavia, não escreveram denominador e decifraram corretamente a mensagem, conforme verificamos na figura 5.9. Ao questionarmos como decifraram a mensagem, visto que não haviam escrito a inversa de forma coerente, responderam que estavam usando o *kit* de encriptação da aula anterior. Podemos inferir que não construíram o entendimento de que a função inversa estava associada a decodificação e isso serviu para ratificar o quanto a pesquisa educacional, com o agravante de estar sendo desenvolvida de forma remota, poderia sofrer interferências que fogem do controle do pesquisador. Se a intervenção tivesse sido presencial, eles não teriam usado o *kit* e poderiam ser melhor orientados. Por outro lado, isso mostra uma certa autonomia ao buscar solução para o problema proposto.

Enunciamos a questão 3 e 4 como desafios:

3- (Desafio 1): A mensagem abaixo é uma frase de Einstein que foi cifrada com a

Figura 5.9: Resposta do Grupo 6 para a 2º Questão da Atividade: Usando Funções para Cifrar e Decifrar Mensagens



Fonte: Dados da pesquisa.

função $f(x) = 3x + 16$, descubra seu conteúdo!

55-58 52-28-40-58 25-16 25-40-31-40-22-76-49-25-16-25-28 28-55-22-58-55-73-67-16-70-28 16 58-61-58-67-73-76-55-40-25-16-25-28

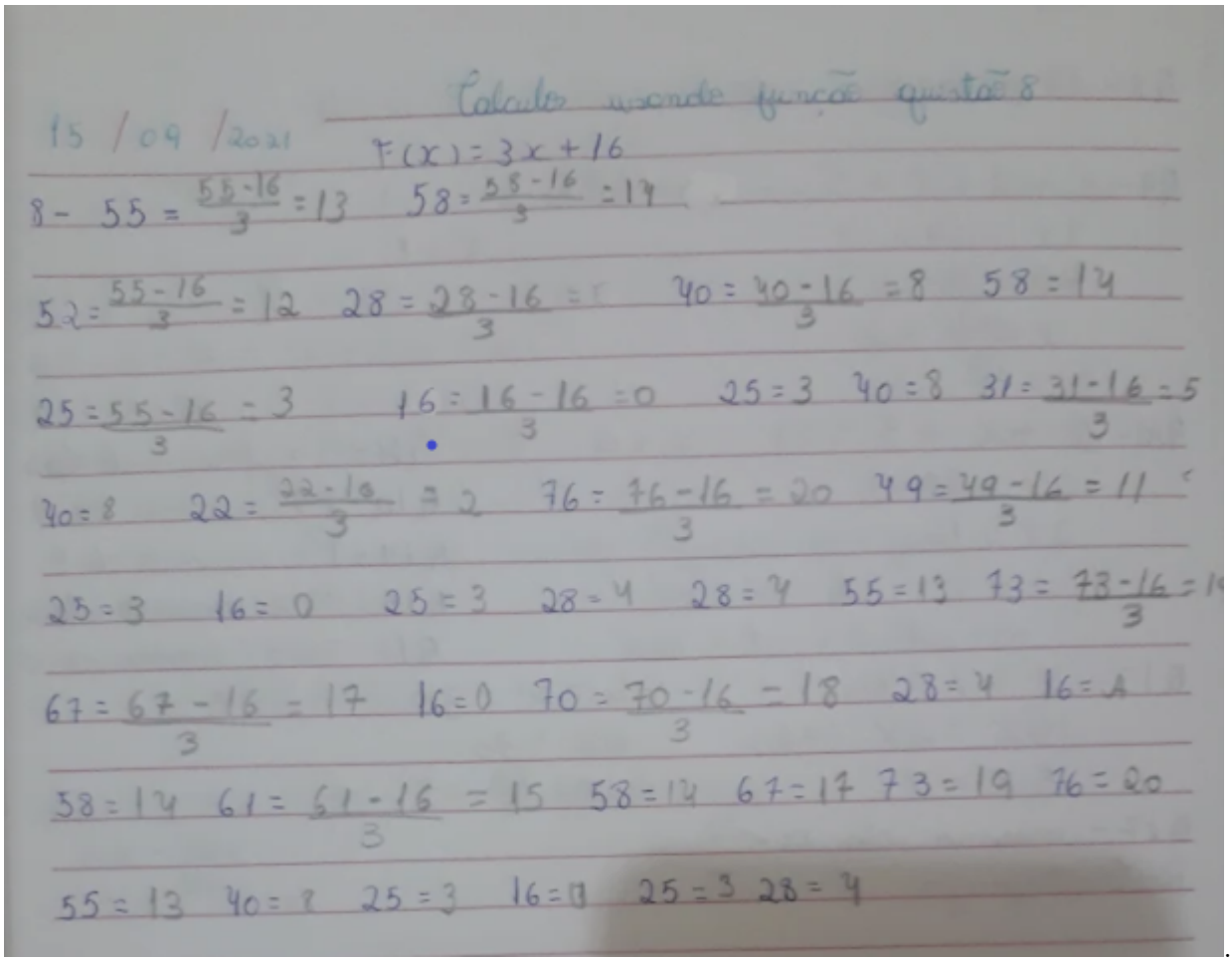
4- (Desafio 2): Agora é com você, escolha uma frase famosa ou crie uma, com no máximo 30 letras, determine uma função e faça a codificação da frase. Depois, trocaremos com outro grupo para que possa decifrá-la.

No primeiro desafio, os estudantes deveriam determinar a função inversa para decifrar a mensagem. No entanto, apesar de não terem escrito a função inversa, fizeram os cálculos de forma coerente, como mostra a resposta do grupo 2, na figura 5.10. Percebemos, portanto, que mesmo não se preocupando com a questão das notações, conseguiram compreender empiricamente a noção de inversa.

Sobre o trabalho com função inversa no 9º ano do Ensino Fundamental, Rodrigues (2013), cujo trabalho já comentamos na seção 2.1.1, cita que a abordagem foi feita de forma implícita, uma vez que tal conteúdo só seria formalizado no Ensino Médio. Entretanto, apesar de estarmos conscientes disso, resolvemos apresentar o conceito, levando em consideração o nível dos participantes e a perspectiva que, no ano seguinte, já estaria familiarizado com o conteúdo, facilitando a sua sistematização.

No segundo desafio, os alunos enviaram, através do *Classroom*, a frase escolhida cifrada e a função que utilizaram, então, fizemos as trocas entre os grupos que conseguiram

Figura 5.10: Resposta do Grupo 2 para a 3º Questão da Atividade: Usando Funções para Cifrar e Decifrar Mensagens



Fonte: Dados da pesquisa.

fazer a decodificação sem nenhuma dificuldade, visto que já tinham discutido as questões anteriores.

Finalizamos esse encontro conversando sobre as dificuldades que encontraram na resolução das questões e com as orientações para os estudos pré-classe que envolveria o Sistema RSA. Disponibilizamos no *Classroom* dois vídeos (<https://youtu.be/3jR62Mew8X4> e <https://youtu.be/GAR1Ur_2IGk> que explicavam o passo a passo do método RSA e um *quiz* (<https://wordwall.net/play/21139/212/458>, figura 5.11, com as opções verdadeiro ou falso com o conteúdo abordado no vídeo.

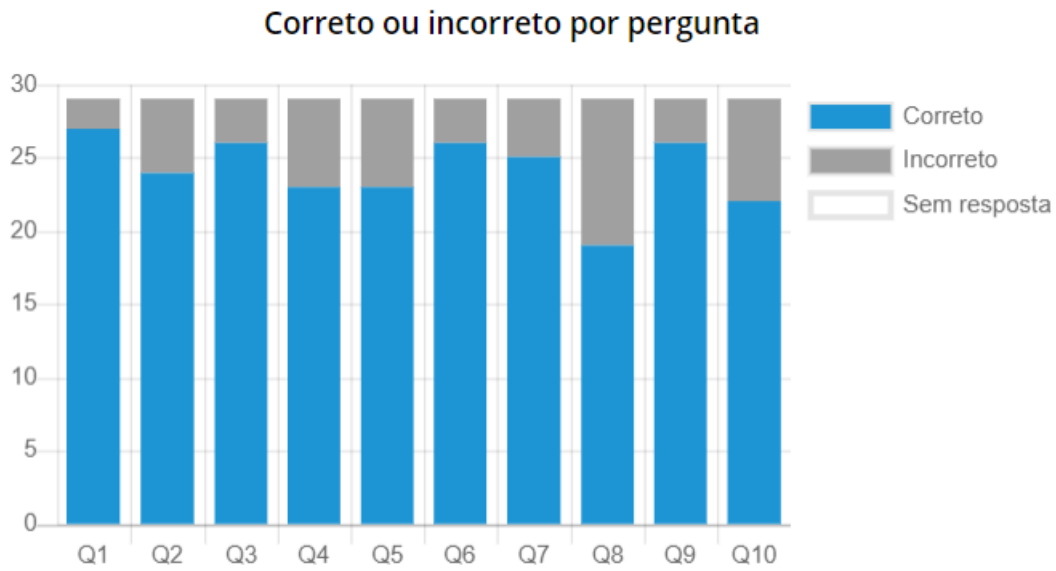
Apesar da complexidade desse método, selecionamos os vídeos, elaboramos o jogo e as atividades levando em consideração o nível dos estudantes. Com a análise do jogo, percebemos que a maioria obteve um resultado satisfatório, acertando mais de sete respostas, ao julgarem as dez afirmações propostas como verdadeiras ou falsas. No gráfico da figura 5.12, apresentamos os resultados por pergunta, gerado pela plataforma do *Wordwall*, no qual verificamos que a questão com maior quantidade de erros foi a 8 com a seguinte afirmação: "Na criptografia RSA, p e q (números primos escolhidos) e o produto

Figura 5.11: Jogo RSA

Fonte: Dados da pesquisa.

$n = p \times q$ são mantidos em segredo, ou seja, formam a chave privada". Acreditamos que esse quantitativo pode estar relacionado pela interpretação equivocada , uma vez que p e q, realmente, fazem parte da chave privada, mas $n = p \times q$, forma a chave pública.

Figura 5.12: Jogo RSA - Resultado



Fonte: Dados da pesquisa.

5.2.4 Quarto Encontro

Neste encontro, abordamos o sistema RSA. Iniciamos com uma conversa para que os alunos expusessem o que conseguiram compreender sobre esse método a partir dos vídeos que assistiram. Alguns alunos estavam mais interessados em conhecer o RSA e, por isso, anotaram o passo a passo e já haviam feito o processo de encontrar a chave pública e privada.

As primeiras etapas da atividade colaborativa foram realizadas com todos os grupos

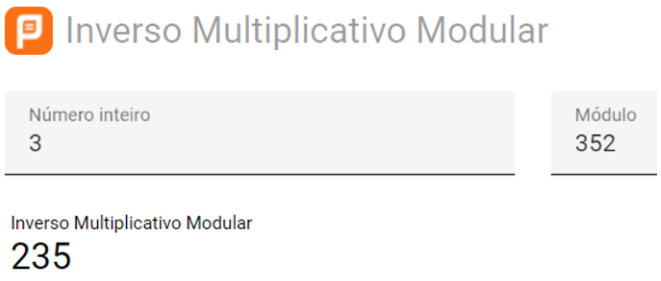
reunidos pelo *Google Meet*. No item 1, solicitamos que os grupos escolhessem dois números primos, mas para facilitar o processo e evitar que selecionassem os mesmos, entregamos a cada grupo os números que seriam utilizados nas etapas seguintes. Fizemos uma revisão sobre o conceito de número primo e indicamos esse site: <http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php> para que pudessem conhecer outros primos.

Chamamos os números primos que cada grupo recebeu de p e q e, como exemplo, usamos $p = 17$ e $q = 23$. No item 2, calcularam $n = p \times q$ ($n = 17 \times 23 = 391$) usando as calculadoras dos celulares, então, não houve dificuldades. Na sequência, item 3, deveriam calcular $\varphi(n) = (p-1)(q-1)$ ($\varphi(n) = (17-1)(23-1) = 352$. Ao apresentar essa expressão, ficamos satisfeitos quando os alunos perceberam que se tratava de uma função, logo, solicitamos que cada grupo determinasse seu $\varphi(n)$.

No item 4, inicialmente, abordamos o conceito de coprimos dando alguns exemplos, para que os grupos pudessem escolher um número e que satisfizesse $1 < e < \varphi(n)$, sendo e e $\varphi(n)$ coprimos. Para evitar equívocos, pedimos que cada grupo escrevesse no chat o número que escolheram. No nosso exemplo, escolhemos $e = 3$.

O próximo item, questão 5, foi o que os grupos tiveram mais dificuldade para compreender. Eles precisavam encontrar um número d que satisfizesse a congruência: $e \times d \equiv 1 \pmod{(p-1)(q-1)}$. Vimos alguns inversos multiplicativos de números inteiros e, a partir do exemplo que demos $3 \times d \equiv 1 \pmod{352}$, ressaltamos que isso significava que o produto $3 \times d$ ao ser dividido por 352 deixava resto 1. Com isso, eles encontraram o número $d = 235$ por tentativa e erro. No entanto, indicamos a calculadora online, de inverso multiplicativo modular, disponível no *link*: <https://pt.planetcalc.com/3311/> para que pudessem fazer esse cálculo. Orientamos que no espaço "número inteiro", deveriam escrever o valor de e, em "módulo" o valor de $\varphi(n)$ e que abaixo apareceria o valor de d, ou seja, do inverso multiplicativo modular, como observamos na figura 5.13.

Figura 5.13: Calculadora de Inverso Multiplicativo Modular



Fonte: Dados da pesquisa.

Com esses números encontrados, informamos que cada grupo já tinha sua chave pública e privada. Os números p, q e d faziam parte da chave privada e deveriam ser mantidos em segredo, enquanto os números n e e formavam a chave pública e poderia ser passada para qualquer pessoa. Por conseguinte, trocamos as chaves públicas entre os grupos e cada um

recebeu uma frase para que fosse pré-codificada com a tabela ASCII e codificada usando a chave que receberam e a congruência $C \equiv M^e \pmod{n}$, que deveria ser resolvida através da calculadora online disponível no *link*: <https://www.calculadoraonline.com.br/divisao-polinomios>. Nesta congruência, C correponde ao texto cifrado, M ao valor de cada bloco pré-codificado, n e e a chave pública.

Como exemplo, ciframos o nome ANA. Ao ser pré-codificado, encontramos: 065-078-065. Na calculadora, figura 5.14, digitamos M^e no dividendo e o valor de n no divisor. Dessa forma, digitamos 65^3 no dividendo, 391 no divisor, clicamos em calcular e consideramos o resto da divisão, isto é, 143. Logo, o bloco 065 é cifrado como 143.

Figura 5.14: Calculadora Online - Divisão de Polinômios

Fonte: Dados da pesquisa.

Orientamos que os grupos fizessem esse processo até que todos os blocos fossem cifrados. Ao finalizar essa etapa, a mensagem deveria ser entregue ao grupo de origem da chave pública para que fizessem a decodificação, usando a mesma calculadora e a chave privada aplicada na congruência: $M \equiv C^d \pmod{n}$. Entretanto, como não havia tempo suficiente, enviaram as questões que resolveram no google sala de aula e a última etapa, seria aplicada como prova da gincana criptográfica, no encontro seguinte.

Finalizamos o encontro síncrono com uma conversa sobre a atividade realizada. Dentre os que participaram da discussão, alguns disseram que achava que seria mais difícil e outros, com uma certa razão, replicaram expondo que só não foi mais complicada, porque utilizaram calculadoras. Então, salientamos, que alguns cálculos demandariam muito tempo, visto que algumas potências apresentaram expoentes elevados e, consequentemente, os dividendos seriam enormes, por isso, optamos por usar as calculadoras, além disso, na prática, o processo é realizado por computadores.

Por fim, orientamos a atividade pré-classe seria nos mesmos grupos e consistia na realização de uma pesquisa com elaboração de um pequeno vídeo, sobre algum tipo de criptografia, que ainda não havia sido abordado nos nossos estudos. Diante dessa tarefa, houve uma certa apreensão, porque acharam que na gravação deveriam se expor. No entanto, explicamos que poderiam gravar somente as imagens com uma narração ou em formato de vídeo animado. Falamos também, que se caso desejassem, poderíamos excluir a tarefa, mas resolveram que iriam fazer e decidimos incluí-la como a primeira prova da gincana criptográfica.

Neste trabalho, surgiram muitas dúvidas sobre conteúdo e ferramentas que poderiam utilizar nas gravações e edições. Tentamos elucidar, através de mensagens pelo *WhatsApp*, mas, percebemos que para obter resultados satisfatórios seria necessário muito mais tempo. Precisaríamos acompanhar desde as pesquisas e a re/construção do conhecimento, para evitar os plágios, até o processo de edição dos vídeos, porque apesar de utilizarem diversas ferramentas tecnológicas, muitos demonstraram que careciam de uma maior orientação para realizar tal tarefa.

Ressaltamos que indicamos O *powerpoint* e o *FlashBack Express Recorde* para gravações de tela, e o *YouCut* para edição, por acreditarmos que seriam mais fáceis de manusear. Contudo, os participante poderiam usar qualquer outro recurso com essa finalidade, uma vez que, comungamos das ideias de Alves (2016, p. 6), ao afirmar que é necessário a construção de um sentido diferenciado para o uso das tecnologias nos espaços escolares, permitindo que os alunos façam suas escolhas e sejam "atores e autores das suas trajetórias de aprendizagem".

5.3 Quinto Encontro

Neste último encontro, realizamos a gincana criptográfica que serviu como um momento de lazer e de avaliação, visto que os estudantes se divertiram com a competição. As provas estavam relacionadas com conteúdos trabalhados nos encontros anteriores, permitindo verificar o quanto conseguiram absorver do que foi estudado.

De início conversamos sobre as regras, sendo definido o seguinte: os grupos seriam os mesmos dos outros encontros e seriam pontuados com 10 pontos para a tarefa cumprida mais uma pontuação extra de acordo com o tempo gasto na prova: 1º lugar: 5 pontos; 2º lugar: 4 pontos; 3º lugar: 3 pontos; 4º lugar: 2 pontos; 5º e 6º lugares: 1 ponto. Questionaram sobre a premiação, então informamos que seria simbólica, cada componente do grupo vencedor, escolheria um livro ou uma caixa de chocolate. Também enfatizamos que numa competição sempre havia vencedores e vencidos, mas, no nosso caso, todos ganhariam conhecimentos. Outro ponto que discutimos foi sobre o respeito entre as equipes, caso contrário, seriam penalizados com a perda de pontos.

Na primeira prova, os grupos deveriam apresentar os vídeos produzidos sobre outras cifras. Todos cumpriram a prova, contudo, conforme já citamos, essa foi uma das atividades

que precisaria de mais tempo para ser realizada com êxito, pois não houve muito capricho e eles praticamente plagearam conteúdos que encontraram na internet, com pouca ou nenhuma discussão. O único ponto positivo foi que perceberam que existem muitos métodos de criptografia, além dos que foram abordados.

A segunda prova envolveu a decodificação da mensagem que os grupos haviam cifrado no encontro anterior usando o RSA. Orientamos que cada grupo receberia a mensagem que foi criptografada por meio da sua chave pública e que usaria a receita $M \equiv C^d \pmod{n}$ e a calculadora online: <https://www.calculadoraonline.com.br/divisao-polinomios>, para decifrá-la. Ressaltamos que nesta congruência, M é o valor da letra de acordo com a tabela ASCII, C é a letra cifrada (que corresponde aos blocos do texto que cada um receberia, d é a chave privada e n é o produto dos dois primos que o grupo recebeu). Como já tinha familiarizado com a calculadora, somente um dos grupos demorou mais tempo na prova, porque confundiu o valor de d com $\varphi(n)$.

Na terceira prova (esteganografia), apresentamos uma imagem com seis faces contendo números, aparentemente ocultos, que os grupos deveriam descobrir para ordená-las numa sequência lógica. Começaram observando a figura, mas não conseguiram identificar a regra, até que o grupo um entendeu a regra, comentando com os outros que na cabeça haviam números. Dessa forma, todos conseguiram completar a tarefa, respondendo através da captura de tela e enviando as respostas no *Whatsapp* e no *Classroom*.

Nesse ponto, ao observar os grupos estavam se ajudando, percebemos que a disputa estava sendo saudável, o que nos deu um certo alívio, pois a nossa maior preocupação era que a competição pudesse ter efeito inverso ao esperado. Diante disso, parabenizamos o grupo pela atitude, incentivando os outros a seguirem o exemplo, desde que fossem apenas dicas, isto é, não poderiam dar a resposta final do desafio.

A quarta prova foi um caça-palavras elaborado pela pesquisadora no *site:* <https://www.geniol.com.br/palavras/caca-palavras/criador/> envolvendo criptografia e matemática. Como na prova anterior, responderam por meio da captura de tela, como mostra a figura 5.16. Não apresentava dificuldades, mas devido a pressa, os dois primeiros grupos que concluíram tiveram que rever a resposta, porque faltavam encontrar palavras.

Na quinta prova, os grupos deveriam responder a duas questões de múltipla escolha que adaptamos do simulado ENEM Integrado 2021, da FTD. Consistia em codificar e decodificar as palavras indicadas por meio de um código secreto com base numa correspondência entre as letras do alfabeto e os números naturais. Era semelhante ao código de César e o deslocamento das letras deveria ser feito de acordo com o número de letras da palavra que seria codificada. Como exemplo, usamos a palavra Alan, uma palavra de 4 letras cifrada com a sequência 4-15-4-17, já que: A→0+4=4

L→11+4=15

A→0+4=4

N→13+4=17

Figura 5.15: Resposta do Grupo Um para a Terceira Prova

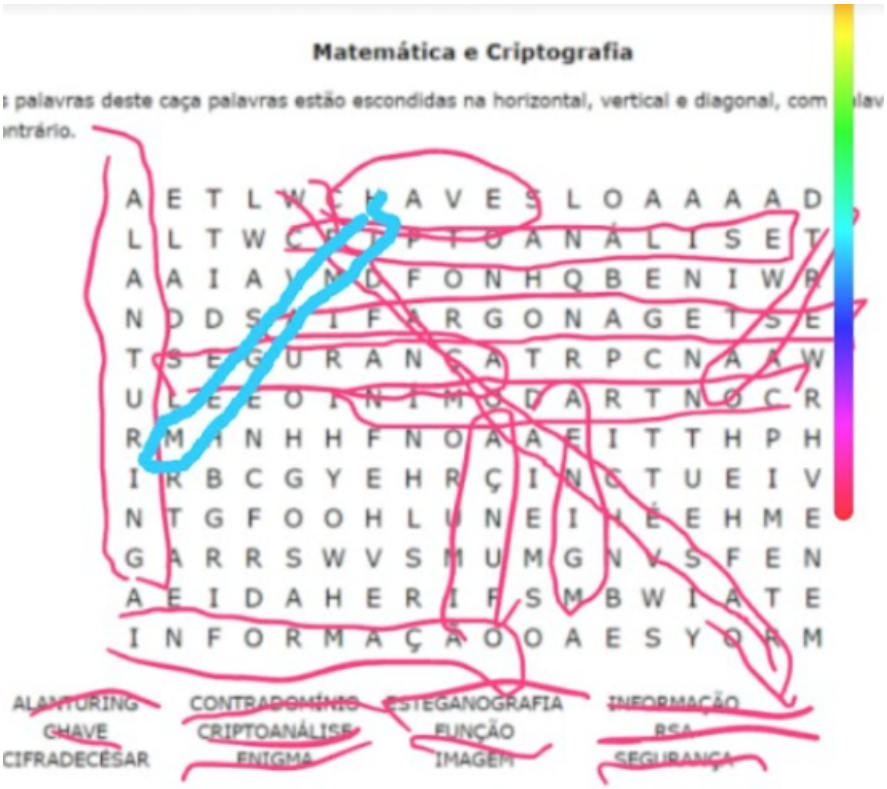
Fonte: Dados da pesquisa.

Com base na explicação, precisavam descobrir a sequência que correspondia a mensagem "ADA" "LOVELACE" e a palavra referente a sequência 10-24-8-20-17-6. Mesmo não usando a notação, os participantes perceberam que se tratava de uma função, semelhante as atividades que haviam feito no terceiro encontro. Então, questionamos como encontraram a resposta da segunda questão, metade falaram que foi pela lógica, mas os demais fizeram cálculos. Como mostra a figura 5.17, o grupo 4 utilizou intuitivamente o conceito de função e de inversa.

Na sexta prova abordamos a Cifra de Cesár e os grupos utilizariam o kit de encriptação, usado no segundo encontro, para cifrar o nome JÚLIO CÉSAR usando a chave 7, na questão 1 e decifrar a mensagem: SFHLZIR com a chave 17, na questão 2. Mais uma vez, responderam com facilidade, demonstrando compreensão do método.

Ao concluir essa tarefa, faltavam somente cinco minutos para finalizar o horário destinado para atividades síncronas. Comentamos que faltavam somente duas tarefas para concluírmos a gincana. A maioria opinou para que fossem realizadas as provas restantes.

Figura 5.16: Resposta do Grupo 2 para a Quarta Questão



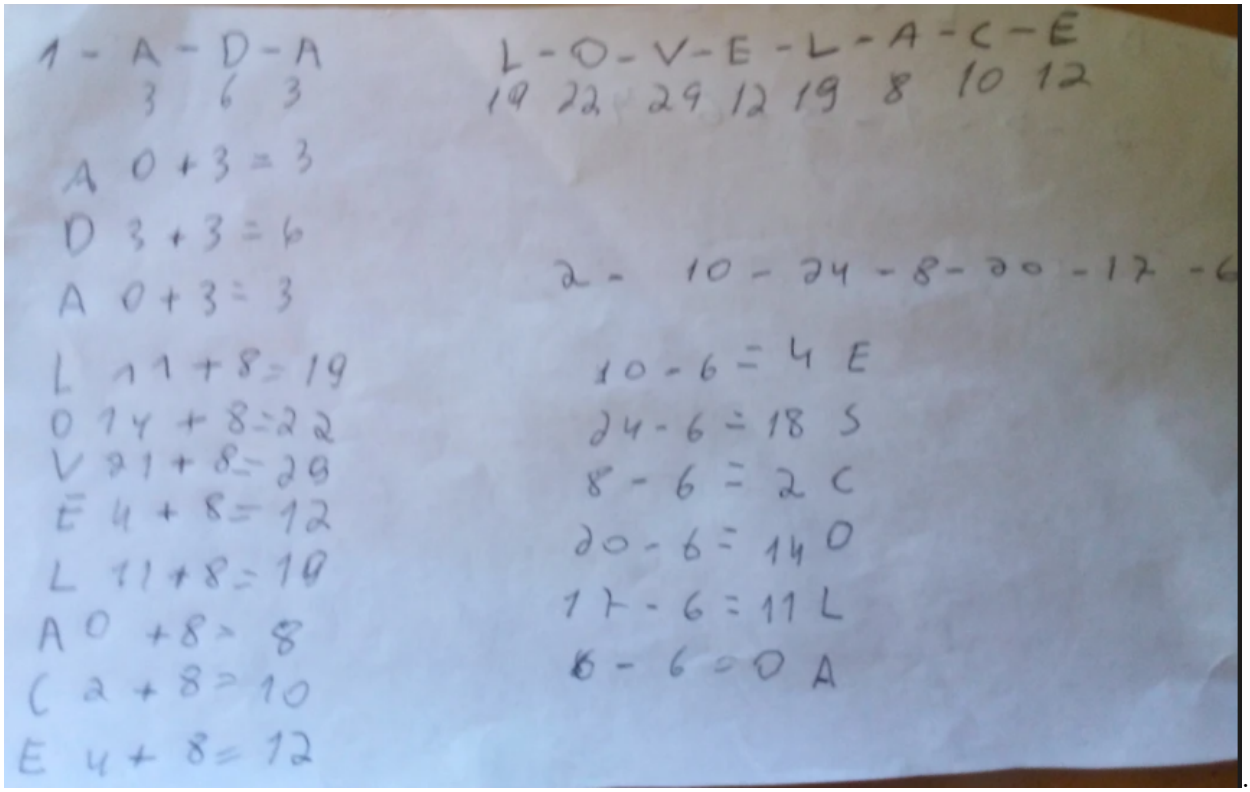
Fonte: Dados da pesquisa.

Essa atitude revelou o interesse dos discentes pela atividade, dado que nos dias de aula normal, dificilmente aceitaria estender o horário. Entretanto os dois alunos que assistiam aula na escola não poderiam participar, visto que a instituição fecharia às 11 horas. Para não deixar ninguém de fora, combinamos que finalizaríamos na segunda-feira seguinte, nas duas aulas de matemática.

Conforme ficou acordado, finalizamos a gincana na segunda-feira da semana seguinte e debatemos sobre o filme: "O jogo da Imitação" que os participantes foram assistindo ao longo da semana.

Na sétima tarefa da gincana, solicitamos que os estudantes cifrassem a palavra CONQUISTAS e decifrassem a mensagem: 21-91-76-21-86-01-66-11-01 usando a função: $f(x) = 5x + 1$ e o alfabeto, conforme tabela tabela 2.7. Nem todas as equipes apresentaram os cálculos de uma forma organizada, mas verificamos que conseguiram associar cada valor da letra a x e fizeram as substituições, de forma coerente, para encontrar $f(x)$. Eles também conseguiram associar a decodificação ao cálculo da inversa, completando a prova de forma satisfatória. Diante disso, foi possível avaliar que as atividades solicitadas anteriormente, foram exitosas no propósito de incitar a aprendizagem do

Figura 5.17: Resposta do Grupo 4 para a Quinta Prova



Fonte: Dados da pesquisa.

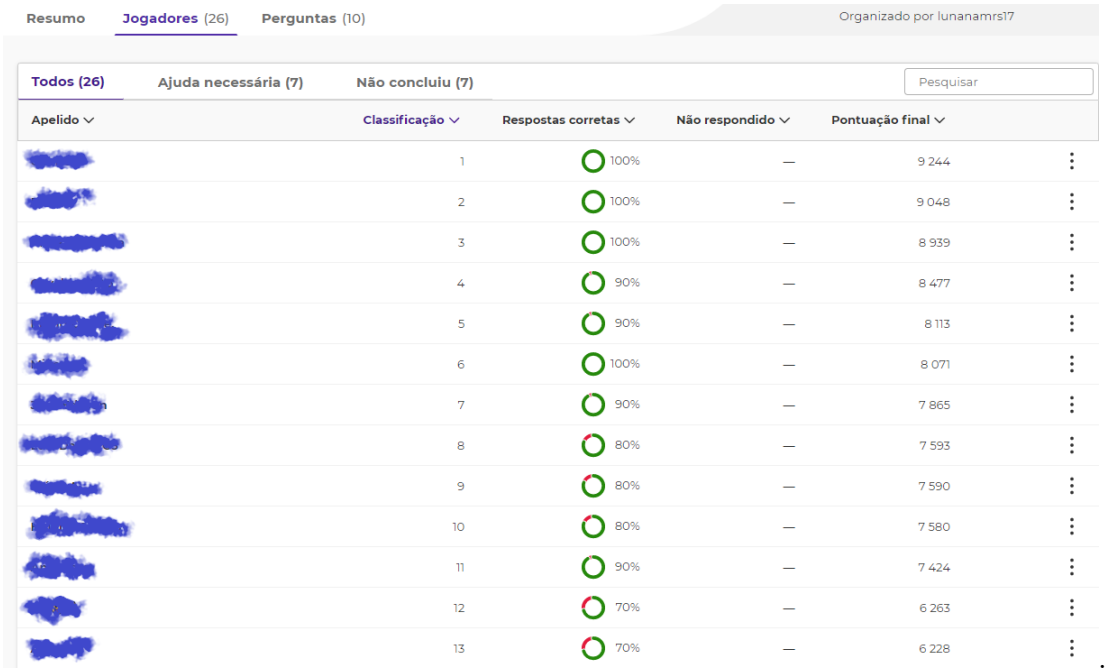
conteúdo abordado nessa questão.

Na última, prova 8, deveriam responder as questões de um jogo que elaboramos no *Kahoot* envolvendo criptografia e matemática. Deveriam participar do jogo individualmente e os grupos seriam pontuados de acordo com o pódio. Segundo os relatórios do jogo, figura 5.18, dos 26 alunos que conseguiram acessar o jogo, sete não conseguiram concluir, relatando problemas de conexão. Considerando os dezenove estudantes que finalizaram, 70% acertaram entre 7 e 10 questões, o que vimos como positivo, uma vez que as questões exigiram conhecimento e controle do tempo (tinham limite de tempo entre 30 e 120 s).

Antes de apresentar o resultado final da gincana, debatemos sobre o filme a partir das perguntas solicitadas que questionaram sobre cenas que os estudantes mais gostaram, relação entre as máquinas de Turing e os modernos computadores, relação entre criptografia, matemática e a Segunda Guerra Mundial e sobre o preconceito. Essa discussão foi planejada para iniciar a intervenção com o objetivo de que os alunos percebessem a importância da criptografia e da matemática, entretanto, devido ao tempo, combinamos que assistiriam ao longo da semana e deixaríamos o debate para a conclusão, tendo o mesmo objetivo.

A diferença de pontuação entre os grupos foi bem pequena: 100, 102, 93, 95, 107 e 98. No entanto, o grupo cinco foi o vencedor e, apesar dos outros também ter se empenhado, seus membros demonstraram mais interesse desde o início, trabalhavam com bastante cooperação e solidariedade, auxiliando colegas das demais equipes. Diante disso,

Figura 5.18: Resultado do Kahoot



Fonte: Dados da pesquisa.

todos consideraram o resultado justo e comentaram que deveriam ser desenvolvidas mais atividades como as que haviam feito ao longo da intervenção.

Conforme já citamos, devido ao tempo disponibilizado para realização da intervenção e o fato do trabalho ser realizado de forma remota, os encontros foram bastante intensos e acreditamos que a diversidade de atividades pode ter favorecido para deixá-los menos cansativos. Finalizamos esta análise com a certeza de que os planos e atividades precisam ser melhorados, mas com a sensação de dever cumprido, visto que, de acordo com as avaliações feitas e diante de todos os obstáculos, os estudantes pareceram estar motivados e a maioria entendeu os conceitos iniciais de função trabalhados a partir da criptografia.

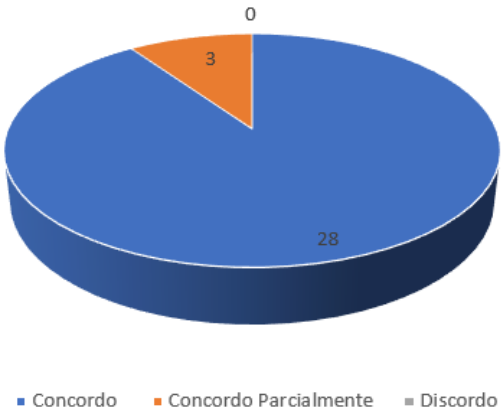
5.4 Avaliação da Intervenção

Ao final da intervenção, solicitamos aos participantes que respondessem outro questionário online, composto por duas questões de identificação, oito questões fechadas e uma questão aberta para que pudessem comentar aspectos positivos e negativos da intervenção. Teve como propósito a avaliação das atividades desenvolvidas e analisar se o objetivo da pesquisa foi atingido, ou seja, se a criptografia possui potencial para estimular a aprendizagem matemática em relação ao conteúdo abordado.

Dentre as questões fechadas, sete eram afirmações que tinham como opções: concordo, concordo parcialmente e discordo. Na primeira, afirmou-se: "Foi interessante estudar matemática relacionada com criptografia.". O gráfico 5.4 mostra que nenhum aluno discordou e que apenas 9,7% concordam parcialmente. Esse resultado foi positivo, uma

vez que, mesmo não concordando totalmente, essa porcentagem ainda é menor do que a dos alunos que dizem não gostar de matemática, cerca de 25%, e pode significar que as atividades conseguiram atraí-los para o estudo do que foi proposto.

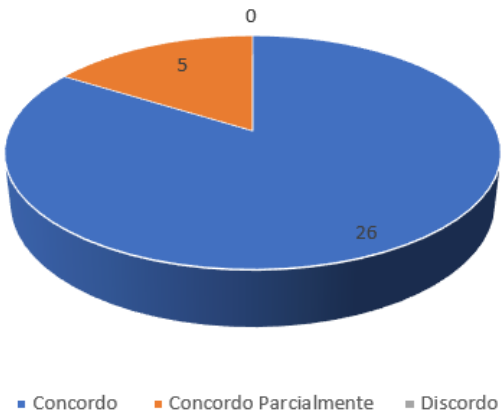
Gráfico 5.4: Respostas dos alunos para a afirmação: "Foi interessante estudar matemática relacionada com criptografia."



Fonte: Elaborado com dados da pesquisa.

A próxima questão, conforme mostra o gráfico 5.5, averigou se na opinião dos estudantes, os estudos propiciaram a aquisição de novos conhecimentos e, apesar da maioria ter concordado, 16% responderam parcialmente, o que pode ser contraditório, visto que o tema e o conteúdo não haviam sido trabalhados anteriormente. Contudo, tais respostas também podem estar relacionadas com o nível de absorção do que foi estudado.

Gráfico 5.5: Respostas dos alunos para a afirmação: "Com os estudos, adquiri novos conhecimentos."



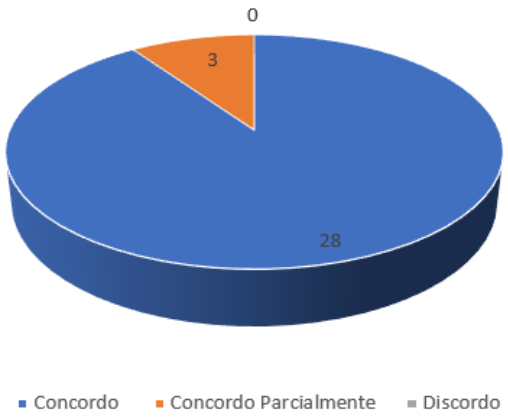
Fonte: Elaborado com dados da pesquisa.

No capítulo 4 apresentamos a metodologia de ensino SAI, os planos de aula e a listagem de atividades que seriam desenvolvidas ao longo dos cinco encontros. No entanto, como tudo seria realizado de forma remota, temíamos não conseguir envolver os alunos nas atividades planejadas. Mas, dos trinta e três estudantes que aceitaram participar da

pesquisa, somente dois deles não conseguiram concluir todas as tarefas solicitadas, uma porcentagem bem menor do que a verificada no cotidiano escolar das duas turmas.

Sobre a forma como o conteúdo foi apresentado, cerca de 81% concordaram que foi atraente e mais de 90% afirmaram que os materiais utilizados (vídeos, textos, filmes, atividades individuais e colaborativas, jogos, entre outros) favoreceram a compreensão do conteúdo. Nesse ponto, demonstraram bastante coerência, pois na questão seguinte, 90% também concordaram que as atividades desenvolvidas contribuíram para entenderem o conceito de função, como mostra o gráfico 5.6.

Gráfico 5.6: Respostas dos alunos para a afirmação: "As atividades desenvolvidas contribuíram para o entendimento do conceito de função."



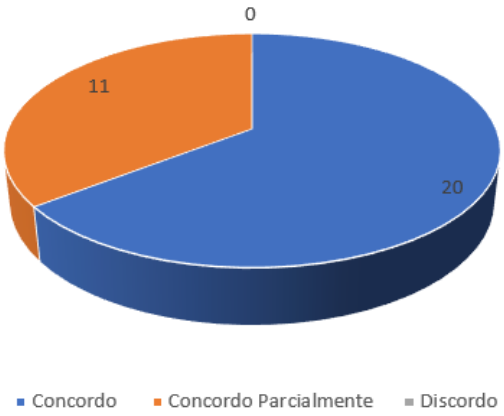
Fonte: Elaborado com dados da pesquisa.

Por outro lado, no item 9, buscamos verificar se os estudantes haviam compreendido o conceito de criptografia e sua finalidade, uma porcentagem bem menor concordou com a afirmação, conforme mostra o gráfico 5.7. Isso pode ser justificado pelo fato de terem percebido a amplitude dessa área, conforme relata A7: "Foi incrível a semana aprendendo criptografia, apesar de ter sido cansativa. Foi ótimo estudar pois era uma área que eu não sabia quase nada e com as aulas e atividades aprendi muito, mas sei que ela envolve muita coisa e que nessa semana eu não aprendi nem metade dela". Porém, no jogo do labirinto (foi descrito na seção do primeiro encontro), ao responderem uma questão fechada que perguntava sobre o objetivo da Criptografia, 100% dos participantes conseguiram acertar.

Na questão 8, averiguamos qual ou quais das atividades desenvolvidas os participantes acharam mais interessantes. Foram listadas 13 atividades mais a opção "todas", logo, o quantitativo total de cada atividade deve levar em consideração os votos obtidos somados com essa opção. Os dados foram tabulados no gráfico 5.8.

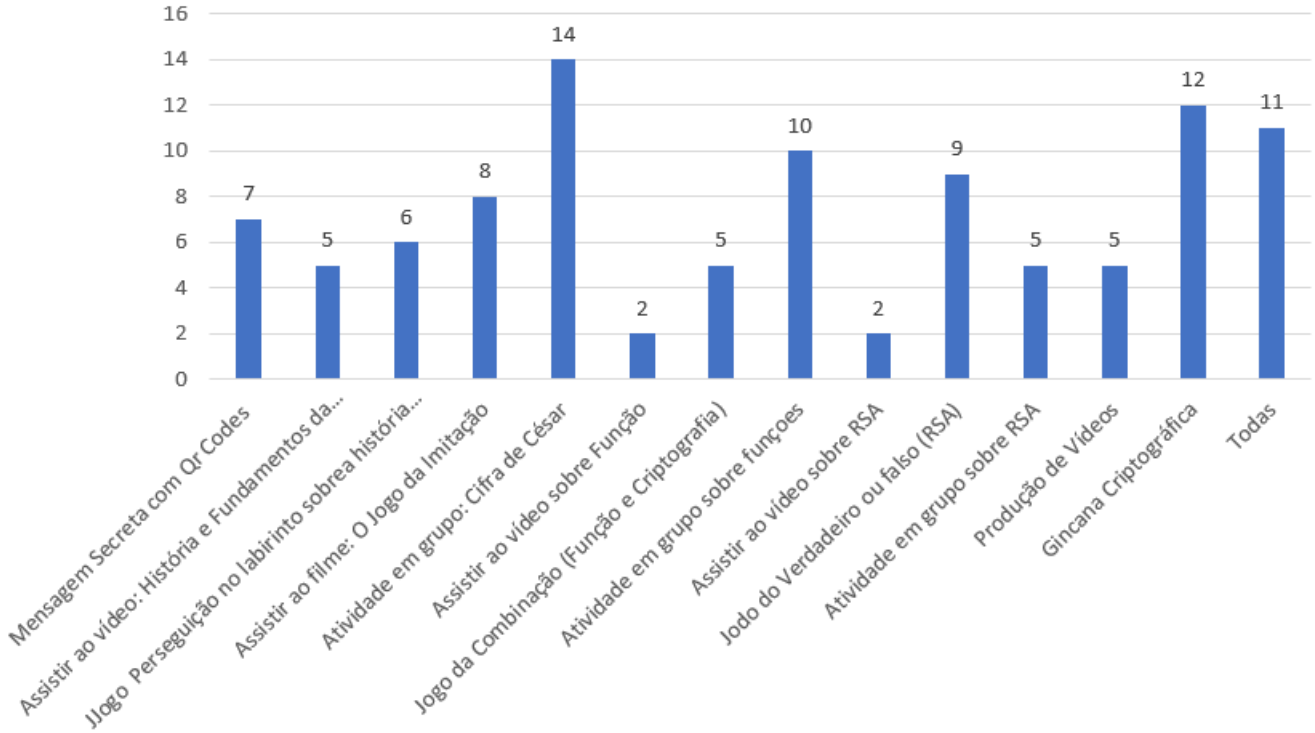
Podemos perceber que eles preferiram as atividades em grupo, a qual foi justificada por A1, na última questão: "As atividades em grupos foram muito boas pois, uns estavam ajudando aos outros, e assim todo mundo entende o assunto". Realmente, foram os momentos de maior interação da pesquisa, pois com eles divididos em grupos e reunidos

Gráfico 5.7: Respostas dos alunos para a afirmação: "Consegui compreender o que é criptografia e sua finalidade."



Fonte: Elaborado com dados da pesquisa.

Gráfico 5.8: Respostas dos alunos para a questão: "Qual (is) das atividades desenvolvidas você achou mais interessante?"



Fonte: Elaborado com dados da pesquisa.

em salas diferentes através do google meet, ficou mais fácil para debaterem, analisarem e responderem as situações problemas e para fazermos as intervenções necessárias.

Além do resultado do questionário, os relatos orais demonstraram que, dentre as atividades colaborativas, a que os estudantes acharam mais interessante foi a Cifra de César, provavelmente, porque manusearam um material concreto, o kit de encriptação, citado no capítulo 4, para auxiliar na solução dos problemas propostos. A motivação para

esta atividade foi importante para a compreensão do principal conteúdo que abordamos na pesquisa, pois fizemos a introdução e explanação do conceito de função a partir da Cifra de César.

A segunda atividade que os participantes acharam mais interessante, foi a gincana criptográfica realizada no último encontro, com o objetivo, de promover um momento de descontração e avaliar, de forma dinâmica, o que foi trabalhado nos quatro encontros anteriores. Nesta atividade, utilizamos os mesmos grupos que os alunos formaram no início da intervenção. A princípio, foram apresentadas as regras: a interação entre eles iria acontecer por meio dos grupos de *Whatsapp*; as tarefas cumpridas seriam pontuadas com 10 pontos acrescidos de mais uma pontuação extra que dependia do tempo gasto para realização da prova; As tarefas deveriam ser entregues no *Whatsapp* ou no *Classroom* criado para a pesquisa; As equipes deveriam manter entre si o respeito e a cordialidade; A equipe vencedora receberia uma premiação simbólica (livro ou chocolate, a critério deles).

Acreditamos que elementos do jogo: regras, pontuação e premiação, tenham colaborado para uma maior motivação entre os alunos, como cita A23 na última questão: "Achei as atividades extremamente empolgantes, consegui compreender bem os conteúdos, como ponto positivo acho que a participação de todos na aula já valeu o esforço, a competição pela gincana foi muito divertida, e achei as aulas da pró muito explicativas, já os pontos negativos... Sinceramente, não vi nenhum, gostei de tudo, até msm as atividades em excesso".

As atividades assíncronas foram as menos prestigiadas, mesmo envolvendo recursos audiovisuais e jogos. Algumas inferências que podem justificar esse resultado são: o fato de terem sido desenvolvidas de forma individual, envolviam o estudo teórico dos conceitos abordados e demandavam mais autonomia do estudante na condução da aprendizagem.

Na última questão, os alunos poderiam avaliar a intervenção de uma forma mais subjetiva, expondo aspectos positivos e negativos. No geral, ficamos satisfeitos com as colocações, pois os poucos aspectos negativos citados, cansaço (cerca de 10%) e dificuldade em algumas questões (cerca de 13%), são pertinentes.

A33: "As atividades são bem difíceis de fazer mais também são bem divertidas."

A1: "As atividades em grupos foram muito boas pois uns estavam ajudando aos outros, e assim todo mundo entende o assunto. Eram "muitas"questões, então acabava que as vezes era cansativo <3."

A17: "Pontos positivos foi que eu aprendi bastante coisa e provavelmente vou está preparado pro ensino médio e o negativo foi que ocupou muito meu tempo."

A16: "Eu simplesmente amei, o ponto negativo é que achei algumas coisas difíceis mais quando fui fazer vi que não era tão difícil assim tirando isso eu amei muito e desenvolvi bastante coisa!!!"

A7: "Foi incrível a semana aprendendo criptografia e função, apesar de ter sido cansativa. Foi ótimo estudar pois era uma área que eu não sabia quase nada e com as aulas e atividades

aprendi muito...".

Percebemos que, apesar de citar os aspectos negativos, os estudantes falam sobre a aquisição de novos conhecimentos e que, de certa forma, o processo foi prazeroso. Em relação ao cansaço, já esperávamos em razão das atividades terem sido planejadas para serem desenvolvidas durante cinco dias consecutivos (de segunda a sexta-feira), mas no decorrer da aplicação, ainda foram utilizadas mais duas aulas de matemática, na segunda-feira seguinte, para conclusão da gincana e aplicação do questionário final. As dificuldades de alguns alunos também fazem parte de todo processo de ensino aprendizagem, uma vez que nem todos aprendem da mesma forma e no ensino remoto, acompanhar essas dificuldades também foi mais desafiador, porém procuramos fazer isso através de feedbacks constantes, usando o *Classroom*, o *Whatsapp* e a reunião dos grupos no *Google Meet*. Além disso, as questões variavam em termos de complexidade, ou seja, haviam aquelas cujas respostas eram mais fáceis, mas existiam outras que requeriam um raciocínio mais elaborado.

Os demais participantes não citaram aspectos negativos e consoante, as respostas mencionadas anteriormente, elogiaram as atividades desenvolvidas, citando que as intervenções auxiliaram na compreensão do conteúdo e que conseguiram se divertir ao longo da semana.

A14: "Eu gostei muito de tudo, pois foram usadas formas divertidas e educativas que ajudou muito na minha compreensão, e ao mesmo tempo, eu me diverti bastante com as brincadeiras e atividades em grupo."

A19: "Foi muito interessante e serviu como um novo conhecimento, um novo aprendizado que eu achei muito interessante ter aprendido, interessante e também importante porém não deu pra se aprofundar mais, oq foi uma pena."

Com a análise de todo o questionário, percebemos que a criptografia pode estimular a aprendizagem matemática, em especial do conceito de função. Mas, respostas como a de A14 e A19, nos deixaram ainda mais animados, porque são alunos que afirmaram não gostar de matemática, no questionário inicial. No caso de A19, assim como outro colega, no início, não queriam participar da pesquisa, todavia conseguimos convencê-los a participar do primeiro encontro como um teste, se não gostassem poderiam desistir. No entanto, participaram de todos os encontros e atividades.

Para concluirmos, segue o mapa mental referente ao capítulo.

Figura 5.19: Mapa Mental - Capítulo V

Fonte: Elaboração da autora.

6 Considerações Finais

Com os estudos e análises que apresentamos ao longo deste trabalho, podemos perceber que a evolução da criptografia está atrelada as necessidades humanas de proteção e segurança de dados. Configura uma ampla área que pode contextualizar o ensino e a aprendizagem de diversos conteúdos matemáticos, conferindo significância, uma vez que observamos claramente a aplicação prática dos conhecimentos abordados. Com essa compreensão, o problema que fundamentou essa pesquisa consistiu em analisar se a criptografia possuía potencial para estimular a aprendizagem do conceito de função no 9º ano do Ensino Fundamental.

Guiados pelos objetivos delineados, refletimos sobre a importância da criptografia, apresentamos o contexto histórico, procedimentos e conhecimentos matemáticos necessários para a compreensão da cifra de César e do Sistema RSA. Também elaboramos e aplicamos algumas atividades que consideramos pertinentes para estimular o interesse pela matemática, além de contribuir para o desenvolvimento de competências e habilidades que favorecem o letramento na área.

A aplicação da intervenção foi um desafio, dado que as atividades foram desenvolvidas de forma remota, devido a pandemia da COVID-19 que assolava o mundo. Foram muitos os obstáculos: problemas de conexão com a internet, necessidade de ampliar o tempo dedicado ao acompanhamento virtual de cada estudante, dificuldades de alguns alunos em resolver tarefas coletivas, entre outros. Todavia, acreditamos que os resultados foram positivos, pois, apesar de não conseguir despertar o interesse de 100% dos participantes para todas as tarefas solicitadas, não houve avaliações negativas sobre o trabalho desenvolvido. Apenas concordaram (a maioria) ou concordaram parcialmente que foi interessante estudar matemática a partir da criptografia e julgaram que os métodos e meios utilizados contribuíram para a aprendizagem do conceito de função. Além disso, registramos que dois estudantes pouco frequentes nas aulas e atividades "normais" se envolveram com o trabalho e participaram das discussões nos grupos. Com isso, podemos afirmar que o objetivo traçado foi alcançado, ou seja, a criptografia tem potencial para estimular a aprendizagem de função.

Contudo, numa possível reaplicação da proposta de forma presencial ou remota, poderíamos fazer alguns ajustes, como a ampliação do tempo para algumas atividades ou diminuir o número de questões, um estímulo maior para a realização das atividades pré

classe e melhorar as orientações para a produção dos vídeos. Uma outra alternativa seria transformar o planejamento num projeto interdisciplinar, pois o tema permite o diálogo entre todas as áreas do conhecimento, podendo trabalhar em cada uma delas:

- Linguagem: leituras, interpretações, produções textuais e elaboração de recursos para auxiliar no processo de encriptação;
- Ciências Humanas: o contexto histórico e geográfico, como os conflitos e descobertas que deram origem aos métodos de criptografia;
- Ciências da natureza: processos físicos e químicos usados na esteganografia;
- Matemática: além do conceito de função, podem ser trabalhados função afim, quadrática e a representação gráfica, uma vez que compõem o currículo do 9º ano.

Inicialmente, essa seria a abordagem do trabalho que foi desenvolvido, mas se tornou inviável, porque as atividades seriam desenvolvidas remotamente e não houve disponibilidade dos colegas de trabalho que se tornariam coparticipantes da pesquisa. Todavia, a abordagem interdisciplinar da criptografia, no processo de ensino e aprendizagem, pode estimular o interesse pelos estudos em todas as áreas e, portanto, é uma temática interessante para uma outra pesquisa.

Gostaríamos de salientar a relevância da metodologia da Sala de Aula Invertida e dos meios virtuais utilizados para alcançarmos resultados positivos. Quase todas as atividades (a única exceção foram as produções de vídeos) projetadas por meio da SAI foram eficientes em seus propósitos, visto que contribuíram para desenvolver nos discentes o interesse pela aprendizagem do conteúdo abordado. Mesmo assim, algumas tiveram uma recepção melhor por parte dos alunos: as atividades em grupos, em especial a que trabalhou com a cifra de César e que serviu de alicerce para introdução do conceito de função.

Destarte, desejamos que os participantes da pesquisa que originou este trabalho continuem a ampliar as habilidades e competências da área, se tornando letrados matematicamente, isto é, capazes de fazer uso dos saberes adquiridos para resolução de problemas em todas as esferas sociais, agindo com protagonismo e responsabilidade.

Nesse ensejo de finalização, precisamos frisar que a escola deve desenvolver atividades que levem o discente a compreender a necessidade de estudarem matemática além dos muros da escola. É preciso que eles vejam os conhecimentos adquiridos na área como importante ferramenta para ler, compreender e intervir na sua realidade, fazendo as transformações necessárias.

Por fim, sabemos que existem várias contribuições de pesquisas envolvendo ciptografia e matemática, entretanto esperamos que esta não seja só mais uma e sim inspiração para que docentes possam, além de usar ou adaptar as atividades propostas, buscar outros temas para tornar o processo de ensino aprendizagem mais dinâmico e significativo.

Referências

ALVES, L. Práticas inventivas na interação com as tecnologias digitais e telemáticas: o caso do gamebook guardiões da floresta. **Revista de Educação Pública**, v. 25, n. 59/2, p. 574–593, 2016. Acesso em 24 set. 2021. 86, 111

ALVES, L. Educação remota: entre a ilusão e a realidade. **Inter Faces Científica, Educação**, v. 8, n. 3, p. 348–365, 2020. Acessado em 24/09/2021. 83, 86, 95

ANDRADE, R. S.; SILVA, F. dos S. Algoritmo de criptograf rsa: análise entre a segurança e velocidade. **Revista Eventos Pedagógicos**, 2012. Acessado em 23/07/2021. 77, 78

ARAUJO, P. F. d. **Aplicações de Criptografia no Ensino Médio**. Dissertação (Mestrado) — Universidade Estadual Federal de Viçosa, 2017. 55, 58

BAHIA. **Documento Curricular Referencial da Bahia para a Educação Infantil e Ensino Fundamental**. Rio de Janeiro: FGV Editora, 2019. 12, 13

BOMFIM, F. de S. **História da matemática e cinema: o caso da criptografia na introdução do ensino da álgebra**. Dissertação (Mestrado) — Universidade Federal de São Paulo, 2017. 62

BRASIL. **Base Nacional Comum Curricular - BNCC**. 2017. Disponível em: <http://portal.mec.gov.br/docman/abril-2018-pdf/85121-bncc-ensino-medio/file>. Acessado em 22/04/2020. 85, 87

CARVALHO, L. R. **O uso de elementos da criptografia como estímulo matemático na sala de aula**. Dissertação (Mestrado) — Universidade Estadual Paulista, 2016. 56, 57, 58, 100

CASTRO, W. C. J. **Criando mensagens secretas na escola básica utilizando a criptografia RSA**. Dissertação (Mestrado) — Universidade Federal da São Carlos, 2015. 60

CIMINO, A. **A História da Quebra dos Códigos Secretos: Dos Antigos Códigos Secretos à Criptografia Quântica**. São Paulo - SP: M. books do Brasil Editora LTDA, 2018. 14, 27, 28, 29, 30, 31, 36, 37, 38

COSTA, C. J. da; FIGUEIREDO, L. M. **Introdução à criptografia**. 2010. Disponível em: <https://portaldaobmep.impa.br/uploads/material_teorico/83bhrw1mjmgwo.pdf>. Acessado em 31/07/2020. 18

COSTA, D. D. **A matemática e os códigos secretos: uma introdução à criptografia**. Dissertação (Mestrado) — Universidade Estadual de Maringá, 2014. 24, 49, 103

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de janeiro: IMPA, 2005. 14, 65, 68, 69, 71, 73

FRANÇA, W. B. de A. **A utilização da criptografia para uma aprendizagem contextualizada e significativa**. Dissertação (Mestrado) — Universidade de Brasília, 2014. 19, 22, 49, 50, 55

GANASSOLI, A. P.; SCHANKOSKI, F. R. **Criptografia e matemática**. Dissertação (Mestrado) — Universidade Federal do Paraná, 2015. 20, 22, 26, 27, 49, 51, 55, 61, 62, 103

GRISELI, R. C. **Criptografia: uma proposta para a educação básica**. Dissertação (Mestrado) — Universidade Federal da Fronteira Sul, 2018. 57, 58

HEFEZ, A. **Aritmética**. Rio de janeiro: SBM, 2005. 14, 65, 67, 69, 70, 71, 72, 73, 80

JANSEN, J. M. **Criptografia: uma abordagem para o Ensino Médio**. Dissertação (Mestrado) — Universidade Federal do Maranhão, 2016. 49, 50, 55, 60

LITOLDO, B. F. **As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração de ideias associadas a função afim**. Dissertação (Mestrado) — Universidade Estadual Paulista, 2016. 46, 47

LOUREIRO, F. O. **Tópicos de criptografia para o ensino médio**. Dissertação (Mestrado) — Universidade Estadual do Norte Fluminense Darcy Ribeiro, 2014. 55, 56

LUDKE, M.; ANDRE, M. E. D. A. **Pesquisa em educação: abordagens qualitativas**. 2. ed. São Paulo: EPU, 2015. 82

MACHADO, A. P. **Teoria dos números e criptografia RSA: uma proposta de ensino para alunos de matemática olímpica**. Dissertação (Mestrado) — Universidade Federal de Santa Maria, 2018. 59, 63

MARCONI, M. A.; LAKATOS, E. M. **Metodologia científica**. 5. ed. São Paulo: Atlas, 2007. 82

MATSUMOTO, M. S. **Despertando o interesse do aluno pela matemática com a criptografia**. Dissertação (Mestrado) — Universidade Federal da Grande Dourados, 2014. 56, 60

MITANI, M. et al. **The manga guide to cryptography**. Tóquio: Ohmsha, 2007. 18, 19, 20, 33, 34, 35, 97

MOURA, M. de O. **A criptografia motivando o estudo das funções no 9º ano do ensino fundamental**. Dissertação (Mestrado) — Universidade Federal do Tocantins, 2019. 47, 48

OLIVEIRA, R. D. de. **A utilização de mensagens criptografadas no ensino de matrizes**. Dissertação (Mestrado) — Universidade Federal de São Carlos, 2013. 53, 54, 56

PINHEIRO, M. S. **Criptografia RSA, números primos e uma sugestão de aplicação no Ensino Médio**. Dissertação (Mestrado) — Universidade Estadual do Ceará, 2018. 59

RODRIGUES, J. de M. **Criptografia e conteúdos de matemática no ensino fundamental**. Dissertação (Mestrado) — Universidade Federal de São Carlos, 2013. 46, 103, 106

ROSSETO, C. K. **Criptografia como recurso didático: uma proposta metodológica aos professores de matemática**. Dissertação (Mestrado) — Universidade Estadual Paulista, 2018. 49, 51

SANT'ANA, G. Proposta metodológica na pós-graduação com o uso da sala de aula invertida. In: SANTOS, P. V. (Ed.). **Metodologias ativas: modismo ou inovação?** Quirinópolis, GO: Editora IGM, 2021. p. 225–240. 85, 86, 95

SANTOS, D. S. dos. **Uso da criptografia como motivação para o ensino básico de matemática**. Dissertação (Mestrado) — Universidade Federal de Sergipe, 2015. 49, 51, 55

SANTOS, J. L. dos. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes motivadoras para atividades de matemática básica**. Dissertação (Mestrado) — Universidade Federal da Bahia, 2013. 19, 23, 25, 27, 49, 50, 51, 55

SANTOS, S. M. da S. **Aprendizagem das funções polinomiais do 1º e 2º grau mediada pelo jogo "Trilha Matemática Criptografa": uma abordagem sob a perspectiva Vygotskyana**. Dissertação (Mestrado) — Universidade Tecnológica do Paraná - Londrina, 2019. 48, 49, 97

SCHUCHMANN, A. Z.; SCHNORRENBERGER, B. L.; CHIQUETTI, M. E.; GAIKI, R. S.; MAEYAMA, B. W. R. an M. A. Isolamento social vertical x isolamento social horizontal: os dilemas sanitários e sociais no enfrentamento da pandemia de covid-19. **Brazilian Journal of Healt**, v. 3, n. 2, p. 3556–3576, 2020. Acessado em 09/10/2021. 82

SCHURMANN. **Criptografia matricial aplicada ao ensino médio**. Dissertação (Mestrado) — Universidade Estadual de Londrina, 2013. 52, 53, 54

SHOKRANIAN, S. **Criptografia para iniciantes**. Rio de janeiro: Editora Ciência Moderna Ltda., 2012. 14, 65, 69, 70, 71, 72, 73, 74, 77

SILVA, I. N. da. **Criptografia na Educação Básica: das escritas ocultas ao código RSA**. Dissertação (Mestrado) — Pontifícia Universidade Católica do Rio de Janeiro, 2016. 58

SILVA, R. E. G. **Criptografia RSA: da teoria a aplicação em sala de aula**. Dissertação (Mestrado) — Universidade de São Paulo, 2019. 55

SILVEIRA JÚNIOR, C. R. da. **Sala de aula invertida: por onde começar?** Goiás: Instituto Federal de Goiás, 2020. 88, 89, 95, 131, 137, 150, 154, 161

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2020. 14, 29, 30, 31, 32, 33, 34, 36, 38, 39

Apêndice A
Plano de Aula 1 e Atividades

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Tabela A.1: Plano de Aula 1

Plano de Aula 1				
Duração	5h			
Objetivos	Resolver problemas envolvendo equação do 1º grau. Conhecer a história da criptografia, compreendendo alguns conceitos básicos.			
Conteúdo	Equação do 1º grau e História da Criptografia.			
Organização dos Espaços				
Espaços	Atividades	Duração	Papel do Aluno	Papel do Professor
Encontro no *Google Meet*.	Conversa inicial.	20 min.	Participar da conversa, esclarecendo possíveis dúvidas.	Conduzir a conversa inicial, expondo os objetivos do projeto de pesquisa, papel dos alunos, papel da professora e atividades que serão desenvolvidas.
Encontro no *Google Meet*.	Questionário Inicial para verificar os conhecimentos prévios dos alunos sobre criptografia e importância da matemática.	20 min.	Responder ao questionário:<https://forms.gle/rUcFZ6XfkcJ6M5Qm8>	Elaborar o questionário no *Google Forms* e disponibilizá-los no *Classroom*, indicando o momento para os alunos responderem.

Encontro no *Google Meet*.	Divisão das turmas em grupos.	5 min.	Formar grupos de acordo com a afinidade.	Mediar o processo de formação dos grupos com 5 ou 6 alunos e definir um líder em cada um deles.
Encontro no *Google Meet*.	Mensagem Secreta com *QR Codes* (resolução de problemas envolvendo equação do 1º grau).	60 min.	Os líderes deverão criar uma reunião no *Google Meet* para que seu grupo possa interagir, fazer a leitura dos *QR Codes* usando aplicativo ou a câmera do celular, discutir e solucionar os problemas do 1º grau.	Elaborar os problemas envolvendo equação do 1º grau e transformá-los em blocos usando o gerador de *QR Codes*. Disponibilizar a atividade no *Classroom*. Fazer as intervenções necessárias para auxiliar os estudantes na atividade.
Encontro pelo *Google Meet*.	Conversa sobre a atividade anterior e orientação para as atividades que deverão fazer em casa.	20 min.	Participar da conversa, expondo se encontram dificuldades e os pontos positivos e negativos da atividade.	Mediar a conversa, fazer questionamentos e orientar as atividades que deverão fazer em casa.

Casa.	História e Fundamentos da Criptografia.	40 min.	Leitura do prólogo do Mangá: (Masaaki Mitani et al. - The Manga Guide to Cryptography-No Starch Press, 2018), o qual foi traduzido para português. Assistir a vídeo aula: <https://www.youtube.com/watch?v=V2V9v089eng>, fazendo as anotações necessárias. Traduzir o prólogo do Mangá: (Masaaki Mitani et al. - The Manga Guide to Cryptography-No Starch Press, 2018) e disponibilizá-lo no *Classroom* para leitura.	Disponibilizar o Mangá citado na íntegra caso os alunos tenham interesse em ler. Gravar a vídeo aula sobre a História da Criptografia, usando o *Powerpoint*, carregar no *Youtube* e disponibilizar no *Classroom* para que os alunos possam assistir.
Casa.	Filme: O Jogo da Imitação.	125 min.	Assistir ao filme, procurando relacionar criptografia, matemática e a segunda guerra mundial.	Disponibilizar o *link* do filme no *Classroom* para que os alunos possam assistir e responder às questões solicitadas.
Casa.	Jogo Perseguição no labirinto sobre a história da criptografia.	10min.	Participar do jogo: <https://wordwall.net/play/21137/642/225> com base no vídeo que assistiram.	Elaborar o jogo no *Wordwall* e disponibilizar no *Classroom* para os alunos realizarem. Dar *feedback* aos alunos e solicitar para a aula seguinte o *kit* de encriptação entregue na reunião.
Avaliação	No *Classroom*, será atribuída uma nota de 0 a 10, em cada atividade, tendo em vista o compromisso, a autonomia, o desempenho e a interação entre os estudantes e entre os estudantes e a professora.			

Fonte: Elaborado pela pesquisadora com base em Silveira Júnior (2020).

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Prezado(a) estudante, esta atividade tem por finalidade revisar o conteúdo de Equação do 1º grau e iniciar as discussões sobre criptografia. Ela compõe a pesquisa intitulada: "A Criptografia como Estímulo à Aprendizagem Matemática" promovida pela professora Ana Lourdes Moreno Rodrigues Silva, aluna do PROFMAT na Universidade do Sudoeste da Bahia - UESB, sob orientação do professor Fernando dos Santos Silva.

Obrigada por colaborar com esse trabalho!

MENSAGEM SECRETA - EQUAÇÃO DO 1º GRAU

O alfabeto da tabela abaixo foi pré-codificado, ou seja, cada letra está relacionada com um número. Observe-o e descubra a mensagem secreta representada pelos *QR Codes*! Você deverá utilizar um leitor de *QR Codes*, resolver o problema contido em cada um deles e com base no alfabeto descobrir a mensagem (por exemplo, se o resultado do problema for 10, então ele representa a letra J.

Tabela A.2: Pré-codificação

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Elaboração da autora.

MENSAGEM:

Figura A.1: *QR Codes* - Mensagem Secreta

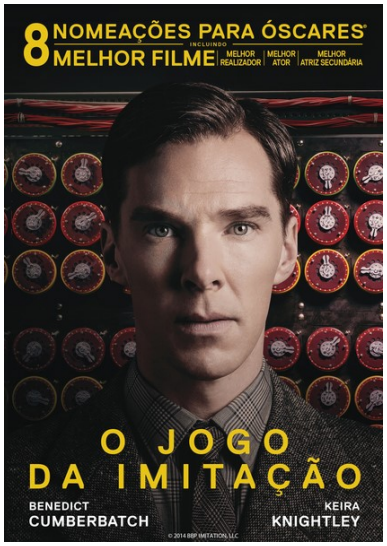
Fonte: Elaboração da autora.

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Prezado(a) estudante, esta atividade tem por finalidade refletir sobre o filme: "O Jogo da Imitação", procurando estabelecer relação entre criptografia, matemática e a Segunda Guerra Mundial. Ela compõe a pesquisa intitulada: "A Criptografia como Estímulo à Aprendizagem Matemática" promovida pela professora Ana Lourdes Moreno Rodrigues Silva, aluna do PROFMAT na Universidade do Sudoeste da Bahia - UESB, sob orientação do professor Fernando dos Santos Silva.

Obrigada por colaborar com esse trabalho!

ATIVIDADE SOBRE O FILME: O JOGO DA IMITAÇÃO



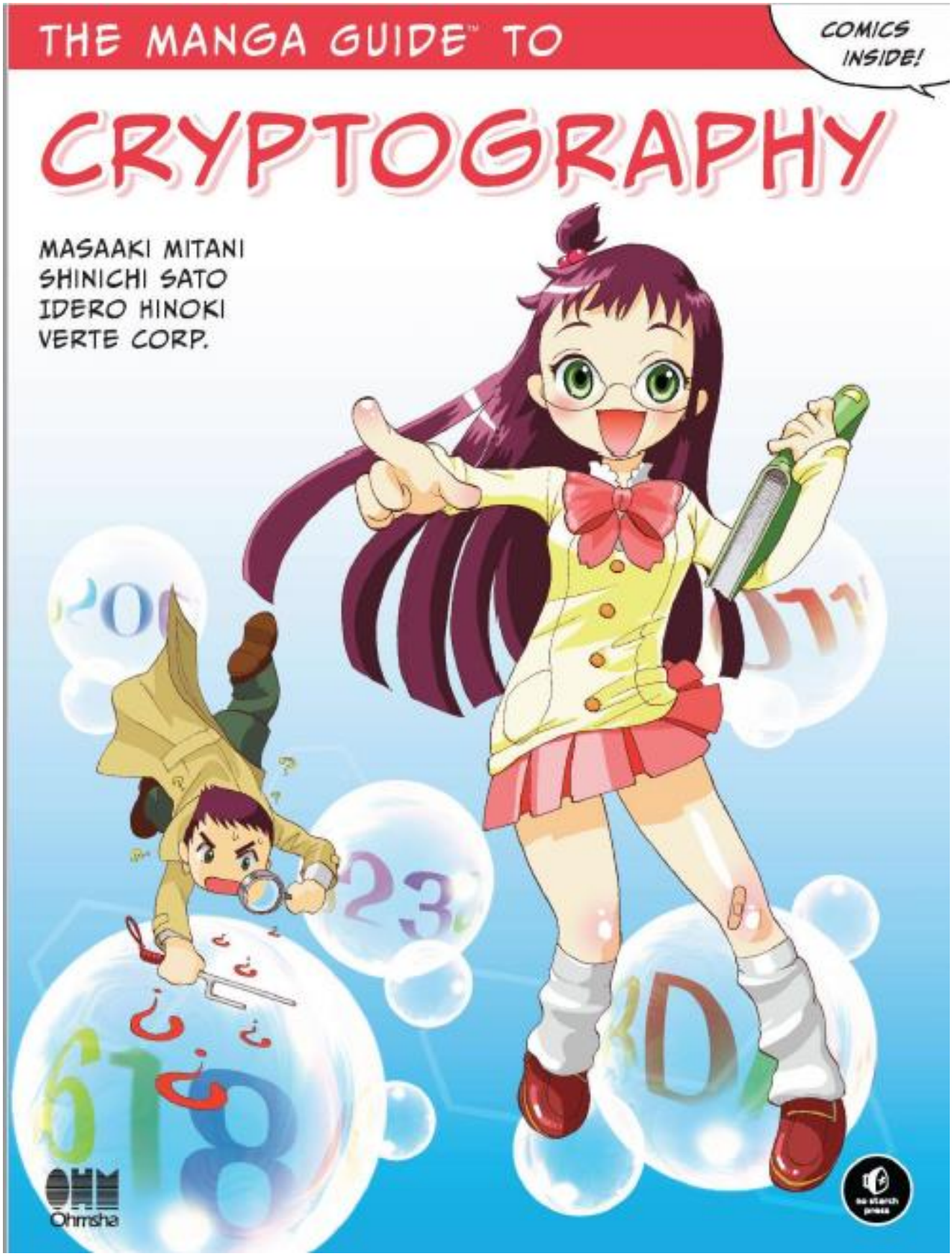
O filme: O Jogo da Imitação retrata o contexto da Segunda Guerra Mundial, no qual o governo britânico formou uma equipe com o objetivo de quebrar o famoso código que os Alemães usavam na troca de informações, o Enigma. Um dos integrantes era Alan Turing, um gênio da matemática com 27 anos de idade. Apesar de sua dificuldade em relacionar-se com as pessoas, teve que trabalhar em equipe e elaborou um projeto para a construção de uma máquina que pudesse decifrar o Enigma.

Embarque nessa história, assistindo ao filme no link: <https://www.youtube.com/watch?v=Q2xrQ5U0Tbo> e responda aos seguintes questionamentos:

1. Qual a parte do filme você achou mais interessante?
2. As máquinas de Turing têm alguma relação com os computadores que utilizamos?
3. Com base no filme, que relação você pode estabelecer entre a criptografia, o trabalho dos matemáticos e a Segunda Guerra Mundial?
4. Alan Turing é considerado um gênio injustiçado pela sociedade. Comente sobre isso.

Capa do Mangá: The Manga Guide To Cryptography

O Guia de Mangá Para Criptografia



Apêndice B
Plano de Aula 2 e Atividades

Universidade Estadual do Sudoeste da Bahia - UESB
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Tabela B.1: Plano de Aula 2

Plano de Aula 2				
Duração	3h			
Objetivos	Compreender a história da criptografia, percebendo a importância da matemática para sua evolução. Cifrar e decifrar mensagens usando a código de César. Entender o conceito de função, identificando a lei de formação e calculando f(x). Relacionar a Cifra de César com uma função afim.			
Conteúdo	História da Criptografia; Cifra de César; Função: conceito, lei de formação e valor.			
Organização dos Espaços				
Espaços	Atividades	Duração	Papel do Aluno	Papel do Professor
Encontro pelo *google meet*.	Conversa sobre criptografia e a Cifra de César.	30 min.	Participar da conversa com base no vídeo e no filme que assistiram.	Mediar as participações dos alunos por meio de questionamentos.
Encontro pelo *Google Meet*.	Manuseio do *kit* de encriptação.	20 min.	Manusear o *kit* de encriptação, seguindo as orientações da professora.	Orientar o uso do *kit* de encriptação que será utilizado na próxima atividade, solicitando que seja feita a codificação e decodificação de algumas palavras.

Encontro pelo *Google Meet*.	Elaboração e descoberta de mensagens secretas usando a Cifra de César.	60 min.	Os líderes dos grupos, formados no encontro anterior, deverão enviar o *link* da reunião pelo *Google Meet* para que possam interagir e resolver a atividade envolvendo a cifragem e decifragem de mensagens usando o código de César.	Mediar as discussões nos grupos, estimulando a participação de todos.
Encontro pelo *Google Meet*.	Conversa sobre a atividade anterior e orientação para as atividades que deverão fazer em casa.	20 min.	Participar da conversa, expondo se encontram dificuldades e os pontos positivos e negativos da atividade.	Mediar a conversa, fazer questionamentos e orientar as atividades que deverão fazer em casa.
Casa.	Construção da ideia de Função usando a Cifra de César.	40 min.	Assistir a vídeo aula: <https://www.youtube.com/watch?v=cI08HSYIzwM> e estudar o texto sobre funções, fazendo as anotações necessárias.	Gravar a vídeo aula relacionando a Cifra de César, a ideia de função, lei de formação e o valor de $f(x)$ e disponibilizar no *Classroom*, juntamente com o texto utilizado como base, para que os alunos possam assistir.
Casa.	Jogando com as funções.	10min.	Participar do jogo: <https://wordwall.net/play/21138/567/227> envolvendo funções e a cifra de César.	Elaborar um jogo de combinação no *Wordwall* envolvendo função e a cifra de César e disponibilizar no *Classroom* para que os alunos possam jogar.
Avaliação	No *Classroom*, será atribuída uma nota de 0 a 10, em cada atividade, tendo em vista o compromisso, a autonomia, o desempenho e a interação entre os estudantes e entre os estudantes e a professora.			

Fonte: Elaborado pela pesquisadora com base em Silveira Júnior (2020).

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

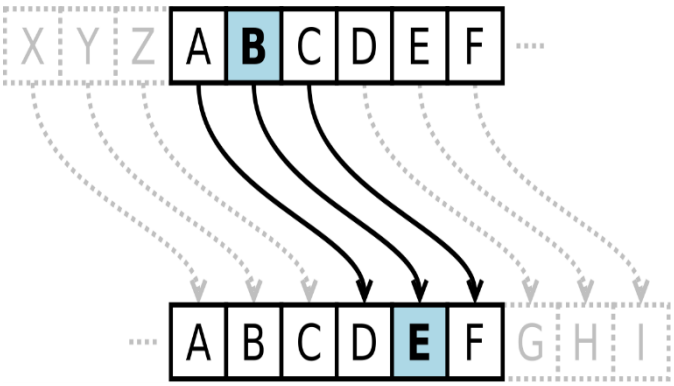
Prezado(a) estudante, esta atividade tem por objetivo compreender a cifra de César utilizando um kit com dois copos descartáveis para auxiliar no processo de cifragem e decifragem de mensagens. A atividade faz parte da pesquisa intitulada: "A Criptografia como Estímulo à Aprendizagem Matemática" promovida pela professora Ana Lourdes Moreno Rodrigues Silva, aluna do PROFMAT na Universidade do Sudoeste da Bahia - UESB, sob orientação do professor Fernando dos Santos Silva.

Obrigada por colaborar com esse trabalho!

ATIVIDADES SOBRE A CIFRA DE CÉSAR

O código de César foi um dos primeiros sistemas de criptografia. Recebeu esse nome porque foi criado pelo general Júlio César para encriptar comunicações governamentais. Para cifrar um texto, César alterava as letras, deslocando-as em três posições. Dessa forma, o A era substituído pelo D, o B por E e assim por diante. Esse deslocamento corresponde a chave do código que, nesse caso, é igual a 03. Atualmente, qualquer cifra baseada na substituição cíclica do alfabeto pode ser considerada como código de César.

Figura B.1: Deslocamento das Letras de Acordo com a Cifra de César



Fonte: <https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar>.

Vamos entender melhor esse sistema, resolvendo as questões abaixo.
Você deverá utilizar o kit entregue na reunião com os pais.
1- Usando o código de César juntamente com o kit, cifre a mensagem:

Figura B.2: Kit de Encriptação

Fonte: Elaboração da autora.

A		V	I	D	A		E		B	E	L	A

2- Usando esse mesmo código, decifre a seguinte frase de Carl Friedrich Gauss:

D		P	D	W	H	P	D	W	L	F	D		H		D

U	D	L	Q	K	D		G	D	V		F	L	H	Q	F	L	D	V

3- Você pode deslocar as letras com um número diferente de três, ou seja, com outra chave. Faça um deslocamento diferente e cifre seu nome.

4- As letras também podem ser trocadas por números, conforme a tabela:

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

Para criptografar uma mensagem usando a chave igual a 3, somamos o número correspondente à letra com o 3. Como exemplo, vamos criptografar a palavra PAZ.

$P = 15 + 3 = 18$

$A = 0 + 3 = 03$

$Z = 25 + 3 = 28$

Mas, na tabela não há nenhuma letra que corresponda ao número 28, então, o que faremos?

Quando a soma for superior a 25, a letra codificada deverá ser associada ao resto da divisão, do valor encontrado, por 26. Assim, se queremos codificar a letra Z, fazemos $25 + 3 = 28$, em seguida, dividimos 28 por 26 e consideramos o resto 02.

Logo, 18-03-02 é a palavra PAZ cifrada com a chave 3.

Percebam que, nesse contexto, faz sentido escrevermos:

$25 + 3 = 2$ $(28 : 26$, deixa resto $2)$

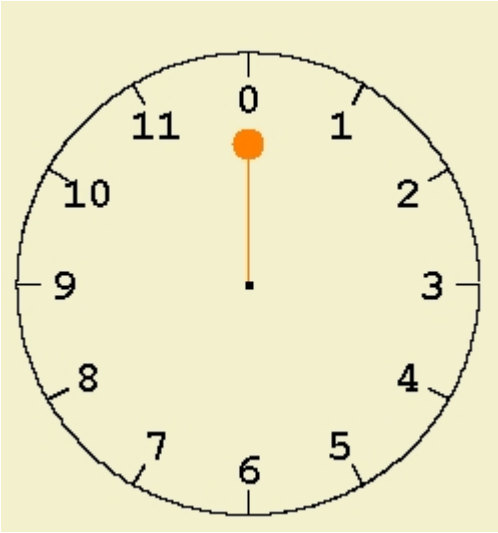
$16 + 10 = 0$ $(26 : 26$, deixa resto $0)$

$21 + 9 = 4$ $(30 : 26$ deixa resto $4)$.

Veja que estamos contando conjuntos de 26 letras e registrando o resto, quando o resultado da operação que estamos efetuando é superior a 25.

Vamos entender isso melhor utilizando um relógio de ponteiro, conforme a imagem:

Figura B.3: Relógio de Ponteiros



Fonte: <https://www.atractor.pt/mat/alg_controlo/mod_texto.html>.

Como o relógio marca o tempo infinitamente, era de se esperar que ele atingisse números muito grandes, pois os ponteiros não param. Mas, essa máquina é indiferente a quantidade de vezes que passa pelo 12 (aqui representado pelo zero), indicando apenas as horas que seguem nas últimas 12 horas. Observe que esse relógio possui 12 divisões e cada uma delas corresponde a uma hora. Como um dia tem 24 horas, ele dará duas voltas completas nesse

período e podemos fazer a seguinte correspondência: 12=0, 13=1, 14=2, . . . , 23=11. Você concorda com essas igualdades?

Nesse caso, estamos contando conjuntos de 12 horas, iniciando no zero e quando o valor é maior que 11, efetua-se uma divisão por 12 em que o resto é a hora correspondente. Assim, 17h corresponde a 5h, pois, 17 : 12 deixa resto 5.

Fora de contexto essas igualdades geram ambiguidades, pois na aritmética usual não temos, por exemplo, $5h + 8h = 1h$. Por isso, existe a aritmética modular, também chamada aritmética do relógio, na qual ao atingir um certo valor, chamado módulo, os números "voltam ao início".

Nesse sistema, a igualdade $5 + 8 = 1$ é escrita como $13 \equiv 1 \pmod{12}$ e lemos; "treze é congruente com um módulo doze". Nesta expressão, o 13 é o resultado da operação $5 + 8$ na aritmética usual, o 1 resto da divisão de 13 por 12 e (mod 12) indica uma contagem em conjuntos de 12.

Para entender melhor a aritmética do relógio, acesse a aula: "Aritmética - Aula 42 -7+6=1. Aritmética modular do Programa de Iniciação Científca da OBMEP no link: <https://www.youtube.com/channel/UC5azyx8w7Y5qzASuxDSseOw,acessoem01/09/2021>.

Vamos voltar para a Cifra de César e aplicar o que acabamos de aprender?

Veja que as operações: $25 + 3 = 2$ (28 : 26 deixa resto 2) , $16 + 10 = 0$ (26 : 26 deixa resto 0), $21 + 9 = 4$ (30 : 26 deixa resto 4), para não gerar ambiguidade são escritas, respectivamente, da seguinte forma:

$28 \equiv 2 \pmod{26}$, $26 \equiv 0 \pmod{26}$ e $30 \equiv 4 \pmod{26}$.

Agora é com você! Com base nos conhecimentos acima, responda os itens a seguir:

a) Utilize a chave 5 para codificar a seguinte mensagem:

A		U	N	I	A	O		F	A	Z		A		F	O	R	C	A

B) Sabendo que a mensagem abaixo foi codificada utilizando a chave 10, descubra seu conteúdo.

13	14	04	02		10	19	04	13	10		00	04	14	22
12	14	13	24	22	10	13	01	04	16	10				

c) Luiza codificou uma palavra de 5 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 1502152411. Ajude Luiza colocando os tracinhos que ela esqueceu e depois escreva a chave que ela codificou.

d) Usando outra chave, Lucas somou os números que representam as letras A, B e C obtendo 48. Que chave Lucas usou?

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Prezado(a) estudante, o objetivo desse texto é apresentar o conceito de função por meio da criptografia (Cifra de César). Ele faz parte da pesquisa intitulada: "A Criptografia como Estímulo à Aprendizagem Matemática" promovida pela professora Ana Lourdes Moreno Rodrigues Silva, aluna do PROFMAT na Universidade do Sudoeste da Bahia - UESB, sob orientação do professor Fernando dos Santos Silva.

Obrigada por colaborar com esse trabalho!

Entendendo Função por meio da Criptografia

Na criptografia, um texto normal torna-se incompreensível por meio de uma chave. Vamos usar como exemplo a Cifra de César. Conforme vimos em aula, inicialmente temos uma tabela, na qual cada letra do alfabeto corresponde a um número.

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

Ao criptografar a palavra MATEMÁTICA com a chave 6, obtemos: 18-06-25-10-18-06-25-14-08-06, conforme mostra a tabela abaixo:

TEXTO NORMAL	TEXTO CRIPTOGRAFADO
M=12	12+6=18
A=00	00+6=06
T=19	19+6=25
E=04	04+6=10
I=08	08+6=14
C=02	02+6=08

Observe que cada valor do texto normal corresponde a um único valor no texto criptografado. Assim, podemos dizer que o texto cifrado (y) é dado em função do texto normal (x).

Na matemática, essa correspondência é chamada de função e pode ser definida como uma relação entre duas grandezas (x e y), tal que para cada valor de x, existe um único valor de y.

Essa relação pode ser expressa por meio de uma sentença chamada lei de formação da função ou lei da função. No exemplo, a lei de formação será:

y=x+6, que também pode ser denotada por $f(x) = x + 6$.

Numa função, as grandezas envolvidas chamam-se variáveis, sendo y a variável dependente e x a variável independente.

Considerando a função dada $f(x) = x + 6$, para calcular seu valor, basta substituir x na lei de formação por um número dado. Veja:

$x = 1$, $f(1) = 1 + 6 = 7$ x=23, $f(23) = 23 + 6 = 29$

Para você entender melhor a ideia de função, podemos compará-la com uma máquina, na qual entram valores x e saem valores $y(f(x))$.

Essa transformação é definida pela lei da função.

Figura B.4: Função - Máquina

Fonte: <https://blog.maxieduca.com.br/tipos-funcao-plinomial/>.

Veja outro exemplo:

A torneira da pia do banheiro de Bia está com defeito e a quantidade de água desperdiçada (y) é função do tempo (x), conforme a tabela:

Quantidade de Água Desperdiçada por uma Torneira com Defeito				
$x(min)$	0	1	2,5	4
$y(ml)$	0	13	32,5	52

Qual a lei de formação da função?

Qual a variável dependente? E a variável independente?

Quantos ml de água serão desperdiçados em $x = 7min$?

Função Injetora, Sobrejetora e Bijetora

No exemplo, envolvendo a Cifra de César, considere:

$A = \{0, 2, 4, 8, 12, 19\}$ e

$B = \{6, 8, 10, 14, 18, 25\}$.

Veja que A e B são conjuntos não vazios e todo $x \in A$ está associado a um único $y \in B$ pela lei $y = f(x)$, tal que $y = x + 6$.

O conjunto dos valores da variável $x \in A$ é chamado de domínio (D) da função f (Pode conter infinitos elementos, mas para ser função, todos eles devem ter um único correspondente em B).

O conjunto B é chamado de contradomínio (CD) da função f (Também pode conter infinitos elementos, mas, dentre eles, pode não haver correspondente em A).

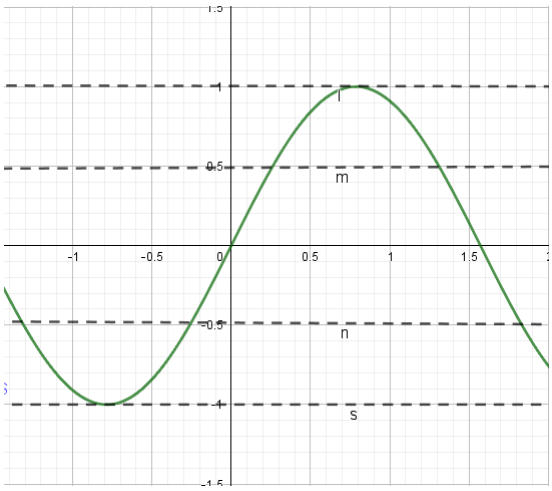
O conjunto formado pelos elementos y de B tais que $y = f(x)$, é chamado de imagem (Im) da função f. Temos que $Im \subset B$, ou seja, são todos os elementos de B que estão relacionados com elementos do domínio. Portanto, no nosso exemplo,

$Im = \{6, 8, 10, 14, 18, 25\}$.

Veja que $CD(f) = Im(f) = B$. Quando isso ocorre, dizemos que a função é sobrejetora.

Na figura B.5, temos o gráfico de uma função sobrejetora. Observe que a reta horizontal traçada no seu contradomínio o intersecta pelo menos uma vez.

Figura B.5: Gráfico de uma Função Sobrejetora



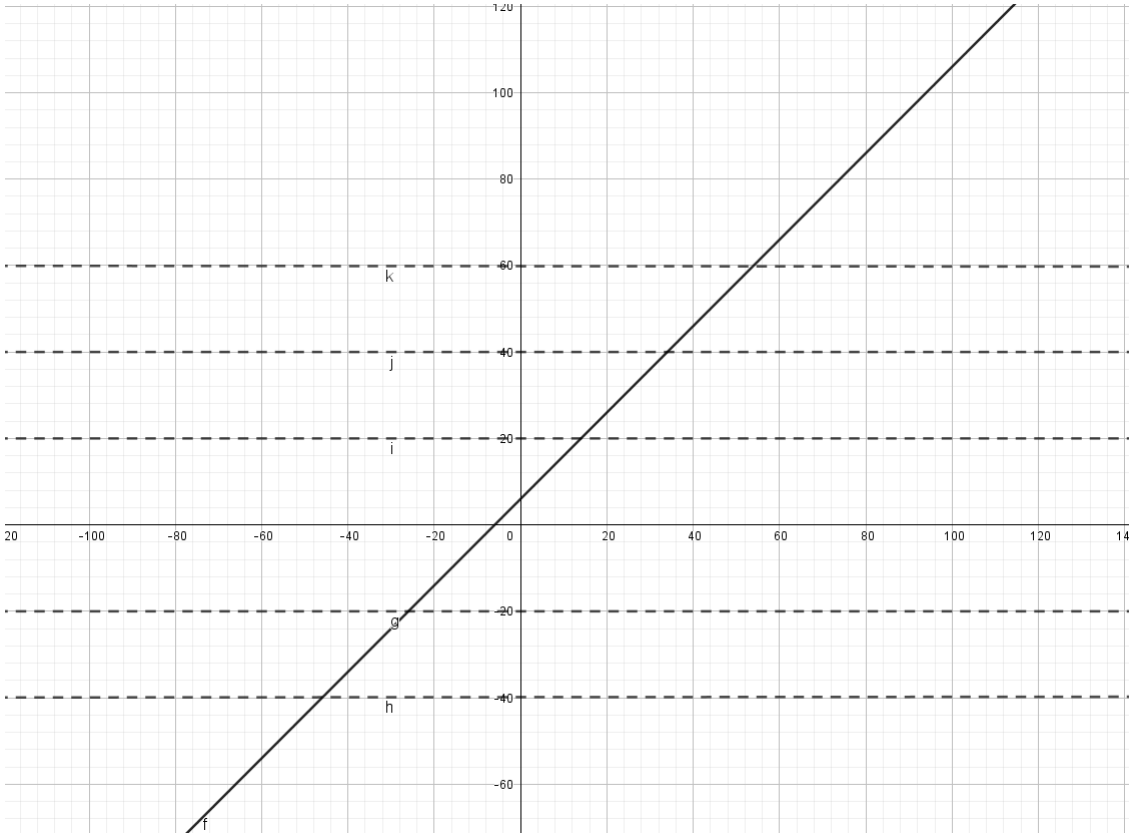
Fonte: Elaboração da autora.

A função $f(x) = x + 6$ também é injetora, pois qualquer que seja $x_1 \in A$ e $x_2 \in A$, temos que $x_1 \neq x_2$, então $f(x_1) \neq f(x_2)$. Isso significa que elementos distintos do domínio, possuem imagens também distintas.

No gráfico de uma função injetora, a reta horizontal traçada no seu contradomínio só pode intersectá-lo em um único ponto, conforme mostra a figura B.6:

A função dada também pode ser classificada como bijetora, visto que é ao mesmo tempo injetora e sobrejetora.

Figura B.6: Gráfico de uma Função Injetora



Fonte: Elaboração da autora.

Agora, observe o que acontece quando ciframos as letras da palavra COMPANHEIRO, usando a transformação: $f(x) \equiv 6x + 1 \pmod{26}$.

TEXTO NORMAL	TEXTO CRIPTOGRAFADO
A	$0 \times 6 + 1 = 01$
C	$2 \times 6 + 1 = 13$
E	$4 \times 6 + 1 = 25$
H	$7 \times 6 + 1 = 43$, $43 : 26$ deixa resto 17
I	$8 \times 6 + 1 = 49$, $49 : 26$ deixa resto 23
M	$12 \times 6 + 1 = 73$, $3 : 26$ deixa resto 21
N	$13 \times 6 + 1 = 79$, $79 : 26$ deixa resto 01
O	$14 \times 6 + 1 = 85$, $85 : 26$ deixa resto 01
P	$15 \times 6 + 1 = 91$, $91 : 26$ deixa resto 13
R	$17 \times 6 + 1 = 103$, $103 : 26$ deixa resto 25

Veja que as letras A e N têm uma mesma imagem, assim como as letras C e P. Logo, essa transformação não é injetora, pois $f(0) \equiv f(13)$ e $f(2) \equiv f(15)$. Consequentemente também não é bijetora.

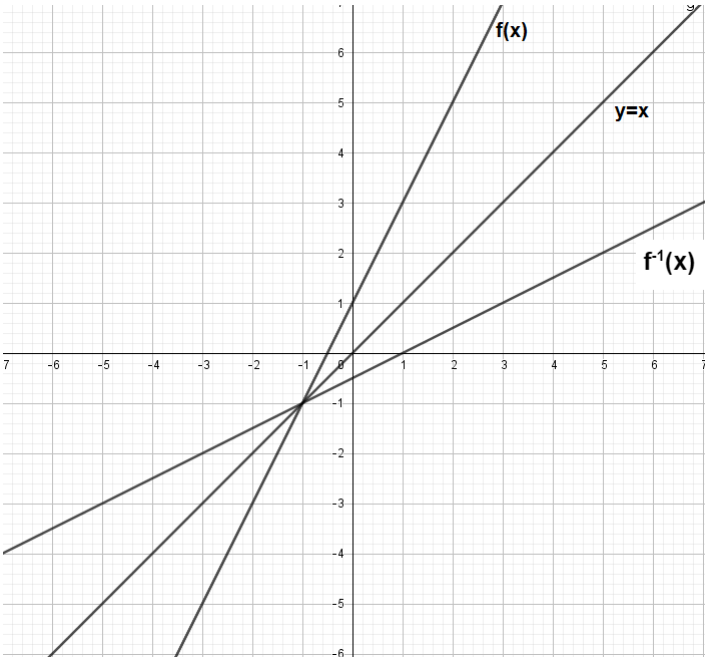
Na criptografia, não poderíamos utilizar essa função para cifrar um texto, visto que ao fazer o processo inverso (descriptografar), geraria ambiguidade, pois um mesmo valor corresponderia a duas letras.

Na verdade, ao decifrar uma mensagem, estamos calculando a função inversa. Assim, no primeiro exemplo, para decifrar a mensagem: **18-06-25-10-18-06-25-14-08-06** que foi codificada com a função $f(x) = x + 6$, encontramos a inversa desta função, utilizando os seguintes procedimentos:

1. $f(x) = x + 6$ (Função dada).
2. $y = x + 6$ (Fazemos $f(x) = y$).
3. $x = y + 6$ (trocamos x por y e y por x).
4. $y = x - 6$ (Isolamos o y).
5. $f^{-1}(x) = x - 6$ (Notação da função inversa).

Atenção! Uma função f só admite inversa se f for bijetora;
O domínio da função f é o conjunto imagem de sua inversa.
O conjunto imagem de f é o domínio de sua inversa.
Os gráficos de f e f^{-1} são simétricos em relação à bissetriz dos quadrantes ímpares, conforme figura B.7.

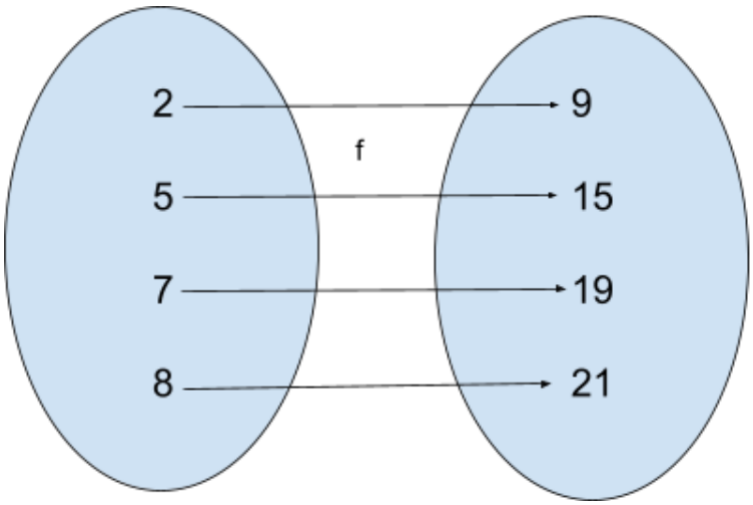
Figura B.7: Gráfico de uma Função e sua Inversa



Fonte: Elaboração da autora.

Vamos ver se você compreendeu?
Considere $A = \{2, 5, 7, 8\}$ e $B = \{9, 15, 19, 21\}$ e a função $f : A \to B$, tal que $f(x) = 2x + 5$.
Fazendo a representação dessa relação por meio do diagrama de *venn*, obtemos:

Figura B.8: Representação da Função $f(x) = 2x+5$ por meio de Diagrama



Fonte: Elaboração da autora.

Temos:
$D(f) = \{2, 5, 7, 8\}$
$CD(f) = \{9, 15, 19, 21\}$
$Im(f) = \{9, 15, 19, 21\}$
Essa função é bijetora, logo, admite inversa. Então,
$f(x) = 2x + 5$
$y = 2x + 5$
$x = 2y + 5$
$y = \frac{x-5}{2}$
$f^{-1}(x) = \frac{x-5}{2}$.

Apêndice C
Plano de Aula 3 e Atividades

Universidade Estadual do Sudoeste da Bahia - UESB
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Tabela C.1: Plano de Aula 3

Plano de Aula 3				
Duração	3h			
Objetivos	Usar funções afim para criptografar e descriptografar mensagens. Resolver problemas envolvendo função. Entender como funciona o RSA.			
Conteúdo	Função; Criptografia RSA.			
Organização dos Espaços				
Espaços	Atividades	Duração	Papel do Aluno	Papel do Professor
Encontro pelo *Google Meet*.	Conversa sobre função, função bijetora e função inversa.	50 min.	Participar da conversa com base no vídeo que assistiram.	Mediar as participações dos alunos por meio de questionamentos.
Encontro pelo *Google Meet*.	Usando Funções Para Cifrar e Decifrar Mensagens.	60 min.	Em grupos, reunidos pelo *Google Meet*, deverão resolver a atividade envolvendo a cifragem e decifragem de mensagens usando função.	Mediar as discussões estimulando a participação de todos.
Encontro pelo *Google Meet*.	Conversa sobre a atividade anterior e orientação para as atividades que deverão fazer em casa.	30 min.	Participar da conversa, expondo se encontram dificuldades e os pontos positivos e negativos da atividade.	Mediar a conversa, fazer questionamentos e orientar as atividades que deverão fazer em casa.

Casa.	Entendendo o RSA.	30 min.	Assistir aos vídeos: <youtu.be/3jR62Mew8X4> e <youtu.be/GAR1Ur_2IGk> fazendo as anotações necessárias.	Disponibilizar o *link* de uma vídeo aula do *Youtube* no *Classroom* para que os alunos possam assistir.
Casa.	Jogo RSA.	10min.	Participar do jogo: <https://wordwall.net/play/21139/212/458> envolvendo a criptografia RSA.	Elaborar um jogo (verdadeiro ou falso) no *Wordwall* envolvendo o RSA e disponibilizar no *Classroom* para que os alunos possam jogar.
Avaliação	No *Classroom*, será atribuída uma nota de 0 a 10, em cada atividade, tendo em vista o compromisso, a autonomia, o desempenho e a interação entre os estudantes e entre os estudantes e a professora.			

Fonte: Elaborado pela pesquisadora com base em Silveira Júnior (2020).

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Prezado(a) estudante, essa atividade tem como objetivo compreender o conceito de função por meio da criptografia (Cifra de César). Ela faz parte da pesquisa intitulada: "A Criptografia como Estímulo à Aprendizagem Matemática" promovida pela professora Ana Lourdes Moreno Rodrigues Silva, aluna do PROFMAT na Universidade do Sudoeste da Bahia - UESB, sob orientação do professor Fernando dos Santos Silva.

Obrigada por colaborar com esse trabalho!

ATIVIDADE - USANDO FUNÇÕES PARA CIFRAR E DECIFRAR MENSAGENS

Para responder as questões que seguem, você deverá utilizar a seguinte tabela:

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

1- Clara deseja enviar uma mensagem codificada para Bia. Sabendo que o conteúdo da mensagem será: ENCONTRE-ME NA PRAÇA DAS ARTES e que a regra será: valor da letra +9, ajude Clara nesta missão.

a) Reescreva a regra na linguagem matemática, atribuindo ao valor da letra da mensagem original a variável x e ao valor da letra cifrada y .

b) utilizando o valor de cada letra na tabela acima, cifre a mensagem.

c) Encontre a função inversa que Bia deverá utilizar para decifrar a mensagem de Clara.

2- Mariana recebeu a seguinte mensagem: LYEPDELCOPOZBFPYFYNL. Ela já havia estudado um pouco sobre criptografia, então, tentou decifrá-la e descobriu que foi utilizada a seguinte regra para criptografar: valor da letra +11. Com essa informação:

a) Utilizando a tabela, reescreva a mensagem usando números.

b) Reescreva a regra na linguagem matemática, atribuindo ao valor da letra da mensagem original a variável x e ao valor da letra cifrada y.

c) Defina a função para decifrar a mensagem.

d) decifre a mensagem.

3- Desafio 1: A mensagem abaixo é uma frase de Einstein que foi cifrada com a função $f(x) = 3x + 16$, descubra seu conteúdo!

55-58 52-28-40-58 25-16 25-40-31-40-22-76-49-25-16-25-28 28-55-22-58-55-73-67-16-70-28 16 58-61-58-67-73-76-55-40-25-16-25-28

4- Desafio 2: Agora é com você, escolha uma frase famosa ou crie uma com no máximo 30 letras, determine uma função e faça a codificação da frase. Depois, trocaremos com outro grupo para que possa decifrá-la.

Apêndice D
Plano de Aula 4 e Atividades

Universidade Estadual do Sudoeste da Bahia - UESB
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Tabela D.1: Plano de Aula 4

Plano de Aula 4				
Duração	3h			
Objetivos	Revisar o conceito de números primos, compreendendo a importância destes para a segurança do RSA. Entender o funcionamento do RSA, criando chaves públicas e privadas.			
Conteúdo	Números primos; Criptografia RSA.			
Organização dos Espaços				
Espaços	Atividades	Duração	Papel do Aluno	Papel do Professor
Encontro pelo *Google Meet*.	Conversa sobre o método RSA.	40 min.	Participar da conversa com base no vídeo que assistiram.	Mediar as participações dos alunos por meio de questionamentos.
Encontro pelo *Google Meet*.	Usando o RSA para criptografar mensagens.	60 min.	Em grupos, reunidos pelo *Google Meet*, deverão resolver a atividade envolvendo o método RSA.	Mediar as discussões estimulando a participação de todos.
Encontro pelo *Google Meet*.	Conversa sobre a atividade anterior e orientação para as atividades que deverão fazer em casa.	20 min.	Participar da conversa, expondo se encontram dificuldades e os pontos positivos e negativos da atividade.	Mediar a conversa, fazer questionamentos e orientar as atividades que deverão fazer em casa.

Casa.	Pesquisa sobre outros métodos de criptografia que ainda não foram abordados.	60 min.	Em grupos, deverão pesquisar e elaborar um vídeo de até 5min falando sobre outro método de criptografia.	Orientar a pesquisa e a elaboração do vídeo.
Avaliação	No *Classroom*, será atribuída uma nota de 0 a 10, em cada atividade, tendo em vista o compromisso, a autonomia, o desempenho e a interação entre os estudantes e entre os estudantes e a professora.			

Fonte: Elaborado pela pesquisadora com base em Silveira Júnior (2020).

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Prezado(a) estudante, essa atividade tem como objetivo compreender a base da criptografia RSA de forma prática. Ela faz parte da pesquisa intitulada: "A Criptografia como Estímulo à Aprendizagem Matemática" promovida pela professora Ana Lourdes Moreno Rodrigues Silva, aluna do PROFMAT na Universidade do Sudoeste da Bahia - UESB, sob orientação do professor Fernando dos Santos Silva.

Obrigada por colaborar com esse trabalho!

Atividade sobre o RSA

Vamos compreender o RSA na prática?

Siga as orientações para que você possa criar a chave pública e a privada.

1- O primeiro passo é a escolha de dois números primos, p e q. Para facilitar o processo, a professora irá entregar dois primos a cada grupo, siga para as etapas seguintes.

Veja alguns números primos nesse site: <http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php>.

Lembre-se! Em situações reais são usados números astronômicos, mas para facilitar nossos cálculos, utilizaremos primos bem menores.

Como exemplo, considere $p = 17$ e $q = 23$

2- Calcule: $n = p \times q$.

$n = 17 \times 23 = 391$.

3- Calcule $\varphi(n) = (p-1)(q-1)$.

$\varphi(n) = (17-1)(23-1) = 352$

4- Escolha o número e, tal que $1 < e < \varphi(n)$, além disso e e $\varphi(n)$ devem ser coprimos, ou seja, não podem ter divisores em comum.

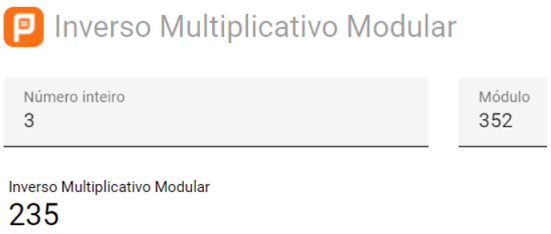
No nosso exemplo, $\varphi(n) = 352$, então vamos escolher $e = 3$, pois $1 < 3 < \varphi(n)$ e os números 352 e 3 são coprimos, veja que 3 é primo e não divide 352.

5- Agora, você deve encontrar um número d que satisfaça a seguinte congruência: $e \times d \equiv 1 \pmod{\varphi(n)}$. Isso significa que o produto de $e \times d$ ao ser dividido por $\varphi(n)$, valor encontrado no item 3, deixa resto 1. Na aritmética modular, d é chamado de inverso multiplicativo de $e : \varphi(n)$

Você irá encontrar d acessando a calculadora online: <https://pt.planetcalc.com/3311/>.

No espaço "número inteiro" escreva o valor de e, em "módulo" escreva o valor de $\varphi(n)$. Abaixo aparecerá o valor de d, ou seja, do inverso multiplicativo, conforme mosta a figura D.1

Figura D.1: calculadora online de inverso multiplicativo modular



Fonte: Dados da pesquisa.

Pronto! Já temos as chaves pública e privada. O par (n, e) é sua chave pública e pode ser disponibilizada para qualquer pessoa, enquanto p, q e d formam a sua chave privada e deve ser mantida em segredo.

Com as chaves encontradas podemos criptografar e descriptografar mensagens.

Cada grupo receberá uma das chaves públicas dos demais grupos e uma mensagem para que faça o processo de cifragem. Quando terminar, deverá devolver a mensagem para que o grupo de origem da chave pública decifre a mensagem usando a chave privada.

Para isso, siga as orientações!

1- De posse da mensagem e da chave pública de outro grupo, faça a pré-codificação da mensagem, isto é, transforme a mensagem em números, usando a tabela ASCII da figura D.2:

Como exemplo, vamos pré-codificar o nome ANA que ficará: 065078065.

2- Separe a mensagem pré-codificada em blocos, podem fazer isso colocando um traço

Figura D.2: Tabela ASCII

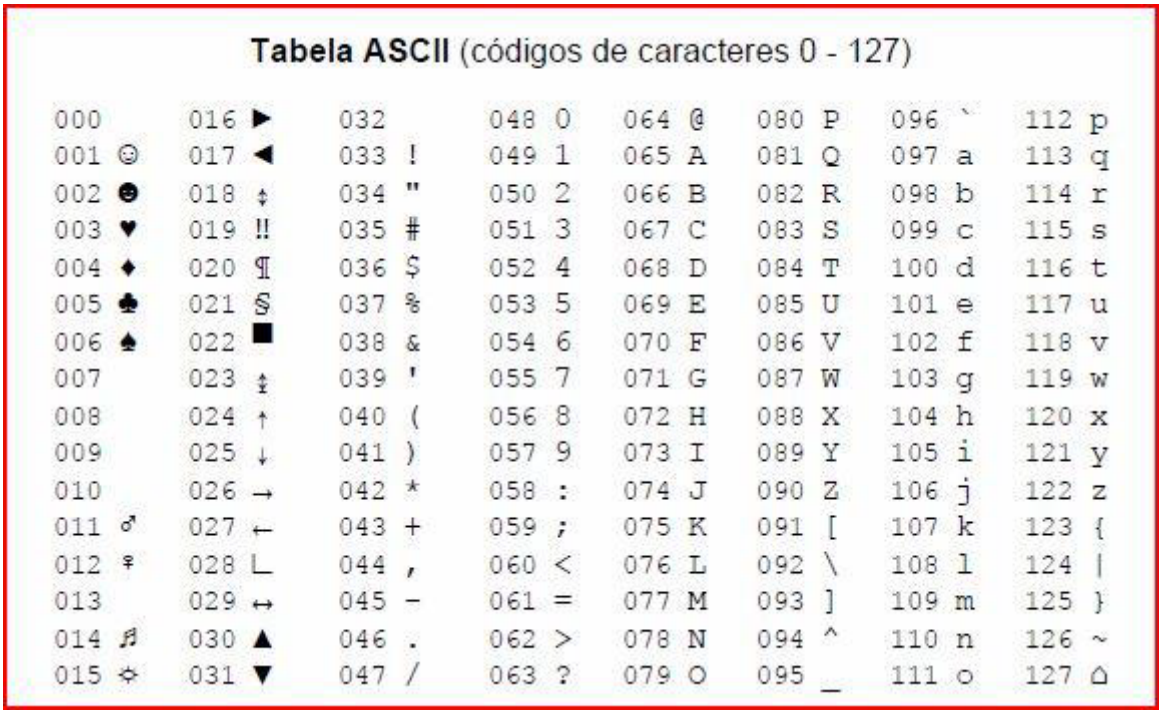


Tabela ASCII (códigos de caracteres 0 - 127)

000	016 ▶	032	048 0	064 @	080 P	096 `	112 p
001 ☺	017 ◀	033 !	049 1	065 A	081 Q	097 a	113 q
002 ☻	018 ↕	034 "	050 2	066 B	082 R	098 b	114 r
003 ♥	019 ‼	035 #	051 3	067 C	083 S	099 c	115 s
004 ♦	020 ¶	036 $	052 4	068 D	084 T	100 d	116 t
005 ♣	021 §	037 %	053 5	069 E	085 U	101 e	117 u
006 ♠	022 ▬	038 &	054 6	070 F	086 V	102 f	118 v
007	023 ↨	039 '	055 7	071 G	087 W	103 g	119 w
008	024 ↑	040 (	056 8	072 H	088 X	104 h	120 x
009	025 ↓	041)	057 9	073 I	089 Y	105 i	121 y
010	026 →	042 *	058 :	074 J	090 Z	106 j	122 z
011 ♂	027 ←	043 +	059 ;	075 K	091 [	107 k	123 {
012 ♀	028 ∟	044 ,	060 <	076 L	092 \	108 l	124 |
013	029 ↔	045 -	061 =	077 M	093]	109 m	125 }
014 ♫	030 ▲	046 .	062 >	078 N	094 ^	110 n	126 ~
015 ☼	031 ▼	047 /	063 ?	079 O	095 _	111 o	127 ⌂

Fonte: Dados da pesquisa.

entre os números que representam cada letra. Chamaremos cada um desses blocos de M. 065-078-065

3- Utilize a receita: $C \equiv M^e \pmod{n}$ para codificar cada um desses blocos. Mas, calma! Farão isso através desta outra calculadora online:

<https://www.calculadoraonline.com.br/divisao-polinomios>.

Digite M^e no dividendo e o valor de n no divisor. Seguindo nosso exemplo, $M = 065$, $e = 3$ e $n = 391$. Assim, digitamos 65^3 no dividendo, 391 no divisor, clicamos em calcular e consideramos o resto da divisão, ou seja, 143, coforme figura D.3

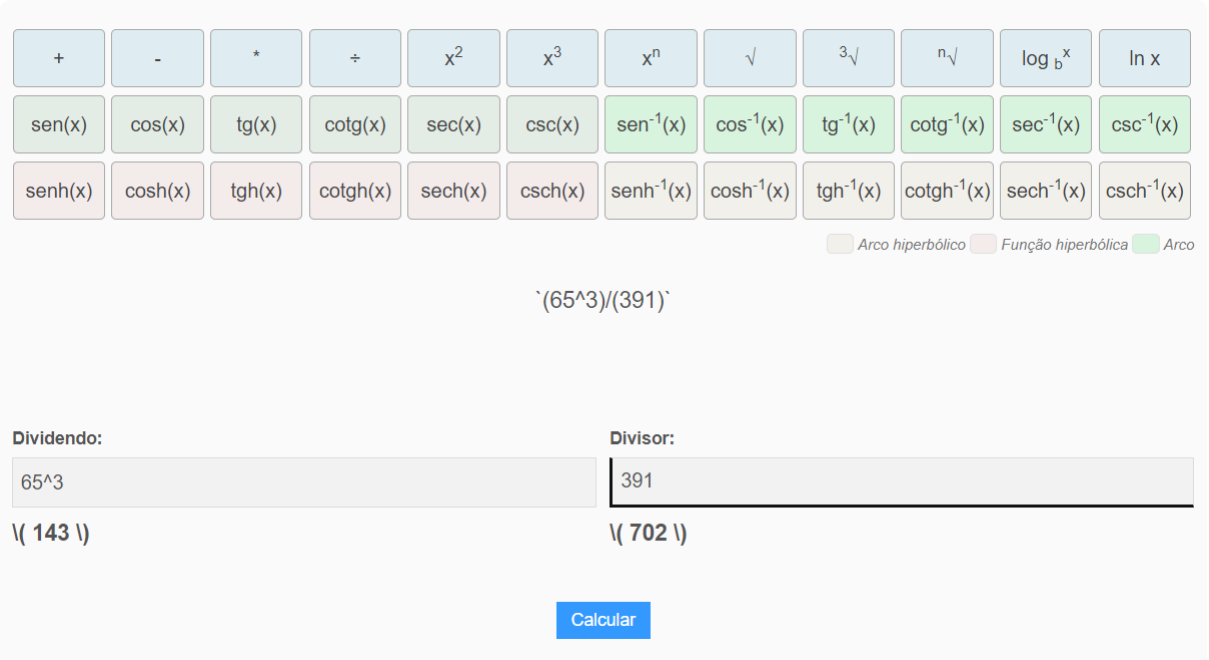
Dessa forma, $C \equiv 65^3 \pmod{(391)}$ equivale a $C \equiv 143 \pmod{391}$. Logo, o bloco 065 é cifrado como 143.

O grupo deve fazer isso até que todos os blocos sejam criptografados.

4- Cada grupo irá receber a mensagem cifrada e deverá descobrir seu conteúdo utilizando a chave privada d e seguindo essa outra receita: $M \equiv C^d \pmod{n}$ e poderão usar a mesma calculadora online da etapa 3.

Veja como fica o texto cifrado: $C \equiv 143 \pmod{391}$, considerando a chave privada $d = 235$.

Figura D.3: Calculadora online - Divisão de Polinômios



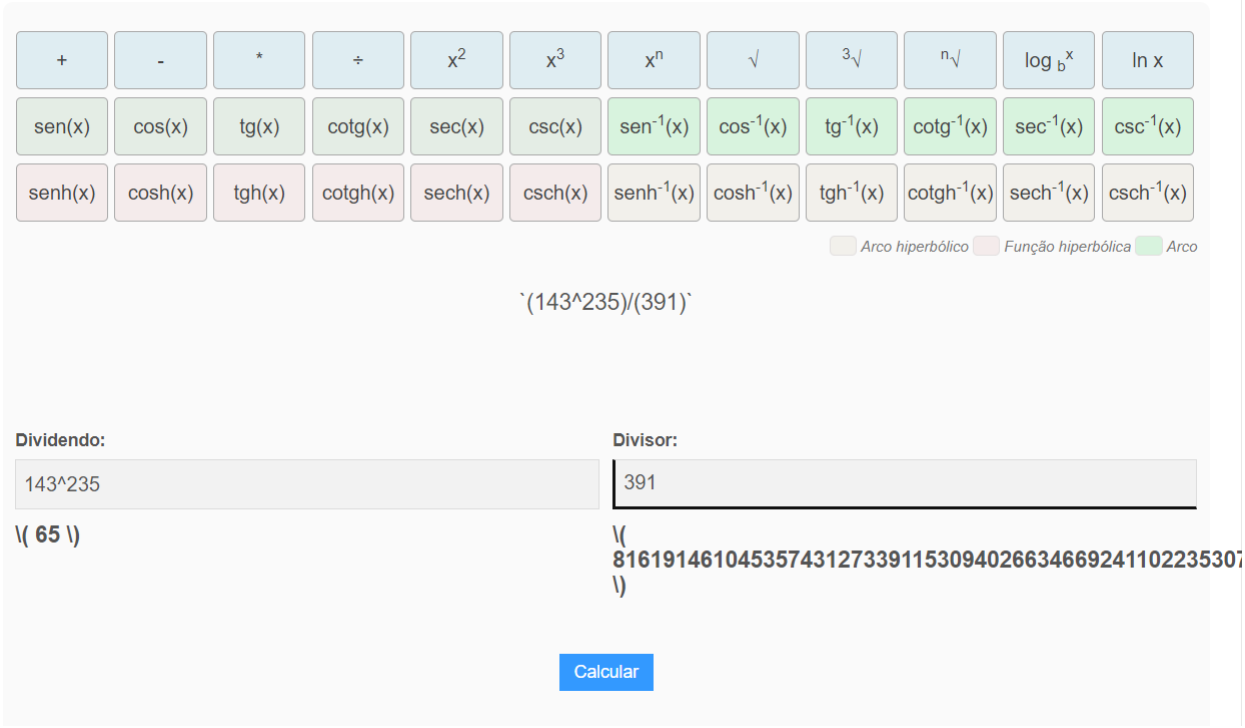
Fonte: Dados da pesquisa.

$M \equiv 143^{235} \pmod{391}$.

Como o resto da divisão é 65, temos $M = 654$. Para descobrir a letra, basta consultar a tabela ASCII, na qual $065 = A$.

O grupo deverá fazer esse processo até descobrir a mensagem criptografada.

Figura D.4: Divisão 143^{235} por 391 na Calculadora Online de Polinômios



Fonte: Dados da pesquisa.

Apêndice E
Plano de Aula 5 e Atividades

Universidade Estadual do Sudoeste da Bahia - UESB
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Tabela E.1: Plano de Aula 5

Plano de Aula 5				
Duração	3h			
Objetivos	Conhecer outros métodos de criptografia. Participar da gincana criptográfica, demonstrando o conhecimento adquirido com as atividades desenvolvidas.			
Conteúdo	Criptografia; Função.			
Organização dos Espaços				
Espaços	Atividades	Duração	Papel do Aluno	Papel do Professor
Encontro pelo *Google Meet*.	Apresentação dos vídeos elaborados sobre outros métodos de criptografia.	40min.	Os grupos deverão apresentar o vídeo para os colegas e professora.	Mediar as apresentações, fazendo as intervenções necessárias.
Encontro pelo *Google Meet*.	Gincana da Criptografia	120 min.	Em grupos, os alunos deverão realizar as atividades propostas dentro do tempo disponível.	Explicar aos alunos as regras e pontuação da gincana. Disponibilizar as tarefas envolvendo criptografia e função de forma gradual, indicando o tempo destinado para cada uma delas. Contabilizar os pontos e encerrar a gincana com a premiação das equipes.

Casa.	Questionário final.	20min.	Responder ao questionário: <https://forms.gle/ZYeNNguaD6NRrAX86> avaliando as atividades propostas.	Elaborar o questionário no *Google Forms* e disponibilizar no *Classroom*.
Avaliação	No *Classroom*, será atribuída uma nota de 0 a 10, em cada atividade, tendo em vista o compromisso, a autonomia, o desempenho e a interação entre os estudantes e entre os estudantes e a professora.			

Fonte: Elaborado pela pesquisadora com base em Silveira Júnior (2020).

Universidade Estadual do Sudoeste da Bahia - UESB
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional
Disciplina: Matemática
Professora: Ana Lourdes Moreno Rodrigues Silva
Etapa: 9º ano do Ensino Fundamental

Gincana Criptográfica

Regras

Os grupos serão os mesmos dos outros encontros e serão pontuados com 10 pontos para a tarefa cumprida, mais uma pontuação extra de acordo com o tempo gasto na prova.

1º lugar: 5 pontos
2º lugar: 4 pontos
3º lugar: 3 pontos
4º lugar: 2 pontos
5º e 6º lugar: 1 ponto

Os membros dos grupos adversários deverão manter o respeito e a cordialidade, sob pena de perder pontuação.

As provas deverão ser entregues por meio do *Classroom* ou *Whatsapp*.

1ª Prova: Apresentação do vídeo produzido pelo grupo sobre outras cifras que não foram abordadas durante os encontros (orientado no quarto encontro).

2ª Prova: Decodificação de mensagens.

No encontro anterior estudamos um pouco sobre o RSA e cada grupo criou uma chave pública e outra privada. Foi codificada uma mensagem entregue pela professora com a chave pública de outro grupo.

Agora, cada grupo receberá a mensagem que foi criptografada com sua chave pública e utilizará sua chave privada para decifrar seguindo a receita: $M \equiv C^d \pmod{n}$, utilizando a calculadora online: <https://www.calculadoraonline.com.br/divisao-polinomios>.

Lembre-se! M é o valor da letra de acordo com a table ASCII; C é a letra cifrada (que corresponde aos blocos do texto que cada um receberá), d é um dos números da sua chave privada e n é o produto dos dois primos que o grupo escolheu.

GRUPO 1

C (Bloco Cifrado)	120	141	94	156		178	115	121		120	121	195	81
M (Bloco Decifrado)													
Bloco Decifrado (letras)													

GRUPO 2

C (Bloco Cifrado)	252	101	81	364		71		118	252	242	86	118
M (Bloco Decifrado)												
Bloco Decifrado (letras)												

GRUPO 3

C (Bloco Cifrado)	185	12	288	12	229		12	288	129	108	50	103	288	103	233
M (Bloco Decifrado)															
Bloco Decifrado (letras)															

GRUPO 4

C (Bloco Cifrado)	136	53	62	221	136		221	53		13	221	53		179	

M (Bloco Decifrado)															
Bloco Decifrado (letras)															

C (Bloco Cifrado)	67	221	60	179	145	221
M (Bloco Decifrado)						
Bloco Decifrado (letras)						

GRUPO 5

C (Bloco Cifrado)	167	246		22	242	195		22	23		175	195	22	195
M (Bloco Decifrado)														
Bloco Decifrado (letras)														

C (Bloco Cifrado)	21	23	129
M (Bloco Decifrado)			
Bloco Decifrado (letras)			

GRUPO 6

C (Bloco Cifrado)	199	285	184		265	50	139	2	285		139	184	199	18	285	136

M (Bloco Decifrado)																
Bloco Decifrado (letras)																

3ª Prova: Esteganografia

Estas cabeças formam uma série, podendo ordenar-se da primeira à sexta segundo uma regra lógica. Qual é essa regra?

Figura E.1: 3ª Prova - Gincana Criptográfica

Fonte: <http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf>.

4ª Prova: Caça-palavras

Encontre as palavras, circule-as e envie uma foto.

Figura E.2: Caça-Palavras

Matemática e Criptografia

As palavras deste caça palavras estão escondidas na horizontal, vertical e diagonal, com palavras ao contrário.

A E T L W C H A V E S L O A A A A D
L L T W C R I P T O A N Á L I S E T
A A I A V M D F O N H Q B E N I W R
N D D S A I F A R G O N A G E T S E
T S E G U R A N Ç A T R P C N A A W
U L E E O I N Í M O D A R T N O C R
R M H N H H F N O Ã A E I T T H P H
I R B C G Y E H R Ç I N C T U E I V
N T G F O O H L U N E I H É E H M E
G A R R S W V S M U M G N V S F E N
A E I D A H E R I F S M B W I A T E
I N F O R M A Ç Ã O O A E S Y O R M

ALANTURING
CHAVE
CIFRADECÉSAR
CONTRADOMÍNIO
CRIPTOANÁLISE
ENIGMA
ESTEGANOGRAFIA
FUNÇÃO
IMAGEM
INFORMAÇÃO
RSA
SEGURANÇA

Fonte: Elaboração da autora.

5ª Prova: Responder à questão.

(Adaptado do simulado ENEM Integrado - 2021, FTD) Alan criou um código secreto, com base em uma correspondência entre as letras do alfabeto e os números naturais de 0 a 25. A relação de cada letra e seu respectivo número natural está exibida na tabela a seguir:

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

A codificação de uma mensagem era feita palavra por palavra, convertendo cada uma das suas letras para os números correspondentes e somando a cada um deles o tamanho da palavra. Os números que representavam letras de uma mesma palavra eram separados por hífen na mensagem codificada.

Assim, "ALAN", que é uma palavra de 4 letras, era codificada com a sequência 4-15-4-17, já que:

A→0+4=4

L→11+4=15

A→0+4=4

N→13+4=17

Obedecendo as regras do código de Alan, responda:

1) A mensagem "ADA" "LOVELACE", corresponderia a qual sequência numérica:

a) "4-7-4" "15-18-25-8-15-4-6-8"

b) "3-6-3" "19-22-29-12-19-8-10-12"

c) "3-6-3" "14-17-24-7-14-3-5-7"

d) "11-14-11" "22-25-32-15-22-11-13-15"

2) A sequência "10-24-8+20-17-6" corresponde a codificação da palavra:

a) ESCOLA

b) MALUCO

c) CÉLULA

d) CHORAR

6ª Prova: Código de César.

Nessa prova, você poderá utilizar o kit de encriptação do encontro II.

1- Cifre o nome do ditador romano Júlio César, com a chave 7.

J	U	L	I	O		C	E	S	A	R

2- Decifre a mensagem utilizando a chave 17.

S	F	H	L	Z	I	R

7ª Prova: Função para cifrar e decifrar mensagens.

1- Use a função $f(x) = 5x + 1$ para cifrar a palavra:

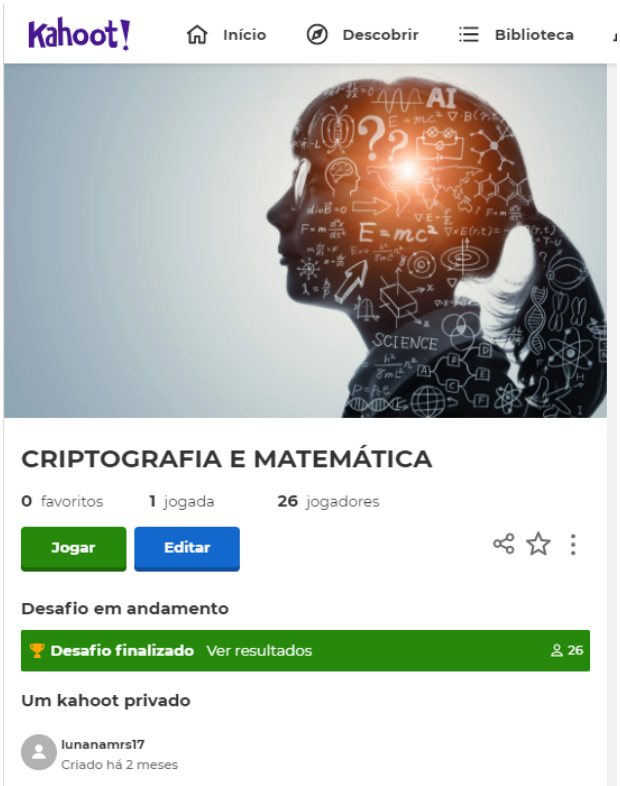
C	O	N	Q	U	I	S	T	A	S

2- Calcule a inversa da função do item 1 e decifre a mensagem:

21	91	76	21	86	01	66	11	01

8ª Prova: Kahoot: Criptografia e Matemática.

Figura E.3: Kahoot: Criptografia e Matemática



Fonte: Dados da Pesquisa.