UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA
INSTITUTO DE CIÊNCIAS EXATAS E DA NATUREZA
CURSO DE LICENCIATURA EM MATEMÁTICA

ELIZANDRO VICTOR ROGERY

A CRIPTOGRAFIA E A MATEMÁTICA: DE UM INSTRUMENTO DE PROTEÇÃO À MÉTODO DE INCENTIVO DE APRENDIZAGEM

REDENÇÃO-CE

2021

ELIZANDRO VICTOR ROGERY

A CRIPTOGRAFIA E A MATEMÁTICA:
DE UM INSTRUMENTO DE PROTEÇÃO À MÉTODO DE INCENTIVO DE APRENDIZAGEM

Monografia apresentada ao Curso de Licenciatura em Matemática do Instituto de Ciências Exatas e da Natureza da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como parte dos requisitos necessários para a obtenção do título de Graduado em Matemática. Área de concentração: Matemática.

Orientador: Prof. Dr. Rafael Jorge Pontes Diógenes

REDENÇÃO - CE

2021

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Rogery, Elizandro Victor.

R631c

A CRIPTOGRAFIA E A MATEMÁTICA: DE UM INSTRUMENTO DE PROTEÇÃO À MÉTODO DE INCENTIVO DE APRENDIZAGEM / Elizandro Victor Rogery. - Redenção, 2021.
44 f: il.

Monografia - Curso de Matemática, Instituto de Ciências Exatas e da Natureza, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2021.

Orientador: Por. Dr. Rafael Jorge Pontes Diógenes.

1. Criptografia. 2. Ensino-aprendizagem. 3. Sala de aula. I. Título

CE/UF/BSP CDD 512

ELIZANDRO VICTOR ROGERY

A CRIPTOGRAFIA E A MATEMÁTICA:
DE UM INSTRUMENTO DE PROTEÇÃO À MÉTODO DE INCENTIVO DE APRENDIZAGEM

Monografia apresentada ao Curso de Licenciatura em Matemática do Instituto de Ciências Exatas e da Natureza da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como parte dos requisitos necessários para a obtenção do título de Graduado em Matemática. Área de concentração: Matemática.

Aprovada em: 20 / 08 / 2021.

BANCA EXAMINADORA

Prof. Dr. Rafael Jorge Pontes Diógenes (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Prof. Dr. Joserlan Perote da Silva
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Prof. Me. Marcos Paulo Barros Lopes
Colégio Ari de Sá Cavalcante

Dedico este trabalho de uma forma muito especial à minha querida e amada avó e professora Domingas Rofino Sanca quem me criou, e a todas as pessoas que contribuíiram direta ou indiretamente com a sua realização.

AGRADECIMENTOS

Primeiramente agradeço à Deus, por me abençoar com saúde, me proteger, guiar e me dar forças nos momentos difíceis para enfrentar os obstáculos.

Aos meus pais, Victor Luis Rogery e Nilsa Maria Rofino Bampoque por me conceber e me apoiar sempre. À toda minha família pela confiança em mim depositada, pelo apoio moral, financeiro e material.

À Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB) por me conceder a oportunidade de ingressar num curso superior, pelas bolsas, pelo auxílios financeiro e por toda a assistência prestada.

À CAPES, pelo apoio financeiro com a manutenção da bolsa de auxílio no Programa Institucional de Bolsa de Iniciação à Docência (PIBID).

Ao meu admirável professor e orientador Prof. Dr. Rafael Jorge Pontes Diógenes, pela excelente orientação, pela compreensão e por aceitar embarcar comigo neste desafio, meu muito obrigado.

Aos professores participantes da banca examinadora Prof. Dr. Joserlan Perote da Silva e Prof. Me. Marcos Paulo Barros Lopes pelo tempo, pelas valiosas colaborações e sugestões.

Aos colegas da turma, pela reflexões, críticas, sugestões, parceria e motivação.

Para finalizar, agradeço a todos os funcionários da UNILAB, os motoristas dos ônibus, os bibliotecários, os seguranças, as tias do RU e da limpeza, que propiciam um ambiente agradável que contribuíram para o meu aprendizado.

"Na maior parte das ciências, uma geração põe abaixo o que a outra construiu, e o que a outra estabeleceu a outra desfaz. Somente na Matemática é que cada geração constrói um novo andar sobre a antiga estrutura. (Hermann Hankel)

RESUMO

O presente trabalho tem por objetivo fazer o uso da criptografia como um método instigante à aprendizagem dos conteúdos matemáticos, como também explanar alguns tipos destas criptografias que possam ser utilizadas como auxílio do professor nas aulas de matemática abordando os conteúdos de permutação simples e com elementos repetido, função polinomial do primeiro grau e a sua inversa, multiplicação de matriz e matriz inversa e a divisão inteira ou resto da divisão. A questão do uso de situações problemas para a visualização da abstração da matemática, tem gerado muitas discussões, nesta linha de pensamento, sendo a criptografia um método de comunicar secretamente, pode ser interessante para cativar a atenção dos alunos. Para a produção, foi feito uma abordagem histórica, depois, apresentação dos tipos de criptografias compatíveis com o objetivo do trabalho e a explanação individual de cada uma delas, e sugeridas as atividades aplicáveis à sala de aula.

Palavras-chave: Criptografia. Ensino-aprendizagem. Sala de aula. Encriptação e desencriptação.

ABSTRACT

This work aims to make the use of cryptography as an exciting method for learning mathematical content, as well as explaining some types of cryptography that can be used as an aid to the teacher in mathematics classes, addressing the simple permutation contents and with repeated elements , polynomial function of the first degree and its inverse, matrix and inverse matrix multiplication and the integer division or remainder of the division. The issue of using problem situations to visualize the abstraction of mathematics has generated many discussions, in this line of thought, as cryptography is a method of secretly communicating, it can be interesting to captivate students' attention. For the production, a historical approach was made, afterwards, a presentation of the types of cryptography compatible with the objective of the work and an individual explanation of each one of them, and the activities applicable to the classroom were suggested.

Keywords: Cryptography. Teaching-learning. Classroom. Encryption and decryption.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O mundo atual, considerado na era digital, está envolvido com a criptografia no cotidiano atuando na maioria das vezes para a proteção e segurança de todos sem mesmo alguns destes terem o mínimo conhecimento dela. A criptografia faz-se presente no nosso cotidiano desde os mais pequenos aspectos eletrônicos aos mais diversos que precisam ser escondidos ou protegidos das invasões externas, como nas contas bancarias, nas transações, os caixas eletrônicos, as comunicações através de aplicativos de mensagens, entre outras ferramentas compartilháveis ou não que necessitam de um nível de privacidade.

A palavra Criptografia é proveniente do grego, onde na língua originaria é composta por duas palavras sendo elas: *kryptos* que significa oculto ou escondido e *gráphein* que significa escrita, formando assim a frase escrita escondida ou escrita oculta. A criptografia como o próprio significado da palavra profere, é a forma de escrever uma mensagem, informação ou dados em códigos decifráveis somente por emissor e o receptor, ou seja, sem correr o risco de fornecer informações à terceiros, pois perante todo o percurso até a chegada ao receptor, essas mensagens não são nadas além de uns códigos ou umas palavras sem sentido de acordo com a técnica utilizada no processo de encriptação.

A criptografia como um método de instigar a aprendizagem na disciplina de matemática, parte da perspectiva de tornar estas aulas mais atraentes, interativas e interessantes, cativando a atenção do aluno e consequentemente gerando aprendizagem, que é o proposito do ensino. Segundo Lima (2003, p. 45),

> as aplicações são a parte ancilar da Matemática. São a conexão entre a abstração e a realidade. Para um grande número de alunos, são o lado mais atraente das aulas, o despertador que os acorda, o estímulo que os incita a pensar. O professor deve considerar como parte integrante e essencial da sua tarefa o desafio, a preocupação de encontrar aplicações interessantes para a matéria que está apresentando. Como dissemos acima, nem sempre isso é fácil. Mas vale a pena indagar, pesquisar, pensar, incomodar os colegas, vasculhar livros. (LIMA, 2003, p. 45)

Prender a atenção do aluno, é um dos principais e fundamental passo no processo de transmissão do conhecimento, Vygostky (1991, p. 101 *apud* TONCHE 2014) afirma que a motivação é a base de todo processo de aprendizagem, que vão do desejo à necessidade. Assim, ter um método fora do tradicional capaz de ser motivador, facilitaria ainda mais o trabalho do professor e obtenção dos seus resultados futuros. Para isso, pensando na melhoria de aprendizado em diversos conteúdos matemáticos, foi pensado em criptografia como o meio de traçar o paralelo entre esses conteúdos e o mundo real, através de atividades desafiadoras que instigam a aprendizagem destes conteúdos.

O presente trabalho tem como objetivo principal utilizar a criptografia como um método motivacional para aprendizagem da matemática. E um dos objetivos específicos centraliza-se em fornecer ferramentas para responder a famosa interrogação

"onde aplicarei esse conhecimento no meu dia-a-dia?"e fornecer uma ferramenta auxiliadora para os professores nas suas aulas. Apresentando a criptografia como uma das aplicações matemáticas, vai além do incentivo a aprendizagem, mas também, como uma resposta de onde podemos nos deparar com o uso de certos conteúdos matemáticos no nosso cotidiano. Dando uma visão ao aluno de que a matemática vai além das abstrações.

Para a produção deste trabalho, foram investigados alguns tipos de criptografias existentes, por que funcionam, a matemática por trás e as possíveis atividades envolvendo essas criptografias na sala de aula para os alunos, como um método de incentivo à aprendizagem da matemática. Para o tal feito, foram selecionados alguns destas criptografias, e explanados os seus modos operantes, a matemática envolvente (para os que usem a matemática) e as possíveis adaptações matemáticos (para os que não usam a matemática diretamente).

Antes, foram investigadas a origem e a historia por trás das criptografias utilizadas, tanto como e o por que surgiram. As suas relevâncias, os papeis desempenhados nas suas primeiras atuações, e por último as modificações sofridas com o passar do tempo e o avanço da tecnologia. Após essa etapa, foram explanados individualmente todos os processos envolventes dos tais métodos, os primeiros passos para criptografar as mensagens, as sequências lógicas dos passos, os aspetos que garantem o processo de desencriptação da mensagem até a chegada na mensagem na forma original.

Por último, foram apresentados algumas sugestões de atividades utilizando os métodos de criptografia anteriormente desenvolvidos. Sendo sugestivos, estas atividades podem ser modificadas de acordo com propósito do professor e o problema da turma. Visto tudo, percebe-se a relevância do uso de criptografia como incentivo de aprendizagem de matemática, levando em conta que o público alvo do ensino básico, é um dos mais envolventes com a tecnologia, facilitaria muito em chamar suas atenções com este método.

2 CRIPTOGRAFIA

Com base em Coutinho (2005, p.1), a criptografia pode ser compreendido como um estudo dos métodos de codificar (encriptar) uma mensagem, de modo que somente o seu destinatário legítimo consiga ler e interpretá-la. Nessa perspetiva, surgiram diversos métodos utilizados por diversas pessoas com o intuito de manter uma certa proteção para os fins à quais esses métodos são utilizados.

O processo pelo qual uma mensagem original é transformada numa mensagem criptografada chama-se **encriptação** e o processo contrario que é transformar a mensagem encriptada na original é chamada de **desencriptação**. No cenário da criptografia, fala-se muito de cifras e códigos, ambos com um mesmo proposito que é de ocultar o significado de uma mensagem "criptografar", as vezes, estas chegam a ser tratados de modos iguais, chamando assim uma cifra de código ou um código de cifra, o que pode não ser considerado errado, mas, há uma leve diferença existente entre os dois, ou melhor entre os seus modos operantes.

O que difere uma cifra de um código não é um fenômeno gigantesco, é o simples fato de que para encriptar e desencriptar através de cifras, independente do método usado, só são trocados as letras das palavras que compõem a mensagem usando o mesmo alfabeto e a língua da mensagem original, ao passo que o código já usa uma outra analogia com os números, os símbolos e umas combinações que precisam ser antes conhecidos para posteriormente chegar na mensagem original. Então nesta linha, chamar a cifra de César ou qualquer uma outra de código não é errado, só que pode gerar um pouco de confusão para a pessoa que já está habituado a distingui-los.

No processo de encriptar e desencriptar uma mensagem, existe um fator relevante chamado chave, que dependendo do método utilizado para a encriptação, pode ser simétrica ou assimétrica. Uma chave é dita simétrica quando é única, usada tanto para encriptar como para desencriptar a mensagem, sendo assim, ele merece ser escondida e só conhecida pelo emissor e receptor (chave secreta), e uma chave é dita assimétrica quando a usada para encriptar a mensagem é diferente da usada no processo inverso, fazendo assim com que conhecer a chave não implicará em descriptografar a mensagem, assim, a chave pode ser conhecido pro qualquer um, também conhecida como chave pública.

2.1 UM POUCO DE HISTÓRIA

A necessidade e o desejo de ter uma informação guardada, bem protegida ou a de ter uma comunicação boa, secreta e segura, não é de hoje, já houve este problema desde as épocas primordiais, mas, se intensificou mais ainda com o evolução do comércio e dos conflitos. Daí a preocupação em manter uma troca de informação (mensagem) segura sem o risco de cair nas mãos dos adversários ou inimigos, virou uma grande preocupação

inicialmente entre os Egícios, Gregos e os Romanos, sendo um dos primeiros a usarem esta técnica. Assim nasceu a criptografia.

A palavra Criptografia provém do grego, onde na língua originaria é composta por duas palavras, *kryptos* e *gráphein* significando respetivamente oculto ou escondido e escrita, formando assim em português a palavra escrita oculta. A criptografia pode ser compreendido como a arte de comunicar secretamente utilizando códigos ou palavras sem sentido compreensíveis e somente pelo emissor e receptor ou pelas pessoas desejadas, esse é o intuito. A criptografia é bastante antiga, segundo (MORENO *et al.* 2005, p. 13), já se utilizava desde a época do uso de hieróglifos (método de escrita no antigo Egíto).

A arte de criptografar uma mensagem funciona na perspectiva de ocultar o significado da mensagem, não a própria mensagem em si, ao passo que o seu antecessor que é a esteganografia busca os meios de transmitir uma mensagem sem que seja notada a sua existência, escondendo assim a própria mensagem. Como salientou o Fiarresga (2010, p.3) um dos meios mais comum era de raspar a cabeça de "escravos"e escrever a mensagem pretendida no couro cabeludo. Após o crescimento dos cabelos, a pessoa é enviada para o seu destino, que ao chegar é cortado o cabelo de novo para ler a mensagem.

Entre os anos 500 e 600 a.C, foi uma época em que a criptografia ganhou mais espaço e destaque, passou a ser utilizado mais para a comunicação (troca de mensagem) de diversos meios e métodos capazes de esconder o significado da mensagem, não a própria mensagem em si. Uns dos primeiros métodos usados para encriptação de uma mensagem foram a **cifra de César** e o **citale espartano**, usados por pessoas diferentes em lugares diferentes mas todos eles com histórico em conflitos armados.

A cifra de César ganhou essa nomenclatura por conta do ex-imperador da Antiga Roma Júlio César, que foi o criador deste método para transmissão de mensagem. Como acima anunciado, o imperador César usava este método para comunicar com os seus soldados no campo da batalha, enviando-lhes instruções de ataques, os pontos considerados fracos dos adversários e o desenrolar da batalha. Para não correr o risco de vazamento de informações, César nas suas mensagens, trocava a letra pretendida ou a letra correta pela terceira que lhe sucede no abecedário, assim deixando a palavra incompreensível ou melhor sem sentido as vezes. Este método será melhor explicado no decorrer do trabalho.

A citale espartano que também pode ser chamado de cifra de espartano, é também, um modelo usado pelos guerreiros espartanos da Antiga Grécia com o mesmo propósito de não correr o risco de fornecer técnicas invasivas ou defensivas aos adversários, caso conseguissem interceptar a mensagem. Para tal, eles usavam uma bastão de madeira onde é enrolada uma fita de couro servindo de folha. Eles escreviam em formas de linhas a qual usamos atualmente contendo cada letra em uma parte da fita. Após a escrita, a fita é removida do bastão e usa-se como cinto disfarçando para amarar as calças no processo de envio até chegar ao respetivo destinatário.

O destinatário ao receber essa mensagem através da fita, faz o mesmo processo

inicial usado por emissor na escrita do texto. Ele enrola a mesma fita numa bastão exatamente igual a usada pelo emissor na produção da mensagem, assim, ele consegue de forma clara e coerente ler a mensagem enviada. Para uma melhor compreensão, veja a Figura 1.

Figura 1 – Citale Espartano

Fonte: Educalingo (2021)

A criptografia teve como uma das funções iniciais estabelecer a comunicação perante conflitos militar, e desempenhou um papel fundamental nessas guerras em que foi usado, desde tempos antigos, aos atuais.

Com o passar do tempo, o aumento da curiosidade, os estudos e o modo constante que o mundo e os conhecimentos vêm se evoluindo, os códigos e as cifras de algumas criptografias conseguiram ser descobertos, fazendo com que esses passassem a ser fracos e assim fáceis de descriptografar até por pessoas não legitimas, então para colmatar esse problema surgiu a necessidade de criação de novas e mais complexas criptografias a fim de não correr o risco de fornecer informações valiosas às pessoas com mau intuito ou para as pessoas adversárias.

Um dos estudos com um propósito oposto a da criptografia é denominado de criptoanálise, que nasceu na perspectiva de quebrar os códigos e as cifras usados para esconder uma mensagem secreta. A criptoanálise estuda as padrões e técnicas usadas no processo para posteriormente desfazê-las usando o processo inverso e assim ter acesso a mensagem original. Essa prática incentivou o uso de uma ferramenta mais complexa para codificação das mensagens com o proposito de torná-los mais difíceis de quebrar, assim, se deu origem ao implementação dos conceitos matemáticos na criptografia.

Os tais conceitos matemáticos na criptografia, antes eram usadas manualmente tanto para criptografar como para o processo inverso, e eram ainda mais difíceis de quebrar pela dificuldade apresentada nos cálculos. Hoje, com o avanço exponencial da era digital e da tecnologia, o trabalho de efetuar os cálculos para codificar como para descodificar a mensagem, fica sob responsabilidade de computadores, assim, diminui o tempo de cálculo, mas não a dificuldade e a eficacia por trás do método, o que quer dizer que mesmo com

auxilio de computador, torna difícil ainda quebrá-los.

2.2 ALGUNS TIPOS DE CRIPTOGRAFIA

Nesta sessão, apresentaremos alguns tipos de criptografia, levando em consideração que essas não são as únicas existentes ou utilizadas no dia-a-dia, mas, necessários ou compatíveis com o nosso objetivo de estudo, sendo essas que usam métodos matemáticos aplicáveis ao ensino básico. Uma vez que a nossa pesquisa foca-se na busca dos métodos motivacionais para a aprendizagem de matemática usando criptografia. Para tal, foram escolhidas as seguintes, que serão desenvolvidas individualmente à frente:

- CIFRA DE TRANSPOSIÇÃO;
- CIFRA DE CÉSAR;
- CRIPTOGRAFIA POR MATRIZ;
- CRIPTOGRAFIA RSA.

A matemática por trás das criptografias exerce um papel de extrema relevância no que tende ao auxilio no quesito da complexidade de proteção contra as invasões externas, pois a criptografia em si já gera uma dificuldade, desde os métodos considerados mais simples, então misturá-lo com a matemática, eleva ainda mais esse grau da dificuldade em violá-lo, então as técnicas matemáticas dão suportes de proteção a criptografias a qual são utilizadas.

Continuando nesta linha de uso da matemática na criptografia, uma das questões indispensáveis é "o por quê ela funciona"? A matemática por trás das criptografias funciona por conta da inversibilidade, dando a possibilidade de desfazer o processo, pois quando o emissor encripta uma mensagem, espera-se que destinatário legitimo consiga vê-la na forma original, que consiste em desfazer a encriptação ou simplesmente inverter a encriptação. Para isto, o método matemático tem que ser inversível, o fato que pode ter variações de método em método de acordo com os seus modos operantes.

A seguir, apresentaremos os conceitos dos tais métodos e ilustraremos seus exemplos, demostrando as suas matemáticas envolventes, como também, os métodos que permitem saber se é inversível ou não de acordo com cada conteúdo matemático envolvido no tal método para o processo de encriptação e desencriptação.

Admitiremos que o leitor tem conhecimento da matemática utilizada a seguir.

2.2.1 Cifra de Transposição

Como o próprio nome **transposição** profere, esta cifra para encriptar uma mensagem usa algoritmo de transposição, que consiste em permutar as letras das palavra que compõem a mensagem, mudando estas das suas posição deixando assim a palavra incompreensível ou sem um sentido. Não há uma regra fixa de mudar as palavras, esta, varia de acordo com o emissor e receptor, desde já que eles conseguem se entender baseando

nas tais permutações feitas, e essas que podem ser entre as letras equidistantes, entre as silabas, entre duas letras sequenciais, entre outras.

2.2.2 Cifra de César

É uma das primeiras e mais conhecidas cifras, que para a encriptação de uma mensagem usa a técnica de substituição no próprio abecedário da língua local. A ideia inicial é de substituir a letra desejada pela terceira letra que lhe sucede nesse abecedário, e assim chegando nas últimas três letras finais do mesmo, é notório que não haverá mais letras sucessoras para prosseguir com a permutação usual, então para completar esse processo, essas últimas letras são substituídas ou permutadas pela três primeiras, pois pelo fato dessas serem as primeiras, não têm um antecessor, assim elas não são sucessores de ninguém.

Para a desencriptação, faz-se a volta do processo inicial, em outras palavras podemos assim dizer o inverso, que consiste em substituir a presente letra pela terceira letra que lhe antecede, usando o mesmo abecedário usado no processo de encriptação. Após a prática deste método em todas as letras das palavras que compõem a mensagem encriptada, automaticamente volta-se a mensagem original, e daí, consegue-se estabelecer uma comunicação entre o emissor e o receptor como pretendido. A tabela a seguir, traz uma ilustração do método acima referido.

Tabela 1 – Método de César

Mensagem Original	A	B	C	D	E	F	G	H	I	J	K	L	M
Mensagem Cifrada	d	e	f	g	h	i	j	k	l	m	n	o	p
Mensagem Original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mensagem Cifrada	q	r	s	t	u	v	w	x	y	z	a	b	c

Fonte: Elaborada pelo autor.

Com a tabela formada, torna-se mais fácil encriptar uma mensagem, uma vez que o único trabalho de emissor, quanto posteriormente do receptor, será simplesmente de converter a letra cifrada pela original sem a necessidade de ter que contar ainda três letras após a desejada. Esse cifra sofre algumas variações com o propósito de ficar ainda mais incompreensível, essas variações que se dão na sequência dos números posteriores a serem tomados, que vão de 1 a 25 desde já estabelecida uma relação compreensível entre ambas as partes, sabendo exatamente o número de letras sucessivas que representa a pretendida.

Exemplo 2.1 *Encriptaremos a frase "EU AMO A MATEMÁTICA" através deste método.* Temos o seguinte:

E	U		A	M	O		A		M	A	T	E	M	Á	T	I	C	A
H	X		D	P	R		D		P	D	W	H	P	D	W	L	F	D	.

Através deste método, o receptor receberá a mensagem na forma:

H X D P R D P D W H P D W K F D

onde que para desencriptá-la, precisa usar a mesma tabela utilizada no processo de encriptação, e fazer as devidas substituições, tendo assim de volta a mensagem na forma original, que será

H	X	D	P	R	D	P	D	W	H	P	D	W	K	F	D
E	U	A	M	O	A	M	A	T	E	M	Á	T	I	C	A

.

Este método para o processo de encriptação e desencriptação, não usa um modelo matemático, mas, segundo Rosseto (2018, p. 30) dá para usar a ideia da função neste método. Que consiste primeiramente em transformar as letras nos números (pré-codificação), depois escolher uma função polinomial do primeiro grau do tipo $f(x) = ax + b$, onde o x é o valor corresponde a letra pretendida, a e b constantes quaisquer fixas, e o resultado desta função é a letra encriptada. Para a pré-codificação, usaremos uma nova tabela a qual converteremos letras em números da seguinte maneira:

Tabela 2 – Pré codificação Metodo de César aplicado a função

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

Fonte: Elaborada pelo autor.

Com a tabela já montada, encriptaremos a mesma mensagem "EU AMO A MATEMÁTICA", só que de um jeito diferente do anterior. Vale ressaltar que, quando utilizamos a matemática para encriptar uma mensagem, temos que estar pensando logo na desencriptação, assim, é necessário pensar na inversibilidade do método.

A questão da inversibilidade que é um fator de extrema relevância para o processo da desencriptação da mensagem. A partir deste método de cifra de César aplicada a função, se vê na bijetividade da função escolhida, assim, estabelece-se uma regra inicial a seguir em que todos os elementos do domínio têm que ter um correspondentes no contradomínio e único para cada elemento escolhido e não mais que isso. No fim da encriptação, a mensagem é enviada em forma numérica, de acordo com as imagens obtidas. O receptor para decodificá-lo, precisa primeiramente calcular a inversa da função codificadora e posteriormente substituir os respetivos valores da nova imagem pela letra correspondente, assim, terá a mensagem original.

Para uma exemplificação, considere a função bijetora dada por $f(x) = 2x - 5$. Agora encriptando a mensagem teremos:

E	U		A	M	O		A		M	A	T	E	M	Á	T	I	C	A
14	30		10	22	24		10		22	10	29	14	22	10	29	18	12	10

$f(14) = 2 \cdot 14 - 5 = 28 - 5 = 23$
$f(30) = 2 \cdot 30 - 5 = 60 - 5 = 55$
$f(10) = 2 \cdot 10 - 5 = 20 - 5 = 15$
$f(22) = 2 \cdot 22 - 5 = 44 - 5 = 39$
$f(24) = 2 \cdot 24 - 5 = 48 - 5 = 43$
$f(10) = 2 \cdot 10 - 5 = 20 - 5 = 15$
$f(22) = 2 \cdot 22 - 5 = 44 - 5 = 39$
$f(10) = 2 \cdot 10 - 5 = 20 - 5 = 15$

$f(29) = 2 \cdot 29 - 5 = 58 - 5 = 53$
$f(14) = 2 \cdot 14 - 5 = 28 - 5 = 23$
$f(22) = 2 \cdot 22 - 5 = 44 - 5 = 39$
$f(10) = 2 \cdot 10 - 5 = 20 - 5 = 15$
$f(29) = 2 \cdot 29 - 5 = 58 - 5 = 53$
$f(18) = 2 \cdot 18 - 5 = 36 - 5 = 31$
$f(12) = 2 \cdot 12 - 5 = 24 - 5 = 19$
$f(10) = 2 \cdot 10 - 5 = 20 - 5 = 15$

a mensagem "EU AMO A MATEMÁTICA" encirptada através do método de César usando uma função, é dado por:

$$23 \quad 55 \quad 15 \quad 39 \quad 43 \quad 15 \quad 39 \quad 15 \quad 53 \quad 23 \quad 39 \quad 15 \quad 53 \quad 31 \quad 19 \quad 15$$

O receptor para a desencriptação da presente mensagem, precisa primeiramente conhecer a inversa da função codificadora, após isso, só substituir os pontos na função que o resultado obtido é a mensagem original na forma pré-codificada. Por último, é só utilizar a tabela para converter os números nas suas respectivas letras correspondidas. A inversa da função $f(x) = 2x - 5$ é dada por:

$$f^{-1}(x) = \frac{x+5}{2},$$

aplicando os valores da mensagem recebida pelo receptor teremos:

$f^{-1}(23) = \frac{23+5}{2} = \frac{28}{2} = 14$
$f^{-1}(55) = \frac{55+5}{2} = \frac{30}{2} = 30$
$f^{-1}(15) = \frac{15+5}{2} = \frac{20}{2} = 10$
$f^{-1}(39) = \frac{39+5}{2} = \frac{44}{2} = 22$
$f^{-1}(43) = \frac{43+5}{2} = \frac{48}{2} = 24$
$f^{-1}(15) = \frac{15+5}{2} = \frac{20}{2} = 10$
$f^{-1}(39) = \frac{39+5}{2} = \frac{44}{2} = 22$
$f^{-1}(15) = \frac{15+5}{2} = \frac{20}{2} = 10$

$f^{-1}(53) = \frac{53+5}{2} = \frac{58}{2} = 29$
$f^{-1}(23) = \frac{23+5}{2} = \frac{28}{2} = 14$
$f^{-1}(39) = \frac{39+5}{2} = \frac{44}{2} = 22$
$f^{-1}(15) = \frac{15+5}{2} = \frac{20}{2} = 10$
$f^{-1}(53) = \frac{53+5}{2} = \frac{58}{2} = 29$
$f^{-1}(31) = \frac{31+5}{2} = \frac{36}{2} = 18$
$f^{-1}(19) = \frac{19+5}{2} = \frac{24}{2} = 12$
$f^{-1}(15) = \frac{15+5}{2} = \frac{20}{2} = 10$

os resultados desta função aplicado a cada ponto são as letras da nossa mensagem, assim, a nossa mensagem desencriptada é:

$$14 \quad 30 \quad 10 \quad 22 \quad 24 \quad 10 \quad 22 \quad 10 \quad 29 \quad 14 \quad 22 \quad 10 \quad 29 \quad 18 \quad 12 \quad 10\,.$$

E usando a tabela de conversão, teremos o nossa mensagem na forma original, que é:

Observação: Vale destacar que para não dificultar muito as contas da função $f(x) = ax+b$ devem ser de tal forma que a imagem tenha três algarismos.

14	30		10	22	24		10		22	10	29	14	22	10	29	18	12	10
E	U		A	M	O		A		M	A	T	E	M	Á	T	I	C	A

2.2.3 Criptografia por Matriz

A criptografia por matriz como o próprio nome profere, pode ser definido como uso dos conceitos matriciais na encriptação. Se prestamos bastante atenção nas sequências até aqui utilizadas, podemos perceber que o processo de encriptação e desencriptação acontece em duas etapas, que são a ida e a volta, onde a volta é nada mais e nada menos que a inversão da ida. A encriptação de uma mensagem por meio de matriz e outros métodos que usam o código, acontecem em duas etapas seguintes: a **pré-codificação** e a **codificação**.

Como já explanado no paralelo traçado entre o código e a cifra, pré-codificação é a etapa em que acontece a substituição da letra desejada pelo caractere correspondente, dependendo do método utilizado na encriptação. Como o nosso caso se refere a matriz, então a substituição será alfabética por numérica, em que começaremos da letra A igual ao número 1 e assim sucessivamente até a ultima letra do alfabeto, depois disso, continuaremos a numeração para determinar o espaço, a virgula, o ponto e o começo de um novo paragrafo. Conforme a Tabela 3 abaixo, temos a ilustração da pré-codificação.

Tabela 3 – Pré codificação do método da matriz

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z	.	,	-	≫
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Fonte: Elaborada pelo autor.

Os quatro últimos números da nossa tabela representam respetivamente: 27 o ponto final ou ponto na mesma linha, 28 a vírgula, que é a mesma vírgula utilizada nos textos normais para marcar uma pausa e separa as expressões, o 29 representa o espaço entre as letras que separam uma palavra da outra, e o último que é 30 representa um novo paragrafo, que já é uma mudança de ideia. Após a pré-codificação, o próximo passo é a codificação propriamente, e essa etapa se define pelo uso dos conceitos matemáticos para encriptação, nesse caso, como o método escolhido se fundamenta no uso da matriz, então a matriz é o método matemático para tal.

Exemplo 2.2 *Vamos pré-codificar a frase "EU AMO A MATEMÁTICA" usando a Tabela 3.*

Fica:

E	U	-	A	M	O	-	A	-	M	A	T	E	M	Á	T	I	C	A	.
5	21	29	1	13	15	29	1	29	13	1	20	5	13	1	20	9	3	1	27

Então a nossa mensagem pré-codificada é:

5	21	29	1	13	15	29	1	29	13	1	20	5	13	1	20	9	3	1	27

Após a pré-codificação, fica a critério do emissor escolher a matriz codificadora inversível, garantindo assim a possibilidade de desencriptação da mensagem. Neste método, a inversibilidade é garantida na matriz codificadora, pois uma matriz é inversível quando seu determinante é diferente de zero ($det \neq 0$). O tipo da matriz codificadora escolhida condicionará na divisão e organização da matriz de pré-codificação, lembrando que para efetuar o produto de matrizes, o número de colunas da primeira que nesse caso é a matriz dividida da pré-codificação que chamaremos de B dado por $B = [b_{ij}]_{m\times n}$, tem que ser igual ao número de linhas da matriz codificadora que chamaremos de A e dado por $A = [a_{jk}]_{n\times p}$.

Continuando o nosso exemplo, escolhemos para a nossa matriz codificadora uma inversivél 3×3 dada por:

$$A = \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix}.$$

Definida a matriz codificadora, leva-se em conta que por obrigação essa terá número de linhas igual ao número de colunas da matriz pré-codificada, então os números devem ser divididos em matrizes $1 \times n$, sendo n número de linhas da codificadora. Quando os elementos da ultima matriz pré-codificada for menor que a linha da codificadora, não é preciso mudar a matriz por completo com o intuito de igualá-los, pois nem sempre será possível, então o ideal é acrescentar os números de elementos necessários adicionando o espaço (29) após o ponto até se igualarem, pois o espaço após o ponto não altera nada na mensagem.

Seguindo essa lógica baseado na nossa pré-codificação do exemplo, as matrizes pré-codificação serão dados por:

$$\begin{bmatrix} 5 & 21 & 29 \end{bmatrix} \begin{bmatrix} 1 & 13 & 15 \end{bmatrix} \begin{bmatrix} 29 & 1 & 29 \end{bmatrix} \begin{bmatrix} 13 & 1 & 20 \end{bmatrix} \begin{bmatrix} 5 & 13 & 1 \end{bmatrix} \begin{bmatrix} 20 & 9 & 3 \end{bmatrix} \begin{bmatrix} 1 & 27 & 29 \end{bmatrix}.$$

Finalizando todo o processo de multiplicação de matriz A por B, teremos assim uma matriz dada por

$$(m \times n) \times (n \times p) = m \times p,$$

onde esse matriz resultante terá o número de linhas igual ao da A e de colunas igual ao da B, e esse resultado é enviado como a mensagem, só que já encriptada. Para uma ilustração, multiplicaremos as nossas matrizes pré-codificação do exemplo pela matriz codificadora.

$$\begin{bmatrix} 5 & 21 & 29 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 13 & -18 & -43 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 13 & 15 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 3 & -4 & -19 \end{bmatrix}$$

$$\begin{bmatrix} 29 & 1 & 29 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 57 & -86 & -55 \end{bmatrix}$$

$$\begin{bmatrix} 13 & 1 & 20 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 32 & -45 & -51 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 13 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} -7 & 2 & 45 \end{bmatrix}$$

$$\begin{bmatrix} 20 & 9 & 3 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 14 & -34 & 55 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 27 & 29 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 3 & -4 & -33 \end{bmatrix}$$

a matriz resultante do produto das duas matrizes, é a nossa mensagem encriptada, o que o o receptor receberá, que é:

$$\begin{bmatrix} 13 & -18 & -43 \end{bmatrix} \begin{bmatrix} 3 & -4 & -19 \end{bmatrix} \begin{bmatrix} 57 & -86 & -55 \end{bmatrix} \begin{bmatrix} 32 & -45 & -51 \end{bmatrix}$$
$$\begin{bmatrix} -7 & 2 & 45 \end{bmatrix} \begin{bmatrix} 14 & -34 & 55 \end{bmatrix} \begin{bmatrix} 3 & -4 & -33 \end{bmatrix}.$$

O receptor para desencriptação, que é desfazer todo o processo para voltar a mensagem original, precisa primeiramente conhecer a matriz codificadora, para posteriormente calcular a sua inversa, daí, dividir o código (mensagem encriptada) em matrizes de linha igual ao coluna da inversa da codificadora, fazer o produto de código pela inversa

que será igual a pré-codificação, e por último usar a tabela para converter os números em letra, assim, terá a mensagem original. Continuando no mesmo exemplo, faremos etapa a etapa a os passos, começando com a inversa da nossa matriz A. Lembrando que a matriz inversa é dada por

$$A^{-1} = \frac{1}{detA} \cdot adjA$$

onde a $adjA$ é dada pela transposta dos cofatores de A, e representado por

$$adjA = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix}^T$$

sendo os cofatores $A_{ij} = (-1)^{i+j} det(M_{ij})$, onde M_{ij} é a submatriz de A obtida eliminando a $i - ésima$ linha e a $j - ésima$ coluna. Assim, calculando a inversa da nossa matriz do exemplo teremos:

$$A = \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} \Rightarrow detA = 1(-4+3) - (-2)(4-3) + 2(1-1) \Rightarrow detA = 1.$$

$$adjA = \begin{bmatrix} (-1)^{1+1}(-4+3) & (-1)^{1+2}(4-3) & (-1)^{1+3}(1-1) \\ (-1)^{2+1}(8+2) & (-1)^{2+2}(-4-2) & (-1)^{2+3}(-1+2) \\ (-1)^{3+1}(-6-2) & (-1)^{3+2}(3+2) & (-1)^{3+3}(1-2) \end{bmatrix} = \begin{bmatrix} -1 & -1 & 0 \\ -10 & -6 & 1 \\ -8 & -5 & -1 \end{bmatrix}^T$$

$$= \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix},$$

por fim, a nossa matriz inversa é dada por

$$A^{-1} = \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix},$$

depois, fazer o produto de A^{-1} com as matrizes da mensagem encriptada.

$$\begin{bmatrix} 13 & -18 & -43 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 21 & 29 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -4 & -19 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 13 & 15 \end{bmatrix}$$

$$\begin{bmatrix} 57 & -86 & -55 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 29 & 1 & 29 \end{bmatrix}$$

$$\begin{bmatrix} 32 & -45 & -51 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 13 & 1 & 20 \end{bmatrix}$$

$$\begin{bmatrix} -7 & 2 & 45 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 13 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 14 & -34 & 55 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 20 & 9 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -4 & -33 \end{bmatrix} \times \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 27 & 29 \end{bmatrix}$$

então por fim, a nossa mensagem desencriptada é dada por:

5 21 29 1 13 15 29 1 29 13 1 20 5 13 1 20 9 3 1 27 29

Se prestarmos atenção, podemos perceber que a nova matriz resultante é a antiga matriz pré-codificada. Nisso, para ter a mensagem original na forma alfabética, basta usamos a tabela e converter os números em letras correspondente, e lembrando que o espaço após o ponto não altera em nada. No fim, a nossa mensagem desencriptada fica:

5	21	29	1	13	15	29	1	29	13	1	20	5	13	1	20	9	3	1	27
E	U	-	A	M	O	-	A	-	M	A	T	E	M	Á	T	I	C	A	.

2.2.4 Criptografia RSA

Este método é denomina de RSA segundo Coutinho (2005, p. 3) baseando nas iniciais dos nomes dos seus criadores, sendo o R. L. Rivest, A. Shamir e L. Adleman, e é um dos mais usados em aplicações comerciais atualmente. Este método para encriptar uma mensagem, através do seu método de chave pública, como já dito, quando envolve o

código é necessário antes de tudo fazer uma pré-codificação, que é simplesmente converter as letras que compõem a mensagem em sequências simbólica ou numéricas, mas, no caso do RSA, a sequência é numérica, onde toda a mensagem passa a ser uns números antes e depois de encriptá-lo.

A tabela de pré-codificação pode ficar a critério de emissor e receptor, uma vez que de qualquer modo organizado, dará para fazer a volta. Assim, apresentaremos a nossa tabela para o presente método. Com a tabela feita, só resta fazer as devidas substituições das letra pelos respetivos números correspondente, que por fim serão divididos em blocos decimais que representam cada letra.

Tabela 4 – Pré codificação do método RSA

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
P	Q	R	S	T	U	V	W	X	Y	Z	.	,	-	≫
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

Fonte: Elaborada pelo autor.

Os quatro últimos números da nossa tabela representam respetivamente: o número 36, o ponto final ou ponto na mesma linha, o 37 representa a vírgula para marcar uma pausa e separa as expressões, o 38 representa o espaço entre as letras e que separa uma palavra da outra, e o último que é o 39 representa um novo paragrafo. Finalizando essa etapa, entramos propriamente na encriptação por RSA, onde o primeiro passo se dá pela escolha de dois números primos distintos chamados de **p** e **q** cujo o produto é igual a **n**, ($\mathbf{p} \cdot \mathbf{q} = \mathbf{n}$). Na escolha de **p** e **q** tem que ter em mente que **n** que é o produto entre os dois tem que ser maior que todos os blocos ($\mathbf{n} > \mathbf{b}$) para que o processo seja inversível.

Antes de apresentar um exemplo, vamos fixar umas notações e definições importantes. Começando pela congruência, pois dois números inteiros ($\mathbb{Z}$) a e b são ditos congruentes módulo n, também inteiro $\mathbb{Z}$, quando a diferença $(a - b)$ é múltiplo de n e escreve-se

$$a \equiv b \ (mod \ n).$$

A congruência gozam das seguintes propriedades.

Proposição 2.1 *Seja a, b, c, n números inteiros então.*

a) **Reflexiva**. $a \equiv a \ (mod \ n)$.

b) **Simetrica**. *Se* $a \equiv b \ (mod \ n)$ *então* $b \equiv a \ (mod \ n)$.

c) **Transitiva**. *Se* $a \equiv b \ (mod \ n)$ *e* $b \equiv c \ (mod \ n)$ *então* $a \equiv c \ (mod \ n)$.

Demostração: Para a), veja que $a - a = 0$ é múltiplo de n, pois zero (0) é múltiplo de qualquer número inteiro. Logo $a \equiv a(modn)$.

Para b) Se $a \equiv b \ (mod \ n)$, pela definição $a - b$ é múltiplo de n, então $b - a = -(a - b)$ é múltiplo de n, o que implica que $b \equiv a \ (mod \ n)$.

Por fim, para c) Suponha que $a \equiv b \ (mod \ n)$ e $b \equiv c \ (mod \ n)$, logo pela definição temos

$a-b$ e $b-c$ são múltiplos de n. Somando as duas teremos $(a-b)+(b-c) = a-b+b-c = a-c$ é ainda múltiplo de n, logo por definição $a \equiv c \ (mod\ n)$.

Continuando, aplicaremos um exemplo para demostrar como é feito a pré-codificação.

Exemplo 2.3 *Neste exemplo, começaremos logo com a pré-codificação da mensagem "EU AMO A MATEMÁTICA" e, prosseguiremos desenvolvendo-o após cada etapa explicada.*

E	U	-	A	M	O	-	A	-	M	A	T	E	M	Á	T	I	C	A	.
14	30	38	10	22	24	38	10	38	22	10	29	14	22	10	29	18	12	10	36

Tomemos os dois primos distintos p e q em que $p = 11$ e $q = 13$, sendo o produto entre eles a chave da nossa mensagem.

$$p \times q = 11 \times 13 \Rightarrow n = 143$$

Conhecendo o **n** não implicará automaticamente em conhecer o **p** e o **q** e para desencriptar a mensagem com base nesse método, precisará em algum etapa conhecer esses dois primos distintos. A próxima e última etapa para encriptação, é a escolha de um número denominado λ que é dado pelo menor primo que não divide o resultado da multiplicação de $[(p-1)\cdot(q-1)]$, feito tudo isso, a codificação é feita de bloco em bloco, pegando cada bloco representado por b e elevar ao mesmo número natural λ com o proposito de descobrir o seu resto da divisão a modulo n, que é:

$$b^{\lambda} \equiv a \ (mod\ n).$$

Para cada bloco b da pré-codificação pegada, encontraremos um a correspondente, que serão diferentes para todos os b diferentes. O total desses a encontrados, serão a nossa mensagem na forma encriptada.

Continuando o nosso exemplo tendo

$$[(p-1)\cdot(q-1)] = [(11-1)\cdot(13-1)] = [(10)\cdot(12)] = 120$$

e neste caso o menor primo que não divide o 120 é o 7, então assim temos que $\lambda = 7$. Sendo este o último passo, podemos dar inicio a encriptação da mensagem iniciando por primeiro bloco da pré-codificação.

$14^7 \equiv a \ (mod\ 143) \Rightarrow 14^7 \equiv (14^2)^3 \cdot 14 \equiv (53^2)\cdot 53 \cdot 14 \equiv (-51)\cdot 53 \cdot 14 \equiv 14 \cdot 14 \equiv 53 \Rightarrow 14^7 \equiv 53 \ (mod\ 143)$

$30^7 \equiv a \ (mod\ 143) \Rightarrow 30^7 \equiv (30^2)^3 \cdot 30 \equiv (42^2)\cdot 42 \cdot 30 \equiv (48)\cdot 42 \cdot 30 \equiv 14 \cdot 30 \equiv 134 \Rightarrow 30^7 \equiv 134 \ (mod\ 143)$

$38^7 \equiv a \ (mod\ 143) \Rightarrow 38^7 \equiv (38^2)^3 \cdot 38 \equiv (14)^3 \cdot 38 \equiv 27 \cdot 38 \equiv 25 \Rightarrow 38^7 \equiv 25 \ (mod\ 143)$

$10^7 \equiv a \ (mod\ 143) \Rightarrow 10^7 \equiv (10^2)^3 \cdot 10 \equiv (100)^3 \cdot 10 \equiv (43)^2 \cdot 43 \cdot 10 \equiv (-10) \cdot 43 \cdot 10 \equiv (-100) \cdot 43 \equiv (-43) \cdot 43 \equiv -(-10) \Rightarrow 10^7 \equiv 10 \ (mod\ 143)$

$22^7 \equiv a \ (mod\ 143) \Rightarrow 22^7 \equiv (22^2)^3 \cdot 22 \equiv (55)^3 \cdot 22 \equiv (55)^2 \cdot 55 \cdot 22 \equiv 22 \cdot 55 \cdot 22 \equiv 55 \cdot 55 \equiv 22 \Rightarrow 22^7 \equiv 22 \ (mod\ 143)$

$24^7 \equiv a \ (mod\ 143) \Rightarrow 24^7 \equiv (24^2)^3 \cdot 24 \equiv (4)^3 \cdot 24 \equiv (4)^2 \cdot 4 \cdot 24 \equiv (-45) \cdot 4 \equiv -(-106) \equiv 106 \Rightarrow 24^7 \equiv 106 \ (mod\ 143)$

$38^7 \equiv a \ (mod\ 143) \Rightarrow 38^7 \equiv (38^2)^3 \cdot 38 \equiv (14)^3 \cdot 38 \equiv 27 \cdot 38 \equiv 25 \Rightarrow 38^7 \equiv 25 \ (mod\ 143)$

$10^7 \equiv a \ (mod\ 143) \Rightarrow 10^7 \equiv (10^2)^3 \cdot 10 \equiv (100)^3 \cdot 10 \equiv (43)^2 \cdot 43 \cdot 10 \equiv (-10) \cdot 43 \cdot 10 \equiv (-100) \cdot 43 \equiv (-43) \cdot 43 \equiv -(-10) \Rightarrow 10^7 \equiv 10 \ (mod\ 143)$

$38^7 \equiv a \ (mod\ 143) \Rightarrow 38^7 \equiv (38^2)^3 \cdot 38 \equiv (14)^3 \cdot 38 \equiv 27 \cdot 38 \equiv 25 \Rightarrow 38^7 \equiv 25 \ (mod\ 143)$

$22^7 \equiv a \ (mod\ 143) \Rightarrow 22^7 \equiv (22^2)^3 \cdot 22 \equiv (55)^3 \cdot 22 \equiv (55)^2 \cdot 55 \cdot 22 \equiv 22 \cdot 55 \cdot 22 \equiv 55 \cdot 55 \equiv 22 \Rightarrow 22^7 \equiv 22 \ (mod\ 143)$

$10^7 \equiv a \ (mod\ 143) \Rightarrow 10^7 \equiv (10^2)^3 \cdot 10 \equiv (100)^3 \cdot 10 \equiv (43)^2 \cdot 43 \cdot 10 \equiv (-10) \cdot 43 \cdot 10 \equiv (-100) \cdot 43 \equiv (-43) \cdot 43 \equiv -(-10) \Rightarrow 10^7 \equiv 10 \ (mod\ 143)$

$29^7 \equiv a \ (mod\ 143) \Rightarrow 29^7 \equiv (29^2)^3 \cdot 29 \equiv (-17)^3 \cdot 29 \equiv (-17)^2 \cdot (-17) \cdot 29 \equiv 3 \cdot (-17) \cdot 29 \equiv 3 \cdot (-493) \equiv 3 \cdot (-64) \equiv -192 \equiv -(-94) \Rightarrow 29^7 \equiv 94 \ (mod\ 143)$

$14^7 \equiv a \ (mod\ 143) \Rightarrow 14^7 \equiv (14^2)^3 \cdot 14 \equiv (53^2) \cdot 53 \cdot 14 \equiv (-51) \cdot 53 \cdot 14 \equiv 14 \cdot 14 \equiv 53 \Rightarrow 14^7 \equiv 53 \ (mod\ 143)$

$22^7 \equiv a \ (mod\ 143) \Rightarrow 22^7 \equiv (22^2)^3 \cdot 22 \equiv (55)^3 \cdot 22 \equiv (55)^2 \cdot 55 \cdot 22 \equiv 22 \cdot 55 \cdot 22 \equiv 55 \cdot 55 \equiv 22 \Rightarrow 22^7 \equiv 22 \ (mod\ 143)$

$10^7 \equiv a \ (mod\ 143) \Rightarrow 10^7 \equiv (10^2)^3 \cdot 10 \equiv (100)^3 \cdot 10 \equiv (43)^2 \cdot 43 \cdot 10 \equiv (-10) \cdot 43 \cdot 10 \equiv (-100) \cdot 43 \equiv (-43) \cdot 43 \equiv -(-10) \Rightarrow 10^7 \equiv 10 \ (mod\ 143)$

$29^7 \equiv a \ (mod\ 143) \Rightarrow 29^7 \equiv (29^2)^3 \cdot 29 \equiv (-17)^3 \cdot 29 \equiv (-17)^2 \cdot (-17) \cdot 29 \equiv 3 \cdot (-17) \cdot 29 \equiv 3 \cdot (-493) \equiv 3 \cdot (-64) \equiv -192 - (-94) \Rightarrow 29^7 \equiv 94 \ (mod\ 143)$

$18^7 \equiv a \ (mod\ 143) \Rightarrow 18^7 \equiv (18^2)^3 \cdot 18 \equiv (38)^3 \cdot 18 \equiv (38)^2 \cdot 38 \cdot 18 \equiv 14 \cdot \cdot 38 \cdot 18 \equiv (-40) \cdot 18 \equiv 138 \Rightarrow 18^7 \equiv 138 \ (mod\ 143)$

$12^7 \equiv a \ (mod\ 143) \Rightarrow 29^7 \equiv (12^2)^3 \cdot 12 \equiv (1)^3 \cdot 12 \equiv 12 \Rightarrow 12^7 \equiv 12 \ (mod\ 143)$

$10^7 \equiv a \ (mod\ 143) \Rightarrow 10^7 \equiv (10^2)^3 \cdot 10 \equiv (100)^3 \cdot 10 \equiv (43)^2 \cdot 43 \cdot 10 \equiv (-10) \cdot 43 \cdot 10 \equiv (-100) \cdot 43 \equiv (-43) \cdot 43 \equiv -(-10) \Rightarrow 10^7 \equiv 10 \ (mod\ 143)$

$36^7 \equiv a \ (mod\ 143) \Rightarrow 36^7 \equiv (36^2)^3 \cdot 36 \equiv (9)^3 \cdot 36 \equiv 14 \cdot 36 \equiv 75 \Rightarrow 36^7 \equiv 75 \ (mod\ 143)$

Assim, a nossa mensagem “EU AMO A MATEMÁTICA”encriptada através do método

RSA é:

53 134 25 10 22 106 25 10 25 22 10 94 53 22 10 94 138 12 10 75

A mensagem chega ao seu receptor legítimos em blocos formados pelas congruência de a com a letra pré-codificada encontrado através do resto da divisão, e ele, para desencriptá-la precisa conhecer os inteiros primos distinto p e q, e com base nestas criar a chave de decodificação que denominamos de d diferente da de codificação e dado por:

$$d \cdot \lambda = 1 \ [mod(p-1) \cdot (q-1)]$$

seguindo o exemplo temos que $p = 11$, $q = 13$ e $\lambda = 7$, então

$$d \cdot 7 \equiv 1 \ [mod(10) \cdot (12)] \Rightarrow d \cdot 7 \equiv 1 \ (mod \ 120)$$

calculando a inversa de 7, teremos que

$$d \equiv 103 \ (mod \ 120) \Rightarrow d = 103.$$

Encontrando o d, faremos o processo similar a da encriptação, lembrando que tínhamos os blocos b da pré-codificação e transformamos-a em a, agora transformaremos essas a em b da seguinte forma:

$$a^d \equiv b \ (mod \ n) \ ou \ a^d \equiv b \ (mod \ 143).$$

O total dos blocos b encontrados representa a mensagem original na forma pré-codificada, então o último passo será utilizar a mesma tabela de pré-codificação para converter os devidos números pelas suas respetivas letras correspondentes, e assim, teremos a mensagem propriamente. Assim, fecharemos o nosso exemplo.

$53^{103} \equiv b \ (mod \ 143) \Rightarrow 53^{103} \equiv (53^2)^{51} \cdot 53 \equiv (51^2)^{25} \cdot 53 \cdot (-51) \equiv (27^2)^{12} \cdot 14 \cdot 27 \equiv (10^2)^6 \cdot (-51) \equiv (53^2)^3 \cdot (-51) \equiv 51^2 \cdot (-51) \cdot (-51) \equiv 27 \cdot 27 \equiv 14 \Rightarrow 53^{103} \equiv 14 \ (mod \ 143)$

$134^{103} \equiv b \ (mod \ 143) \Rightarrow 134^{103} \equiv (134^2)^{51} \cdot 134 \equiv (62^2)^{25} \cdot 134 \cdot (-62) \equiv (17^2)^{12} \cdot (-14) \cdot (-17) \equiv (3^6)^2 \cdot (-48) \equiv (14)^2 \cdot (-48) \equiv 53 \cdot (-48) \equiv -(-30) \equiv 30 \Rightarrow 134^{103} \equiv 30 \ (mod \ 143)$

$25^{103} \equiv b \ (mod \ 143) \Rightarrow 25^{103} \equiv (25^2)^{51} \cdot 25 \equiv (53^2)^{25} \cdot 53 \cdot 25 \equiv (51^2)^{12} \cdot (-51) \cdot 38 \equiv (27^2)^6 \cdot 64 \equiv (14^2)^3 \cdot 64 \equiv 53^2 \cdot 53 \cdot 64 \equiv (-51) \cdot (-40) \equiv 38 \Rightarrow 25^{103} \equiv 38 \ (mod \ 143)$

$10^{103} \equiv b \ (mod \ 143) \Rightarrow 10^{103} \equiv (10^2)^{51} \cdot 10 \equiv (43^2)^{25} \cdot 10 \cdot (-43) \equiv (10^2)^{12} \cdot (-1) \cdot (-10) \equiv ((-43)^2)^6 \cdot 10 \equiv ((-10)^2)^3 \cdot 10 \equiv 43^3 \cdot 10 \cdot (-43) \equiv (-10) \cdot (-1) \equiv 10 \Rightarrow 10^{103} \equiv 10 \ (mod \ 143)$

$22^{103} \equiv b \ (mod \ 143) \Rightarrow 22^{103} \equiv (22^2)^{51} \cdot 22 \equiv (55^2)^{25} \cdot 55 \cdot 22 \equiv (22^2)^{12} \cdot 22 \cdot 66 \equiv (55^2)^6 \cdot 22 \equiv$

$(22^2)^3 \cdot 22 \equiv 55^2 \cdot 55 \cdot 22 \equiv 22 \cdot 66 \equiv 22 \Rightarrow 22^{103} \equiv 22 \ (mod\ 143)$

$106^{103} \equiv b \ (mod\ 143) \Rightarrow 106^{103} \equiv (-37)^{103} \equiv (37^2)^{51} \cdot (-37) \equiv (61^2)^{25} \cdot (-61) \cdot (-37) \equiv (3^6)^4 \cdot 3 \cdot (-31) \equiv (14^2)^2 \cdot 50 \equiv 53^2 \cdot 50 \equiv (-51) \cdot 50 \cdot -(-24) \equiv 24 \Rightarrow 106^{103} \equiv 24 \ (mod\ 143)$

$25^{103} \equiv b \ (mod\ 143) \Rightarrow 25^{103} \equiv (25^2)^{51} \cdot 25 \equiv (53^2)^{25} \cdot 53 \cdot 25 \equiv (51^2)^{12} \cdot (-51) \cdot 38 \equiv (27^2)^6 \cdot 64 \equiv (14^2)^3 \cdot 64 \equiv 53^2 \cdot 53 \cdot 64 \equiv (-51) \cdot (-40) \equiv 38 \Rightarrow 25^{103} \equiv 38 \ (mod\ 143)$

$10^{103} \equiv b \ (mod\ 143) \Rightarrow 10^{103} \equiv (10^2)^{51} \cdot 10 \equiv (43^2)^{25} \cdot 10 \cdot (-43) \equiv (10^2)^{12} \cdot (-1) \cdot (-10) \equiv ((-43)^2)^6 \cdot 10 \equiv ((-10)^2)^3 \cdot 10 \equiv 43^3 \cdot 10 \cdot (-43) \equiv (-10) \cdot (-1) \equiv 10 \Rightarrow 10^{103} \equiv 10 \ (mod\ 143)$

$25^{103} \equiv b \ (mod\ 143) \Rightarrow 25^{103} \equiv (25^2)^{51} \cdot 25 \equiv (53^2)^{25} \cdot 53 \cdot 25 \equiv (51^2)^{12} \cdot (-51) \cdot 38 \equiv (27^2)^6 \cdot 64 \equiv (14^2)^3 \cdot 64 \equiv 53^2 \cdot 53 \cdot 64 \equiv (-51) \cdot (-40) \equiv 38 \Rightarrow 25^{103} \equiv 38 \ (mod\ 143)$

$22^{103} \equiv b \ (mod\ 143) \Rightarrow 22^{103} \equiv (22^2)^{51} \cdot 22 \equiv (55^2)^{25} \cdot 55 \cdot 22 \equiv (22^2)^{12} \cdot 22 \cdot 66 \equiv (55^2)^6 \cdot 22 \equiv (22^2)^3 \cdot 22 \equiv 55^2 \cdot 55 \cdot 22 \equiv 22 \cdot 66 \equiv 22 \Rightarrow 22^{103} \equiv 22 \ (mod\ 143)$

$10^{103} \equiv b \ (mod\ 143) \Rightarrow 10^{103} \equiv (10^2)^{51} \cdot 10 \equiv (43^2)^{25} \cdot 10 \cdot (-43) \equiv (10^2)^{12} \cdot (-1) \cdot (-10) \equiv ((-43)^2)^6 \cdot 10 \equiv ((-10)^2)^3 \cdot 10 \equiv 43^3 \cdot 10 \cdot (-43) \equiv (-10) \cdot (-1) \equiv 10 \Rightarrow 10^{103} \equiv 10 \ (mod\ 143)$

$94^{103} \equiv b \ (mod\ 143) \Rightarrow 94^{103} \equiv (-94)^{103} \equiv (49^2)^{51} \cdot (-49) \equiv (30^2)^{25} \cdot (-30) \cdot (-49) \equiv (42^2)^{12} \cdot 42 \cdot 40 \equiv (48^2)^6 \cdot (-36) \equiv (16^2)^3 \cdot (-36) \equiv 30^2 \cdot (-30) \cdot (-36) \equiv 42 \cdot (-64) \equiv -(-29) \equiv 29 \Rightarrow 94^{103} \equiv 29 \ (mod\ 143)$

$53^{103} \equiv b \ (mod\ 143) \Rightarrow 53^{103} \equiv (53^2)^{51} \cdot 53 \equiv (51^2)^{25} \cdot 53 \cdot (-51) \equiv (27^2)^{12} \cdot 14 \cdot 27 \equiv (10^2)^6 \cdot (-51) \equiv (53^2)^3 \cdot (-51) \equiv 51^2 \cdot (-51) \cdot (-51) \equiv 27 \cdot 27 \equiv 14 \Rightarrow 53^{103} \equiv 14 \ (mod\ 143)$

$22^{103} \equiv b \ (mod\ 143) \Rightarrow 22^{103} \equiv (22^2)^{51} \cdot 22 \equiv (55^2)^{25} \cdot 55 \cdot 22 \equiv (22^2)^{12} \cdot 22 \cdot 66 \equiv (55^2)^6 \cdot 22 \equiv (22^2)^3 \cdot 22 \equiv 55^2 \cdot 55 \cdot 22 \equiv 22 \cdot 66 \equiv 22 \Rightarrow 22^{103} \equiv 22 \ (mod\ 143)$

$10^{103} \equiv b \ (mod\ 143) \Rightarrow 10^{103} \equiv (10^2)^{51} \cdot 10 \equiv (43^2)^{25} \cdot 10 \cdot (-43) \equiv (10^2)^{12} \cdot (-1) \cdot (-10) \equiv ((-43)^2)^6 \cdot 10 \equiv ((-10)^2)^3 \cdot 10 \equiv 43^3 \cdot 10 \cdot (-43) \equiv (-10) \cdot (-1) \equiv 10 \Rightarrow 10^{103} \equiv 10 \ (mod\ 143)$

$94^{103} \equiv b \ (mod\ 143) \Rightarrow 94^{103} \equiv (-94)^{103} \equiv (49^2)^{51} \cdot (-49) \equiv (30^2)^{25} \cdot (-30) \cdot (-49) \equiv (42^2)^{12} \cdot 42 \cdot 40 \equiv (48^2)^6 \cdot (-36) \equiv (16^2)^3 \cdot (-36) \equiv 30^2 \cdot (-30) \cdot (-36) \equiv 42 \cdot (-64) \equiv -(-29) \equiv 29 \Rightarrow 94^{103} \equiv 29 \ (mod\ 143)$

$138^{103} \equiv b \ (mod\ 143) \Rightarrow 138^{103} \equiv (-5)^{103} \equiv (5^4)^{21} \cdot (-5) \equiv (53^2)^{12} \cdot 53 \cdot 18 \equiv ((-53)^2)^6 \cdot (-47) \equiv (27^2)^3 \cdot 47 \equiv 14^3 \cdot (-47) \equiv 27 \cdot (-47) \cdot -(-18) \equiv 18 \Rightarrow 138^{103} \equiv 18 \ (mod\ 143)$

$12^{103} \equiv b \ (mod\ 143) \Rightarrow 12^{103} \equiv (12^2)^{51} \cdot (12) \equiv (1)^{51} \cdot 12 \equiv 1 \cdot 12 \equiv 12 \Rightarrow 12^{103} \equiv 12 \ (mod\ 143)$

$10^{103} \equiv b \ (mod\ 143) \Rightarrow 10^{103} \equiv (10^2)^{51} \cdot 10 \equiv (43^2)^{25} \cdot 10 \cdot (-43) \equiv (10^2)^{12} \cdot (-1) \cdot (-10) \equiv ((-43)^2)^6 \cdot 10 \equiv ((-10)^2)^3 \cdot 10 \equiv 43^3 \cdot 10 \cdot (-43) \equiv (-10) \cdot (-1) \equiv 10 \Rightarrow 10^{103} \equiv 10 \ (mod\ 143)$

$75^{103} \equiv b \ (mod\ 143) \Rightarrow 75^{103} \equiv (75^2)^{51} \cdot 75 \equiv (48^2)^{25} \cdot 75 \cdot 48 \equiv (16^2)^{12} \cdot 16 \cdot 25 \equiv$

$((-30)^2)^6 \cdot (-29) \equiv (42^2)^3 \cdot (-29) \equiv 48^2 \cdot 48 \cdot (-29) \equiv 16 \cdot 38 \equiv 36 \Rightarrow 75^{103} \equiv 36\ (mod\ 143)$.

Portanto, a nossa mensagem desencriptada em blocos é dada por:

14	30	38	10	22	24	38	10	38	22	10	29	14	22	10	29	18	12	10	36

Analisando coluna a coluna, percebe-se que voltamos a ter as mesmas colunas da pré-codificação. Nisto, para termos a mensagem original na forma alfabética, basta usamos a Tabela 4 e converter os números em letras correspondentes. Assim, voltaremos a nossa mensagem original que é:

14	30	38	10	22	24	38	10	38	22	10	29	14	22	10	29	18	12	10	36
E	U	-	A	M	O	-	A	-	M	A	T	E	M	Á	T	I	C	A	.

3 ATIVIDADES COM CRIPTOGRAFIA EM SALA DE AULA

Antes de entrarmos nas atividades com criptografia a serem desenvolvidas na sala de aula, precisamos primeiramente ter em mente quais assuntos essas atividades abordam, depois, quais conteúdos destes assuntos serão essenciais no estudo desta atividade. Feito isso, o uso da criptografia desempenhará um papel auxiliador e motivacional na aprendizagem dos alunos, pois a curiosidade em saber codificar e decodificar as mensagens implicaram em motivação para o aprendizado do tal conteúdo pela tamanha curiosidade que ela é capaz de gerar nos alunos.

Para tal, o próprio conteúdo matemático em si, precisa antes de tudo, e de um modo geral, ser ensinado e bem definido pelo professor, assim, depois de uma apresentação de um mínimo de noção sobre o conteúdo da parte dos alunos já com resolução de exemplos básicos, o professor pode se por a uma interrogação bastante utilizada nesses níveis de ensino, que o famoso fato de "onde eu aplicarei isso na minha vida?", a partir desta interrogação, pode-se apresentar a criptografia como uma das aplicações dependendo do conteúdo a ser ministrado.

Como o foco é centralizado no aperfeiçoamento do conteúdo ensinado envolvido no tal método criptográfico, as etapas matemáticas devem ser bem especificadas para que a sua relevância torne-se notória para os alunos, e também, deve ser explicitados os passos e apresentados os devidos assuntos matemáticos que servem de sustento para a execução do tal passo. Em síntese, é fundamental deixar o aluno ciente de que aprender essas criptografias implicará em aprender a matemática por trás do método.

A organização e divisão da turma fica a critério do professor, mas, será melhor que essa organização ou divisão fosse feita em grupos, assim, gerando mais interação aluno-aluno e promovendo um novo meio de aprendizagem, pois segundo o Colaço (2004, p.339, *apud* DAMIANI 2008) as crianças, ao trabalharem juntas, orientam, apoiam, dão respostas e inclusive avaliam e corrigem a atividade do colega, com o qual dividem a parceria do trabalho. Sem contar que a partir deste modelo, eles perdem a complexidade em fazer certos questionamentos uma vez que não seria escutado por toda a turma como seria se fosse o caso para o professor.

3.1 ATIVIDADES

As atividades a serem apresentados a seguir, são modelos sugestivos, que o professor ao aplicá-los, pode fazer algumas alterações de acordo com o seu objetivo. E algumas destas atividades foram baseados em outros trabalhos.

3.1.1 Cifra de Transposição

Começaremos com atividades utilizando o método de **Cifra de Transposição**. O presente método não utiliza diretamente a matemática para sua (des)encriptação, mas, baseado na dissertação de (GANASSOLI e SCHANKOSKI, 2015), dá para criar umas atividades motivadora a partir deste método para fortalecer o aprendizado de um determinado assunto matemático. Para tal feito, foi utilizado a analise combinatória com enfase em permutações, já que o referido método utiliza uma ideia semelhante.

Atividade 1: Com os grupos já divididos, o professor pode propor que cada grupo escrevesse uma palavra com no mínimo cinco (5) letras e sem repetições, e depois, trocar as palavras entre grupos, de modo que ninguém fique com a própria palavra. No final, o professor pede para que, usando a mensagem recebida, calcular quantas possibilidades diferentes existem de criptografá-la, lembrando que a própria mensagem não pode ser uma das opções.

Assunto a abordar: Permutação Simples

Solução: Suponha que uma das palavras selecionada foi a ESCOLA, então teremos:

- seis (6) possibilidades para escolher a primeira letra, seja qualquer que for a letra;
- cinco (5) possibilidades para escolher a segunda letra dos cinco (5) restantes, sendo que não pode ser a primeira;
- quatro (4) possibilidades para escolher a terceira letra dos quatro (4) restantes, pois não pode ser o mesmo escolhido como segundo nem o primeiro;
- três (3) possibilidades para escolher a quarta letra dos três (3) restantes que são diferentes dos já escolhidos;
- duas (2) possibilidades para escolher a quinta letra, não sendo os demais já escolhidos;
- uma (1) possibilidades para escolher a segunda letra, sendo a única restante.

Visto no principio fundamental da contagem, o número das permutações possíveis são dados pelo produto das possibilidades, sendo assim, fica:

$$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6! = 720.$$

assim, 720 são todas os possíveis permutações da palavra ESCOLA, incluindo a própria palavra, como ela não deve fazer parte, então teremos $720 - 1 = 719$. Conclui-se que há 719 maneiras diferente de criptografar a palavra ESCOLA.

Atividade 2: Continuando, dessa vez o professor pede que o mesmo grupo escolha uma palavra com no mínimo cinco (5) letras em que pelo menos uma delas se repete. Depois, trocar as palavras entre os grupos, de modo que ninguém fique com a própria frase. No final, o professor pede para que, usando a mensagem recebida, calcular quantas possibilidades diferentes existem de criptografá-la, sem a opção da própria palavra.

Assunto a abordar: Permutação com Repetição
Solução: Suponha que uma das palavras selecionada foi o CALCULAR. Sendo assim, primeiramente deve-se analisar as repetições, que num total de oito (8) letras, são:

- C=2
- A=2
- L=2

$$P_8^{2,2,2} = \frac{8!}{2! \cdot 2! \cdot 2!\cdot} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 4 \cdot 3 \cdot 2!}{2 \cdot 1 \cdot 2!} = \frac{20160}{4} = 5040.$$

5040 são todas as possíveis permutações da palavra CALCULAR, incluindo a própria palavra, como ele não deve fazer parte, então teremos $5040 - 1 = 5039$. Conclui-se que há 5039 maneiras diferente de criptografar a palavra CALCULAR.

3.1.2 Cifra de César

Para atividades na sala de aula utilizando o método do imperador Júlio César **(Cifra de César)**, utilizaremos o método aplicado a função, baseado no trabalho de Roseto e Meira (2020), pois, o próprio método não utiliza matemática no seu processo, mas, como anteriormente mostrado, dá para aplicar a ideia de função a este método e instigar o aluno à aprender o tal importante conteúdo. Vale ressaltar que a função precisa ser bijetora, para garantir o processo inverso.
Atividade 1: Para primeira atividade baseado neste método, o professor pode propor uma bem mais simples e de caráter individual, onde se pede para encriptar uma palavra que pode ser a ESCOLA e a função codificadora dada por $f(x) = x + 3$. Aí utilizando a tabela, os alunos vão fazer a pré-codificação e depois a encriptação da mensagem.
Assunto a abordar: Função polinomial do primeiro grau
Solução: Utilizando a tabela Tabela 2 de pré-codificação, a palavra escola fica:

E	S	C	O	L	A
14	28	12	24	21	10

$$f(14) = 14 + 3 = 17 \qquad f(24) = 24 + 3 = 27$$
$$f(28) = 28 + 3 = 31 \qquad f(21) = 21 + 3 = 24$$
$$f(12) = 12 + 3 = 15 \qquad f(10) = 10 + 3 = 13$$

a palavra escola na forma encriptada fica:

$$[17; 31; 15; 27; 24; 13]$$

Atividade 2: Dividido os grupos, o professor pode propor que cada grupo forme uma frase com no mínimo três (3) palavras e no máximo cinco (5), para não ser tão curto e

nem tão longo ao ponto de roubar muito tempo. Utilizando uma mesma tabela de pré-codificação de letra em número (Tabela 2) para toda a turma, cada grupo deve converter a sua mensagem em número, em seguida, o professor atribui uma função para cada grupo encriptar a sua mensagem. Feito isso, a mensagem já pré-codificada é trocado entre os grupos de modo que ninguém fique com a própria mensagem, assim, usando a pré-codificação e a função, cada grupo vai encriptar a nova mensagem.

Assunto a abordar: Função Polinomial do Primeiro Grau

Solução: Suponhamos que uma das frases é a "O CONHECIMENTO É A BASE DE TUDO"e a função é $f(x) = \frac{4x-60}{2}$, teremos primeiro a pré-codificação:

Tabela 5 – Método de César: Atividade 2

	O		C	O	N	H	E	C	I	M	E	N	T	O	
	24		12	24	23	17	14	12	18	22	14	23	29	24	
É		A		B	A	S	E		D	E		T	U	D	O
14		10		11	10	28	14		13	14		29	30	13	24

Fonte: Elaborada pelo autor.

Encriptando a essa mensagem utilizando função teremos:

$f(24) = \frac{4\cdot 24-60}{2} = \frac{36}{2} = 18$
$f(12) = \frac{4\cdot 12-60}{2} = \frac{-12}{2} = -6$
$f(24) = \frac{4\cdot 24-60}{2} = \frac{36}{2} = 18$
$f(23) = \frac{4\cdot 23-60}{2} = \frac{32}{2} = 16$
$f(17) = \frac{4\cdot 17-60}{2} = \frac{8}{2} = 4$
$f(14) = \frac{4\cdot 14-60}{2} = \frac{-4}{2} = -2$
$f(12) = \frac{4\cdot 12-60}{2} = \frac{-12}{2} = -6$
$f(18) = \frac{4\cdot 18-60}{2} = \frac{12}{2} = 6$
$f(22) = \frac{4\cdot 22-60}{2} = \frac{28}{2} = 14$
$f(14) = \frac{4\cdot 14-60}{2} = \frac{-4}{2} = -2$
$f(23) = \frac{4\cdot 23-60}{2} = \frac{32}{2} = 16$
$f(29) = \frac{4\cdot 29-60}{2} = \frac{56}{2} = 28$
$f(24) = \frac{4\cdot 24-60}{2} = \frac{36}{2} = 18$

$f(14) = \frac{4\cdot 14-60}{2} = \frac{-4}{2} = -2$
$f(10) = \frac{4\cdot 10-60}{2} = \frac{-20}{2} = -10$
$f(11) = \frac{4\cdot 11-60}{2} = \frac{-16}{2} = -8$
$f(10) = \frac{4\cdot 10-60}{2} = \frac{-20}{2} = -10$
$f(28) = \frac{4\cdot 28-60}{2} = \frac{52}{2} = 26$
$f(14) = \frac{4\cdot 14-60}{2} = \frac{-4}{2} = -2$
$f(13) = \frac{4\cdot 13-60}{2} = \frac{-8}{2} = -4$
$f(14) = \frac{4\cdot 14-60}{2} = \frac{-4}{2} = -2$
$f(29) = \frac{4\cdot 29-60}{2} = \frac{56}{2} = 28$
$f(30) = \frac{4\cdot 30-60}{2} = \frac{60}{2} = 30$
$f(13) = \frac{4\cdot 13-60}{2} = \frac{-8}{2} = -4$
$f(24) = \frac{4\cdot 24-60}{2} = \frac{36}{2} = 18.$

A mensagem na forma encriptada é dada por: [18;-6;18;16;4;-2;-6;6;14;-2;16;28;18;-2;-10;-8;-10;26;-2;-4;-2;28;30;-4;18].

Atividade 3: Com os mesmos grupos, o professor orienta que a mensagem já encriptada anteriormente, fosse enviada para um grupo diferente do que a criou. Assim, os grupos com as mensagens encriptada recebidas, vão desencriptografá-las e lê-las.

Assunto a abordar: Inversa da Função Polinomial do Primeiro Grau.

Solução: A nossa mensagem encriptada é dada por: [18;-6;18;16;4;-2;-6;6;14;-2;16;28;-2;-10;-8;-10;26;-2;-4;-2;28;30;-4;18] e a nossa função inversa será: $f^{-1}(y) = \frac{2y+60}{4}$. Aplicando os valores da mensagem encriptada recebida na função inversa teremos.

$f^{-1}(18) = \frac{2\cdot 18+60}{2} = \frac{96}{4} = 24$
$f^{-1}(-6) = \frac{2\cdot(-6)+60}{2} = \frac{48}{4} = 12$
$f^{-1}(18) = \frac{2\cdot 18+60}{2} = \frac{96}{4} = 24$
$f^{-1}(16) = \frac{2\cdot 16+60}{2} = \frac{92}{4} = 23$
$f^{-1}(4) = \frac{2\cdot 4+60}{2} = \frac{68}{4} = 17$
$f^{-1}(-2) = \frac{2\cdot(-2)+60}{2} = \frac{56}{4} = 14$
$f^{-1}(-6) = \frac{2\cdot(-6)+60}{2} = \frac{48}{4} = 12$
$f^{-1}(6) = \frac{2\cdot 6+60}{2} = \frac{72}{4} = 18$
$f^{-1}(14) = \frac{2\cdot 14+60}{2} = \frac{88}{4} = 22$
$f^{-1}(-2) = \frac{2\cdot(-2)+60}{2} = \frac{56}{4} = 14$
$f^{-1}(16) = \frac{2\cdot 16+60}{2} = \frac{92}{4} = 23$
$f^{-1}(28) = \frac{2\cdot 28+60}{2} = \frac{116}{4} = 29$
$f^{-1}(18) = \frac{2\cdot 18+60}{2} = \frac{96}{4} = 24$
$f^{-1}(-2) = \frac{2\cdot(-2)+60}{2} = \frac{56}{4} = 14$
$f^{-1}(-10) = \frac{2\cdot(-10)+60}{2} = \frac{40}{4} = 10$
$f^{-1}(-8) = \frac{2\cdot(-8)+60}{2} = \frac{44}{4} = 11$
$f^{-1}(-10) = \frac{2\cdot(-10)+60}{2} = \frac{40}{4} = 10$
$f^{-1}(26) = \frac{2\cdot 26+60}{2} = \frac{112}{4} = 28$
$f^{-1}(-2) = \frac{2\cdot(-2)+60}{2} = \frac{56}{4} = 14$
$f^{-1}(-4) = \frac{2\cdot(-4)+60}{2} = \frac{52}{4} = 13$
$f^{-1}(-2) = \frac{2\cdot(-2)+60}{2} = \frac{56}{4} = 14$
$f^{-1}(28) = \frac{2\cdot 28+60}{2} = \frac{116}{4} = 29$
$f^{-1}(30) = \frac{2\cdot 30+60}{2} = \frac{120}{4} = 30$
$f^{-1}(-4) = \frac{2\cdot(-4)+60}{2} = \frac{52}{4} = 13$
$f^{-1}(18) = \frac{2\cdot 18+60}{2} = \frac{96}{4} = 24.$

A nossa mensagem desencriptada é:

$$[24; 12; 24; 23; 17; 14; 12; 18; 22; 14; 23; 29; 24; 14; 10; 11; 10; 28; 14; 13; 14; 29; 30; 13; 24]$$

usando a tabela de conversão (Tabela 2), chegaremos a mensagem "O CONHECIMENTO É A BASE DE TUDO", então a mensagem está desencriptada.

3.1.3 Matriz

Para atividades utilizando matriz, seguindo todo conceito acima apresentado, vale lembrar que a matriz codificadora deve ser uma quadrada e inversível ($det \neq 0$), e a matriz pré-codificadora deve ter número de colunas igual ao número de linhas da codificadora, que é um conceito da multiplicação.

Atividade 1: Para a primeira atividade, o professor pode propor uma simples e de caráter individual pedindo o seguinte: Suponhamos que você gosta da matemática mas tem problemas como decorar, e precisa criar uma palavra passe "alfabética"e não quer correr o risco de perdê-la e nem deixá-la cair nas mãos das outras pessoas. Então você encripta a palavra passe e guarda a matriz pré-codificadora e a codificadora, e no caso de esquecimento, é só fazer a desencriptação. Para não correr o risco de criar uma matriz não inversível, o professor pode cria duas matrizes, uma 2×2 e uma 3×3 para ser utilizado de acordo com números de letras que compõem a palavra passe.

Assunto a abordar: Multiplicação de Matrizes

Solução: Suponha que uma das palavras passe fosse "avidaebela". A palavra é composta por dez (10) letras, então o melhor concorrente é uma matriz codificadora 2×2 dada por:

$$A = \begin{bmatrix} 2 & 3 \\ -3 & -4 \end{bmatrix},$$

fazendo a pré-codificação que para este método consiste na substituição alfabética em numérica utilizando a Tabela 3, fica:

A	V	I	D	A	E	B	E	L	A
01	22	09	04	01	05	02	05	12	01

Feito isso, só resta separar a pré-codificação em matrizes 1×2 e fazer as devidas multiplicações.

$$\begin{bmatrix} 1 & 22 \end{bmatrix} \times \begin{bmatrix} 2 & 3 \\ -3 & -4 \end{bmatrix} = \begin{bmatrix} -64 & -85 \end{bmatrix}$$

$$\begin{bmatrix} 9 & 4 \end{bmatrix} \times \begin{bmatrix} 2 & 3 \\ -3 & -4 \end{bmatrix} = \begin{bmatrix} 6 & 11 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 5 \end{bmatrix} \times \begin{bmatrix} 2 & 3 \\ -3 & -4 \end{bmatrix} = \begin{bmatrix} -13 & -17 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 5 \end{bmatrix} \times \begin{bmatrix} 2 & 3 \\ -3 & -4 \end{bmatrix} = \begin{bmatrix} -11 & -14 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 1 \end{bmatrix} \times \begin{bmatrix} 2 & 3 \\ -3 & -4 \end{bmatrix} = \begin{bmatrix} 21 & 32 \end{bmatrix}$$

assim, temos a palavra chave na forma encriptada,

-64 -85 6 11 -13 -17 -11 -14 21 32

que para conhecê-la na forma alfabética, precisa-se conhecer antes a matriz codificadora, calcular a sua inversa e por ultimo fazer a multiplicação da encriptada com a inversa.

Atividade 2: Para esta atividade, o professor pode seguir com a ideia de dividir a turma em grupos, depois, pedir que cada grupo crie uma frase. Em seguida, usando a tabela pré-codificadora (Tabela 3), que façam a pré-codificação e passem essa mensagem pré-codificada para outro grupo. Para evitar problemas com matriz inversível, e baseando na melhor opção para divisão da pré-codificadora, o professor pode passar uma matriz codificadora para cada grupo.

Assunto a abordar: Multiplicação de Matrizes

Solução: Suponha que uma das frases foi a "SOMOS OS MELHORES", e a melhor opção para matriz codificadora é uma 3x3 dado por:

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

onde teremos a seguinte pré-codificação:

S	O	M	O	S	-	O	S	-	M	E	L	H	O	R	E	S	.
19	15	13	15	19	29	15	19	29	13	5	12	8	15	18	5	19	27

Assim, as matrizes pré-codificação são:

$$\begin{bmatrix} 19 & 15 & 13 \end{bmatrix} \begin{bmatrix} 15 & 19 & 29 \end{bmatrix} \begin{bmatrix} 15 & 19 & 29 \end{bmatrix} \begin{bmatrix} 13 & 5 & 12 \end{bmatrix} \begin{bmatrix} 8 & 15 & 18 \end{bmatrix} \begin{bmatrix} 5 & 19 & 27 \end{bmatrix}.$$

Efetuando a multiplicação chegaremos que:

$$\begin{bmatrix} 19 & 15 & 13 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 45 & 92 & 62 \end{bmatrix}$$

$$\begin{bmatrix} 15 & 19 & 29 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 73 & 136 & 82 \end{bmatrix}$$

$$\begin{bmatrix} 15 & 19 & 29 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 73 & 136 & 82 \end{bmatrix}$$

$$\begin{bmatrix} 13 & 5 & 12 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 37 & 67 & 35 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 15 & 18 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 44 & 85 & 56 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 19 & 27 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 59 & 110 & 70 \end{bmatrix}$$

assim, as matrizes resultantes formam a mensagem encriptada.

Atividade 3: Esta atividade pode ser a continuação da anterior, onde com as mensagens já encriptadas, o professor pode pedir que os grupos passassem as suas mensagens encriptadas e a matriz codificadora, levando em conta que essas mensagens não devem voltar aos grupos que o criou. Daí pedir que o novo grupo desencriptasse a mensagem e transformá-la na forma original.

Assunto a abordar: Inversa de uma Matriz

Solução: Primeiramente, calcula-se a inversa da matriz A e depois multiplica-se pela

matriz resultante, que é a nossa mensagem encriptada. Lembrando que a matriz inversa é dada por: $A^{-1} = \frac{1}{detA} \cdot adjA$

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \Rightarrow detA = 1(1-6) - 2(0-4) + 1(0-2) \Rightarrow detA = 1.$$

$$adjA = \begin{bmatrix} (-1)^{1+1}(1-6) & (-1)^{1+2}(0-4) & (-1)^{1+3}(0-2) \\ (-1)^{2+1}(2-3) & (-1)^{2+2}(1-2) & (-1)^{2+3}(3-4) \\ (-1)^{3+1}(4-1) & (-1)^{3+2}(2-0) & (-1)^{3+3}(1-0) \end{bmatrix} = \begin{bmatrix} -5 & 4 & -2 \\ 1 & -1 & 1 \\ 3 & -2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix}$$

$$A^{-1} = \frac{1}{detA} \cdot adjA = \frac{1}{1} \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} \Rightarrow A^{-1} = \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix}.$$

Efetuando a multiplicação da matriz encriptada pela inversa chega-se que:

$$\begin{bmatrix} 45 & 92 & 62 \end{bmatrix} \times \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 19 & 15 & 13 \end{bmatrix}$$

$$\begin{bmatrix} 73 & 136 & 82 \end{bmatrix} \times \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 15 & 19 & 29 \end{bmatrix}$$

$$\begin{bmatrix} 73 & 136 & 82 \end{bmatrix} \times \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 15 & 19 & 29 \end{bmatrix}$$

$$\begin{bmatrix} 37 & 67 & 35 \end{bmatrix} \times \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 13 & 5 & 12 \end{bmatrix}$$

$$\begin{bmatrix} 44 & 85 & 56 \end{bmatrix} \times \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 15 & 18 \end{bmatrix}$$

$$\begin{bmatrix} 59 & 110 & 70 \end{bmatrix} \times \begin{bmatrix} -5 & 1 & 3 \\ 4 & -1 & -2 \\ -2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 19 & 27 \end{bmatrix}$$

a matriz resultante dado por:

$$\begin{bmatrix} 19 & 15 & 13 \end{bmatrix} \begin{bmatrix} 15 & 19 & 29 \end{bmatrix} \begin{bmatrix} 15 & 19 & 29 \end{bmatrix} \begin{bmatrix} 13 & 5 & 12 \end{bmatrix} \begin{bmatrix} 8 & 15 & 18 \end{bmatrix} \begin{bmatrix} 5 & 19 & 27 \end{bmatrix}$$

é a mensagem desencriptada, utilizando a tabela (Tabela 3) de pré-codificação chegamos em:

19	15	13	15	19	29	15	19	29	13	5	12	8	15	18	5	19	27
S	O	M	O	S	-	O	S	-	M	E	L	H	O	R	E	S	.

3.1.4 RSA

Vale ressaltar que está que o conteúdo deste método vai além do ensino básico (fundamental e médio), mas pode ser adaptado como incentivo à aprendizado. O método RSA utiliza a congruência linear, que tem a ver com o resto da divisão, assim, podemos adaptá-lo para a aprendizagem da divisão com restos (divisão não exata), não só, também para a potenciação. Mas, como envolve uma potenciação muito grande, fica a critério do professor ver se será ou não produtivo e facultativo para com os seus alunos.

Atividade 1: Para esta atividade, como alguns dos passos do método vão além do ensino básico, o professor pode já resolver estes e passá-los pronto, deixando assim só a parte de calcular os restos da divisão que em outras palavras é a mensagem encriptada ou desencriptada. Suponhamos que a atividade é individual e valendo recompensas par os cinco (5) primeiros que terminaram a encriptar uma mensagem.
Assunto a abordar: Divisão inteira ou resto da divisão
Solução: Primeiramente o professor pede para encriptar uma palavra ou uma mensagem, e suponhamos que foi a palavra "AMOR". E depois fornece os primos p e q tal que $p = 3$ e $q = 5$, assim $n = 15$. Para o menor primo que não divide $(p-1)(q-1) = 2 \cdot 4 = 8$, temos o 3, que será $\lambda = 3$. Tendo todas essas informações, pode-se naturalmente encriptar a mensagem, sendo que a pré-codificação feita através de Tabela 4 é dada por:

A	M	O	R
10	22	24	27

Vale ressaltar que o conceito de potenciação também podia ser aplicado como incentivo à este método, mas, como envolve números grandes, pode mais atrapalhar do que ajudar. Então para este feito, o professor pode liberar que os alunos usassem a

calculadora para calcular as potências e depois dividí-las manualmente, uma vez que o foco é aperfeiçoar a divisão.

então, $10^3 \equiv a \ (mod\ 15)$ (calcular o resto da divisão de 10^3 por 15)
temos assim $\frac{1000}{15}$ que fazendo a nossa divisão natural, chegaremos que é igual a 66 tendo como resto menor que 15 igual a 10, então assim dizemos que:

$$10^3 \equiv 10 \ (mod\ 15).$$

e $22^5 \equiv a \ (mod\ 15)$ (calcular o resto da divisão de 22^3 por 15)
temos assim $\frac{10648}{15}$ que fazendo a nossa divisão natural, chegaremos que é igual a 70 tendo como resto menor que 15 igual a 13, então assim dizemos que:

$$22^3 \equiv 13 \ (mod\ 15).$$

o $24^3 \equiv a \ (mod\ 15)$ (calcular o resto da divisão de 24^3 por 15)
temos assim $\frac{13824}{15}$ que fazendo a nossa divisão natural, chegaremos que é igual a 921 tendo como resto menor que 15 igual a 9, então assim dizemos que:

$$24^3 \equiv 9 \ (mod\ 15).$$

por último, $27^3 \equiv a \ (mod\ 15)$ (calcular o resto da divisão de 10^3 por 15)
temos assim $\frac{19683}{15}$ que fazendo a nossa divisão natural, chegaremos que é igual a 1312 tendo como resto menor que 15 igual a 3, então assim dizemos que:

$$27^3 \equiv 3 \ (mod\ 15).$$

assim, a mensagem amor na forma encriptada é dada por: [10;13;9;3].

Atividade 2: Divididos em grupos, o professor pode sugerir que cada grupo crie uma frase, e trocar as mensagens entre grupos. Onde cada grupo vai fazer a pré-codificação baseando na Tabela 4 e encriptar a mensagem. Depois, os grupos vão passar a mensagem encriptada para um novo grupo que vai fazer a desencriptação e converter a mensagem na original. Lembrando que o professor precisa primeiramente fornecer a chave de encriptação e desencriptação.
Assunto a abordar: Divisão inteira ou resto da divisão
Solução: Suponha que uma das mensagens é a "A MATEMÁTICA ESTÁ EM TUDO", e a chave de encriptação é (55,5) em que $n = 55$ e $\lambda = 5$. A pré-codificação é dada por: Fazendo os devidos cálculos chegaremos que:

Tabela 6 – RSA: Pré-codificação Atividade 2

A	-	M	A	T	E	M	Á	T	I	C	A	-
10	38	22	10	29	14	22	10	29	18	12	10	38
E	S	T	A	-	E	M	-	T	U	D	O	
14	28	29	10	38	14	22	38	29	30	13	24	

Fonte: Elaborada pelo autor.

$10^5 \equiv 10\ (mod\ 55)$ $18^5 \equiv 2\ (mod\ 55)$ $14^5 \equiv 49\ (mod\ 55)$
$38^5 \equiv 37\ (mod\ 55)$ $12^5 \equiv 23\ (mod\ 55)$ $22^5 \equiv 33\ (mod\ 55)$
$22^5 \equiv 33\ (mod\ 55)$ $10^5 \equiv 10\ (mod\ 55)$ $38^5 \equiv 37\ (mod\ 55)$
$10^5 \equiv 10\ (mod\ 55)$ $38^5 \equiv 37\ (mod\ 55)$ $29^5 \equiv 24\ (mod\ 55)$
$29^5 \equiv 24\ (mod\ 55)$ $14^5 \equiv 49\ (mod\ 55)$ $30^5 \equiv 50\ (mod\ 55)$
$14^5 \equiv 49\ (mod\ 55)$ $28^5 \equiv 7\ (mod\ 55)$ $13^5 \equiv 52\ (mod\ 55)$
$22^5 \equiv 33\ (mod\ 55)$ $29^5 \equiv 24\ (mod\ 55)$ $24^5 \equiv 19\ (mod\ 55)$
$10^5 \equiv 10\ (mod\ 55)$ $10^5 \equiv 10\ (mod\ 55)$
$29^5 \equiv 24\ (mod\ 55)$ $38^5 \equiv 37\ (mod\ 55)$

a mensagem na forma encriptada é dada por:

$$10; 37; 33; 10; 24; 49; 33; 10; 24; 2; 23; 10; 37; 49; 7; 24; 10; 37; 49; 33; 37; 24; 50; 52; 19$$

Atividade 3: Esta atividade pode ser uma inversa da segunda, onde o professor pode pedir que os grupos passassem as mensagens encriptadas para um novo grupo sem que seja o grupo que o criou. Tendo como a chave de desencriptação (55,27) em que $n = 55$ e $\lambda = 27$. Desencriptando chegaremos que:

$10^{27} \equiv 10\ (mod\ 55)$ $2^{27} \equiv 18\ (mod\ 55)$ $49^{27} \equiv 14\ (mod\ 55)$
$37^{27} \equiv 38\ (mod\ 55)$ $23^{27} \equiv 12\ (mod\ 55)$ $33^{27} \equiv 22\ (mod\ 55)$
$33^{27} \equiv 22\ (mod\ 55)$ $10^{27} \equiv 10\ (mod\ 55)$ $37^{27} \equiv 38\ (mod\ 55)$
$10^{27} \equiv 10\ (mod\ 55)$ $37^{27} \equiv 38\ (mod\ 55)$ $24^{27} \equiv 29\ (mod\ 55)$
$24^{27} \equiv 29\ (mod\ 55)$ $49^{27} \equiv 14\ (mod\ 55)$ $50^{27} \equiv 30\ (mod\ 55)$
$49^{27} \equiv 14\ (mod\ 55)$ $7^{27} \equiv 28\ (mod\ 55)$ $52^{27} \equiv 13\ (mod\ 55)$
$33^{27} \equiv 22\ (mod\ 55)$ $24^{27} \equiv 29\ (mod\ 55)$ $19^{27} \equiv 24\ (mod\ 55)$.
$10^{27} \equiv 10\ (mod\ 55)$ $10^{27} \equiv 10\ (mod\ 55)$
$24^{27} \equiv 29\ (mod\ 55)$ $37^{27} \equiv 38\ (mod\ 55)$

A mensagem na forma desencriptada é dada por:

$$10; 38; 22; 10; 29; 14; 22; 10; 29; 18; 12; 10; 38; 14; 28; 29; 10; 38; 14; 22; 38; 29; 30; 13; 24$$

utilizando a Tabela 4 para converter, chegaremos na mensagem original que é:

Tabela 7 – RSA: Conversão Atividade 3

10	38	22	10	29	14	22	10	29	18	12	10	38
A	-	M	A	T	E	M	Á	T	I	C	A	-
14	28	29	10	38	14	22	38	29	30	13	24	
E	S	T	A	-	E	M	-	T	U	D	O	

Fonte: Elaborada pelo autor.

4 CONCLUSÃO

No decorrer do trabalho tivemos a oportunidade de ver um pouco da história da criptografia, o seu desenvolvimento ao longo do tempo, paralelo ao desenvolvimento humano e tecnológico, as adaptações e modificações sofridas na busca de melhoria de qualidade de suas proteções. Vimos a matemática por trás dos métodos que o usam e como pode ser aplicado aos métodos que não o usa diretamente, e como tirar um proveito à prol do ensino aprendizado através destas criptografias.

Levando em consideração o fato de ensino com situações problemas objetivando a deixar o aluno em pé de igualdade com uma das situações reais em que o conteúdo aprendido ou ensino se encaixa, a criptografia torna-se uma forte concorrente pensando na perspectiva tecnológica. Pois com o avanço da era digital ou tecnológica, segundo TIC Kids Online Brasil (2019, p. 23) no ano de 2019, 89% da população entre 9 e 17 anos se envolvem diretamente com a tecnologia, e essa faixa etária é o dominante do ensino básico, que é o nosso público alvo. Então oferecendo uma ferramenta necessária para pessoas em busca do mesmo, tornará mais interessante a necessidade de aprendizado destas, assim, despertar a atenção dos alunos em aprender sobre criptografia pode não ser um problema.

Para este feito, o trabalho buscou juntar alguns tipos de criptografias com o propósito de oferecer ao professor uma ferramenta aplicável à sala de aula em busca de melhorias de aprendizado e a motivação dos seus alunos relativo a conteúdo de permutação simples e com elementos repetidos, divisões não exatas, multiplicação de matrizes e matriz inversa e a função do primeiro grau e a sua inversa. Além de fornecer essas ferramentas, o trabalho deu uma breve explanação sobre a criptografia para o professor que não têm o conhecimento sobre o tal.

REFERÊNCIAS

COUTINHO, S. C. Números Inteiros e RSA. Rio de Janeiro: IMPA, 2005.

CGI.BR. TIC Kids Online Brasil [livro eletrônico]: Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil 2019. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

DAMIANI, M. F. Entendendo o trabalho colaborativo em educação e revelando seus benefícios. Educar em revista, p. 213-230, 2008.

EDUCALINGO. Skytale. [s.i]: [s.n], [2021?]. Disponível em: <educalingo.com/pl/dic-pl/skytale> . Acesso em: 20 fev. 2021.

GANASSOLI, Ana Paula; SCHANKOSKI, Fernanda Ricardo. Criptografia e Matemática. 2015. 103 f. Tese de Doutorado. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). UFPR. Curitiba, PR, 2015.

LIMA, E.L. Ensino Médio da Matemática.Gazeta de matemática, p. 42-47. Rio de Janeiro: IMPA, 2003.

MORENO, E.; PEREIRA, F.; CHIARAMONTE, R. Criptografia em Software e Hardware. 1st edition. ed. São Paulo: Novatec, 2005.

ROSSETO, C. K. Criptografia como recurso didático: uma proposta metodológica aos professores de matemática. 2018. 95 f. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). UNESP. São José do Rio Preto, SP, 2018.

TONCHE, J. C. S. O desinteresse dos alunos das séries iniciais do ensino fundamental pela educação escolar: causas e possíveis intervenções. 2014. 19 f. Dissertação Mestrado (Curso de Especialização em Coordenação Pedagógica). UFPR. Curitiba, PR, 2014.