UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

GUILHERME HENRIQUE LIMA SILVA

ENSINO DE MATEMÁTICA BÁSICA USANDO CRIPTOGRAFIA

JUAZEIRO DO NORTE
2023

GUILHERME HENRIQUE LIMA SILVA

ENSINO DE MATEMÁTICA BÁSICA USANDO CRIPTOGRAFIA

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Dra. Clarice Dias de Albuquerque

JUAZEIRO DO NORTE
2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Cariri
Sistema de Bibliotecas

S586e Silva, Guilherme Henrique Lima.
Ensino de matemática básica usando criptografia/ Guilherme Henrique Lima Silva – 2023.
61 f. il. color.; 30 cm.
(Inclui bibliografia, p.59-60).

Dissertação (Mestrado) – Universidade Federal do Cariri, Centro de Ciências e Tecnologia, Programa de Pós-graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2023.

Orientadora: Dra. Clarice Dias de Albuquerque.

1. Lúdico. 2. Matemática. 3. Cifra. I. Título.

CDD 510.7

Bibliotecário: João Bosco Dumont do Nascimento – CRB 3/1355

GUILHERME HENRIQUE LIMA SILVA

ENSINO DE MATEMÁTICA BÁSICA USANDO CRIPTOGRAFIA

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada em: 21 de agosto de 2023.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br CLARICE DIAS DE ALBUQUERQUE
Data: 27/10/2023 16:30:33-0300
Verifique em https://validar.iti.gov.br

Profª. Drª. Clarice Dias de Albuquerque
UFCA

Documento assinado digitalmente
gov.br VALDINES LEITE DE SOUSA JUNIOR
Data: 28/10/2023 15:08:27-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Valdinês Leite de Sousa Júnior
UFCA

Documento assinado digitalmente
gov.br ANDERSON JOSE DE OLIVEIRA
Data: 27/10/2023 19:30:38-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Anderson José de Oliveira
UNIFAL-MG

Para minha mãe e meu pai.

Agradecimentos

Gostaria de expressar meus sinceros agradecimentos. Em primeiro lugar, agradeço a Deus por conceder-me sabedoria, saúde e determinação ao longo do mestrado. À minha esposa, Geovana Soares de Alencar, agradeço pelo apoio durante todo o processo de conclusão do mestrado. Aos meus pais, Maria Alcilene Silva e Fernando Oliveira Silva, agradeço pela minha educação e pelos incentivos aos estudos desde a minha infância.

Gostaria de agradecer à orientadora, Clarice, por aceitar me guiar neste trabalho, contribuindo com incentivos, sugestões e ideias. Agradeço também por sua paciência ao longo do processo. Aos meus colegas de mestrado e a todos que, de alguma forma, contribuíram para trilhar esse caminho, meu sincero agradecimento.

Por fim, expresso minha gratidão à UFCA e ao programa PROFMAT por proporcionarem oportunidades de mestrado a muitos professores, tornando-nos mais qualificados para o ensino.

RESUMO

A matemática desempenha um papel fundamental em nosso cotidiano, mesmo que muitas vezes passe despercebida. Nos últimos anos, a comunicação por meio da internet, seja por celulares, computadores ou outros dispositivos, tornou-se comum. As mensagens trocadas pelos usuários são enviadas criptografadas, de forma a garantir que o conteúdo não possa ser lido caso alguém tente invadir a comunicação. Esse processo ocorre de maneira mais discreta nos dias de hoje. No entanto, essa prática existe há muito tempo e remonta à era dos reis e rainhas, muitos anos antes de Cristo. Naquela época, os reis se comunicavam com seus aliados de longa distância por meio de mensagens enviadas por mensageiros. Aqueles que conseguiram manter suas mensagens apenas entre o remetente e o destinatário, por meio de uma escrita secreta, conseguiram manter seus reinos intactos mesmo que suas mensagens fossem interceptadas. Por outro lado, aqueles que utilizavam uma escrita secreta fraca permitiam que seus inimigos obtivessem informações valiosas contidas nas mensagens, o que poderia levar à ruína de seus reinos. A matemática desempenhou um papel crucial na decifração dessas mensagens criptografadas no passado e passou a ser fundamental na criptografia atual. Este trabalho aborda a história da criptografia, com vários métodos e a utilização da matemática para decifrar e criptografar mensagens, sendo o produto final atividades que podem ser utilizadas em sala de aula para tornar a aplicação da matemática mais relevante e lúdica para os alunos, demonstrando a importância da matemática na garantia de uma comunicação segura.

Palavras-chave: Lúdico. Matemática. Cifra.

ABSTRACT

Mathematics plays a fundamental role in our daily lives, even though it often goes unnoticed. In recent years, communication through the internet, whether via cell phones, computers, or other devices, has become commonplace. The messages exchanged by users are sent encrypted, ensuring that the content cannot be read if someone tries to intercept the communication. This process is less explicit nowadays. However, this practice has existed for a long time, dating back to the era of kings and queens, many years before Christ. During that time, kings communicated with their distant allies through messages sent by messengers. Those who managed to keep their messages solely between the sender and the receiver, using secret writing, could keep their kingdoms intact even if their messages were intercepted. On the other hand, those who used weak secret writing allowed their enemies to obtain valuable information contained in the messages, which could lead to the ruin of their kingdoms. Mathematics played a crucial role in deciphering these encrypted messages in the past and has become essential in modern cryptography. This work addresses the history of cryptography, with various methods and the use of mathematics to decipher and encrypt messages. The end product is activities that can be used in the classroom to make the application of mathematics more relevant and engaging for students, demonstrating the importance of mathematics in ensuring secure communication.

Keywords: Ludic. Mathematics. Cipher.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Atualmente, com o avanço da tecnologia, as pessoas ganharam várias comodidades. Antigamente, para realizar compras era necessário sair de casa e ir em lojas físicas, mas com o surgimento das lojas on-line, as pessoas podem fazer compras sem sair de casa, basta ter um celular ou computador com acesso à internet, em seguida, acessar o site desejado, realizar o cadastro com seus dados pessoais e, assim, pesquisar os produtos para finalizar a compra, podendo optar por várias formas de pagamento como cartão de crédito, débito, boleto, entre outros.

Essa comodidade não existe somente para compras, também é possível utilizar o *Internet Banking*, para *smartphones* e computadores, que tem como objetivo realizar consultas de saldos e extratos bancários, pagar boletos, efetuar transações bancárias por Pix, Ted e outras funções, o que evita a necessidade da pessoa se locomover de casa até uma agência bancária.

A tecnologia também proporcionou comunicações a longa distância com rapidez e segurança, por meios das mídias sociais tais como *WhatsApp*, *Instagram*, *E-mail*, *Skype*, entre outros.

Para garantir a privacidade dos dados pessoais nas transações bancárias, em sites confiáveis, assim como para manter o sigilo das conversas entre o remetente e o destinatário, são utilizadas técnicas de Criptografia.

De acordo com Carneiro (2017), “A palavra criptografia originou-se da fusão de duas palavras gregas - kryptos = secreto, oculto e graphein = escrita, escrever - significa escrita secreta”.

Vale destacar que a criptografia não é uma novidade da atualidade, ela já existe há milhares de anos, sendo utilizada por reis, rainhas, imperadores, amantes, entre outros. Essa ferramenta auxiliava na permanência dos seus reinos ou relacionamentos. No entanto, aqueles que tiveram as suas informações reveladas para pessoas não autorizadas, viram seus reinos e impérios serem dominados. E no campo do amor os amantes tinham como consequência o fim do relacionamento, ou penalidades severas que poderiam resultar em morte.

Dessa forma, observa-se que há aqueles que desejam manter a comunicação secreta, como também há os que desejam ler essas mensagens sem autorização. Assim, com o surgimento da

Criptografia, logo surge a Criptoanálise, a arte de decifrar mensagens secretas, logo, iniciando-se uma batalha entre as duas, uma luta que ocorre até os dias atuais.

Usam-se os termos *codificador* e *decodificador*, para as pessoas que tem o conhecimento do método específico que está em ação para manter a comunicação secreta, enquanto, o termo *decifrador* é dado ao interceptador que procura ler as mensagens secretas sem autorização.

Na observação das criptografias mais antigas, nota-se que poderiam ser utilizados conceitos matemáticos para decifrar as tais mensagens codificadas, que posteriormente, obteve o reconhecimento da importância dos matemáticos no tema de Criptografia. É tanto que a matemática contribuiu para umas das criptografias mais utilizada hoje, a criptografia RSA.

Tendo em vista a conexão entre essas duas áreas, o objetivo principal dessa dissertação é apresentar atividades lúdicas e com contextualização sobre a Matemática e a Criptografia, com intuito de contribuir na aprendizagem dos alunos do Ensino Fundamental II e Médio.

É comum os professores se depararem com alunos desmotivados, principalmente em relação à disciplina de Matemática, sendo um dos principais motivos, a falta de associação do conteúdo com o cotidiano. Dessa forma, procura-se utilizar a ludicidade e a contextualização, proporcionando uma aula mais atrativa para os alunos e, consequentemente, contribuindo para o processo de ensino e aprendizagem.

Para tanto, está dissertação inicia-se com o Capítulo 1, o qual discorre introdutoriamente sobre a relevância desta temática, a estruturação do trabalho, bem como algumas definições para a leitura.

Em seguida, o Capítulo 2 versa sobre a evolução da criptografia levando em consideração o contexto histórico, distinguindo a criptografia de chave privada e a de chave pública.

No Capítulo 3 é feita uma revisão dos conceitos matemáticos que podem ser utilizados nas criptografias mencionadas no Capítulo 2, ressaltando como tais conceitos podem ser introduzidos na sala de aula. Os assuntos matemáticos abordados são: Divisibilidade, Números Primos, Fatoração, Função Afim, Função Inversa e Permutação.

Já no capítulo 4, são apresentadas atividades matemáticas para serem trabalhadas em sala de aula, com intuito de motivar os alunos, por meio de um desenvolvimento reflexivo, criativo, interativo e trabalho em equipe.

As atividades apresentam oportunidades para o desenvolvimento de diversas habilidades entre os participantes, conforme destacado por Brasil (2018):

Ensino Fundamental II:

- (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.

- (EF07MA18) Resolver e elaborar problemas que possam ser representados por equações polinomiais de 1º grau, redutíveis à forma $ax + b = c$, fazendo uso das propriedades da igualdade.

- (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.

Ensino Médio:

- (EM13MAT301) Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais.
- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.
- (EM13MAT302) Construir modelos empregando as funções polinomiais de 1º ou 2º graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais.
- (EM13MAT310) Resolver e elaborar problemas de contagem envolvendo agrupamentos ordenáveis ou não de elementos, por meio dos princípios multiplicativo e aditivo, recorrendo a estratégias diversas, como o diagrama de árvore.
- (EM13MAT311) Identificar e descrever o espaço amostral de eventos aleatórios, realizando contagem das possibilidades, para resolver e elaborar problemas que envolvem o cálculo da probabilidade.

A dissertação se finaliza com o Capítulo 5 que traz as considerações finais. Além disso, os recursos para desenvolver as atividades propostas podem ser encontrados no Apêndice, após o Capítulo 5.

Capítulo 2

História da Criptografia

Neste capítulo aborda-se brevemente a história da criptografia desde a antiguidade até os dias atuais, apresentando situações envolvendo codificações e decodificações.

Durante a história das civilizações, pode-se observar que mensagens entre pessoas socialmente poderosas, tinham que manter suas conversas secretas, pois caso o conteúdo da mensagem estivesse em mãos não autorizadas, poderiam influenciar o destino de outras pessoas, povos ou até mesmo reinos da época. Esses que buscavam ter conhecimento das mensagens codificadas sem autorização, utilizavam meios de interceptá-las e em seguida tentavam decifrá-las. Era necessário muito estudo para decifrar as mensagens e esse estudo, posteriormente, ficou conhecido como Criptoanálise, e as pessoas que a fazem são chamados de criptoanalistas.

Segundo Singh (2008), "Enquanto o criptógrafo desenvolve novos métodos de escrita secreta, é o criptoanalista que luta para encontrar fraqueza nesses métodos, de modo a quebrar a mensagem secreta". Dessa forma, a Criptografia e a Criptoanálise se desenvolvem mutuamente, e ambas unidas se tornam a Criptologia.

Nas codificações utiliza-se de um *algoritmo*, o método utilizado, por exemplo, alterar a ordem das letras originais da mensagem, ou substituir por outras letras ou números ou símbolos. Após a escolha do *algoritmo*, tem-se a *chave*, que especifica os detalhes para a codificação. As chaves podem ser *simétricas* ou *assimétricas*.

Desse modo, neste capítulo são apresentadas a história da criptografia em cifras de chave simétrica e assimétrica. O texto a seguir está fundamentado nas seguintes referências (CARNEIRO, 2017), (CIMINO, 2018), (SINGH, 2008) e (COUTINHO, 2014).

2.1 Cifras de Chave Simétrica

A chave simétrica recebe esse nome, pois a chave que codifica também pode decodificar, sendo necessário mantê-la em segredo entre o remetente e o destinatário das mensagens.

2.1.1 Cifras de Transposição

A cifra de transposição consiste em desordenar as letras da mensagem, ou seja, trocar as posições das letras da mensagem.

A complexidade da cifra de transposição encontra-se na quantidade de letras da mensagem, caso a mensagem seja curta como "**SUL**", seria facilmente decifrável, pois tem-se 3! = 6 anagramas, que são: **SUL, SLU, LSU, LUS, ULS** e **USL**. No entanto, se a mensagem fosse "**Suprimento ao Sul**" seriam 15 letras, onde as letras "S" e "u" se repetem duas vezes, gerando o seguinte número de anagramas possíveis:

$$P_{15}^{2,2} = \frac{15!}{2! \cdot 2!} = 326.918.592.000.$$

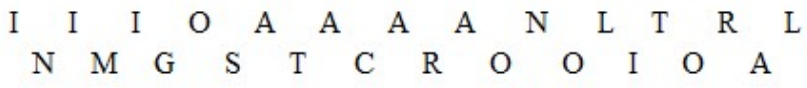
Devido às muitas possibilidades de reordenar as letras dessa mensagem, garante-se um nível maior de confiança. Mas, de acordo com Singh (2008), para que se torne efetiva a utilização desse método, o destinatário e o remetente deverão entrar em acordo antecipadamente para decidir as regras do embaralhamento e desembaralhamento das letras, ou seja, a regra para codificação e a decodificação da mensagem.

2.1.2 Cerca da Ferrovia ou Cifra do Trilho

Um método simples é conhecido por "Cerca da Ferrovia", nome utilizado por Singh (2008) e Carneiro (2017) e também conhecido pelo nome "Cifra do Trilho", utilizado por Cimino (2018). O método consiste em alternar as letras da mensagem em 2 linhas, a primeira letra na linha superior, a segunda letra na linha inferior, terceira letra na linha superior, quarta letra na linha inferior e assim por diante. Ao terminar o processo, juntam-se todas as letras da linha superior formando o bloco 1 e depois faz o mesmo com as letras da linha inferior formando o bloco 2. Por fim, juntam-se o bloco 1 e o bloco 2, lado a lado, finalizando a codificação. A seguir é apresentado um exemplo desse método.

Exemplo 1. *Mensagem: "**INIMIGOS ATACARÃO NO LITORAL**":*

Figura 2.1: Cerca da Ferrovia ou Cifra do Trilho.



Fonte: Autor.

***Bloco 1** = IIIOAAAANLTRL*
***Bloco 2** = NMGSTCROOIOA*
***Mensagem Codificada** = IIIOAAAANLTRLNMGSTCROOIOA*

O destinatário ao receber a mensagem codificada deverá revertê-la através de um processo simples: primeiro passo é saber a quantidade de letras (25 letras), o segundo passo é dividir por 2 para saber quantas letras ficará em cada linha, ($\frac{25}{2} = 12$ e resto 1), como há resto nesta divisão, essa unidade será acrescentado na primeira linha, sendo assim, a primeira linha terá $12 + 1 = 13$ letras iniciais da mensagem codificada e a segunda linha com as 12 letras restante. Depois, escrevem-se as letras da primeira linha deixando um espaço entre as letras, em seguida escrevem-se as letras da segunda linha abaixo dos espaços deixado na linha superior, ao encaixar os dois blocos por meio dos espaços tem-se a mensagem decodificada.

No método Cerca da Ferrovia, pode-se acrescentar mais que duas linhas.

Exemplo 2. *Considere a mensagem "**Matemática e Criptografia**", onde deseja-se dividir a mensagem em três linhas, como pode ser visto na Figura 2.2.*

Figura 2.2: Cerca da Ferrovia com três linhas.

M E T A R T R I
A M I E I O A A
T A C C P G F

Fonte: Autor.

Mensagem Codificada: ***METARTRIAMIEIOAATACCPGF***

Observa-se que a mensagem tem 23 letras, portanto, o destinatário para decodificá-la irá dividir 23 por 3, resultando a parte inteira em 7 e o resto igual a 2. Assim, ao sobrar duas unidades no resto, acrescenta-se uma letra na primeira linha e uma letra na segunda linha, ou seja, a primeira linha terá $7 + 1 = 8$ *letras, a segunda linha* $7 + 1 = 8$ *letras e a terceira linha* 7 *letras.*

Neste método, tem-se que o *algoritmo* é escrever a mensagem em diagonais, em seguida unir linha por linha, a chave no primeiro exemplo é dada pelas diagonais de duas linhas, enquanto no segundo exemplo, é determinada pelas diagonais de três linhas.

Todavia, esse método de criptografia é facilmente decifrável caso a mensagem seja interceptada e a pessoa reconheça o algoritmo utilizado.

2.1.3 Método Retangular

Carneiro (2017) relata uma forma de transposição mais eficaz do que a anterior, chamada "método retangular". O método consiste em primeiro escolher uma chave, que será uma palavra qualquer conhecida apenas pelo destinatário e o remetente, depois escreve-se a mensagem sob a palavra-chave, linha por linha, caso fique espaço em branco, deve-se preencher com "#". Ao terminar, enumeram-se as colunas na ordem alfabética da palavra-chave, em seguida, para

codificar a mensagem, é preciso unir as letras da mensagem da coluna numerada por 1 com as letras da mensagem da coluna numerada por 2 e assim por diante, até não sobrar mais colunas.

Para decodificar a mensagem, o destinatário deve usar a palavra-chave, primeiro para contar quantos caracteres tem a mensagem codificada e depois dividir pela quantidade de letras da chave, com isso tem-se a informação da quantidade de caracteres em cada coluna da palavra-chave. Em seguida, enumeram-se as letras da palavra-chave em ordem alfabética e depois escreve-se a mensagem codificada verticalmente, iniciando pela coluna enumerada com 1, depois com 2 e assim por diante até preencher todas as colunas. Por fim, é possível ler a mensagem horizontalmente linha por linha.

Observa-se o método apresentado no Exemplo 3, conforme Figura 2.3 a seguir.

Exemplo 3. ***Mensagem original:*** *A MATEMÁTICA É A MINHA MATÉRIA PREFERIDA.*
Chave: *ÍMPARES*

Figura 2.3: Método Retangular.

ORDEM	3	4	5	1	6	2	7
CHAVE	**I**	**M**	**P**	**A**	**R**	**E**	**S**
MENSAGEM	A	M	A	T	E	M	A
	T	I	C	A	E	A	M
	I	N	H	A	M	A	T
	E	R	I	A	P	R	E
	F	E	R	I	D	A	#

Fonte: Autor.

Tem-se, coluna 1 "TAAAI", coluna 2 "MAARA", coluna 3 "ATIEF", coluna 4 "MINRE", coluna 5 "ACHIR", coluna 6 "EEMPD" e coluna 7 "AMTE#". A mensagem codificada será a junção das letras da colunas de 1 até 7:

TAAAIMAARAATIEFMINREACHIREEMPDAMTE#

No processo de decodificação, o destinatário deve ter conhecimento da palavra-chave ***ÍMPARES****, a mensagem codificada tem 35 caracteres, a palavra-chave tem 7 letras, fazendo a divisão 35 por 7 obtém-se 5. Separa a mensagem codificada em blocos de 5 caracteres.*

TAAAI - MAARA - ATIEF - MINRE - ACHIR - EEMPD - AMTE#.

Depois, escreve-se verticalmente o primeiro bloco, ***TAAAI****, sob a primeira letra que aparece em ordem alfabética da palavra-chave, Em seguida, escreve-se o segundo bloco sob a segunda letra na ordem alfabética da palavra-chave, seguindo dessa maneira, o procedimento e o resultado será a Figura 2.4, então lê-se a mensagem horizontalmente, linha por linha.*

Figura 2.4: Decodificação do Método Retangular.

1

ORDEM	3	4	5	1	6	2	7
CHAVE	I	M	P	A	R	E	S
MENSAGEM				T			
				A			
				A			
				A			
				I			

2

ORDEM	3	4	5	1	6	2	7
CHAVE	I	M	P	A	R	E	S
MENSAGEM				T		M	
				A		A	
				A		A	
				A		R	
				I		A	

3

ORDEM	3	4	5	1	6	2	7
CHAVE	I	M	P	A	R	E	S
MENSAGEM	A			T		M	
	T			A		A	
	I			A		A	
	E			A		R	
	F			I		A	

Quadro Completo

ORDEM	3	4	5	1	6	2	7
CHAVE	I	M	P	A	R	E	S
MENSAGEM	A	M	A	T	E	M	A
	T	I	C	A	E	A	M
	I	N	H	A	M	A	T
	E	R	I	A	P	R	E
	F	E	R	I	D	A	#

Fonte: Autor.

2.1.4 Cítala

De acordo com Singh (2008), o primeiro aparelho criptográfico militar foi criado no século V a.C, utilizado pelos espartanos. Este aparelho consiste em um bastão de madeira, conhecida como **cítala** (Figura 2.5), no qual o remetente enrolava uma tira de couro ou pergaminho em volta do bastão, em seguida escrevia a mensagem ao longo do comprimento do bastão, ao terminar, desenrolava a tira, deixando a mensagem codificada, pois todas as letras da mensagem estariam fora de ordem. Por fim, o destinatário deveria ter um bastão de mesmas dimensões para enrolar a tira com a mensagem e assim conseguir decodificar a mensagem.

Figura 2.5: Cítala.

Fonte: https://pt.wikipedia.org/wiki/C%C3%ADtala#/media/Ficheiro:Skytale.png.

Em um acontecimento no ano 404 a.C, um mensageiro ensanguentado e ferido, utili-

zando a tira com a mensagem codificada como um cinturão, conseguiu encontrar Lisandro de Esparta, a quem entregou o cinturão. Lisandro por sua vez, pegou sua cítala e decodificou a mensagem. Dessa forma, Lisandro descobre que o persa Farnabazo estava planejando atacá-lo. Consequentemente, Lisandro conseguiu se preparar para o ataque e garantiu a vitória.

2.1.5 Cifras de Substituição

As cifras de substituição têm o objetivo de trocar as letras da mensagem original por outras letras, números ou símbolos.

Atualmente, em registros, tem-se que a cifra de César é a mais antiga cifra de substituição. O Imperador Romano cansado de seus mensageiros serem capturados pelos inimigos, decide mandar as mensagens codificadas. O sistema de codificação de César baseava-se na troca da letra original da mensagem por outra letra 3 casas adiante do alfabeto. Transformando essa ideia para o alfabeto da língua portuguesa, tem-se que a letra "A" seria substituída por "D", "B" por "E", "X" por "A", "Y" por "B", "Z" por "C", assim por diante, como mostra a Figura 2.6.

Figura 2.6: Cifra de César.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: Autor.

Para decodificar a mensagem secreta, basta fazer o processo reverso.

Sendo a mensagem **"A MATEMÁTICA É IMPORTANTE PARA A CRIPTOGRAFIA"** codificada através do método de cifra de César, tem-se **"D PDWHPDWLFD H LPSRUWDQWH SDUD D FULSWRJUDILD"**.

O defeito da cifra de César é que há somente 25 maneiras de transladar o alfabeto, ou seja, 25 chaves possíveis. Dessa forma, uma pessoa que conheça o algoritmo basta testar no máximo 25 chaves para que finalmente torne a mensagem legível.

Para aumentar a segurança da cifra de César pode-se permutar as letras do alfabeto para aumentar as chaves codificadoras:

$$P_{26} - 1 = 26! - 1 = 403.291.461.126.605.635.583.999.999.$$

O valor apresentado anteriormente representa a quantidade de chaves possíveis, dessa forma o interceptador não teria somente 25 chaves para testar, aumentando a segurança dessa cifra.

Em Cimino (2018), Bernardo Provenzano, chefe da máfia siciliana, foi capturado em 2006, ao usar uma variação da cifra de César. Em vez de substituir "A" por "D", ele substitui "A" por 4, "B" por 5, "C" por 6 e assim por diante. Quando as mensagens foram interceptadas pelos policiais foram facilmente decifradas.

De acordo com Singh (2008), escolher uma chave aleatória para poder codificar as mensagens poderia fazer com que o remetente e o destinatário precisassem anotar e guardar o alfabeto codificador em um papel, correndo o risco de uma pessoa roubá-lo. Então, para que ambos não precisassem ter o alfabeto codificador guardado em papel, surge a ideia de usarem uma *palavra-chave* ou uma *frase-chave*. Por exemplo, para usar **IMPERADOR** como palavra-chave, primeiro retira-se as letras repetidas **(IMPERADO)**, esse resultado será o início do alfabeto codificador, e completa o alfabeto codificador a partir da última letra da palavra-chave, veja a Figura 2.7.

Figura 2.7: Alfabeto Codificador.

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

Fonte: Autor.

Ao utilizar uma palavra-chave ou frase-chave diminui a quantidade de chaves distintas, no entanto há uma quantidade grande suficiente para dificultar a força bruta do invasor.

Este método de criptografia é simples e forte para a época, tanto que dominou o primeiro milênio a ponto de acreditarem que essa cifra era indecifrável. Porém, no século IX, os criptoanalistas iriam encontrar um atalho para que não precisassem verificar grandes quantidades de chaves.

2.1.6 Análise de Frequência

No século IX, em um grande centro intelectual em Bagdá conhecido como Casa da Sabedoria, encontrava-se o polímata Abu al-Kindî, o "filósofo dos árabes", que trabalhava em um manuscrito denominado "Da elucidação de correspondência codificada", no qual continha detalhes de como decifrar um documento pela análise de frequência, estudo do número de vezes que aparece cada letra ou grupo de letras em um texto codificado.

Abu al-Kindî ensina que, para decifrar uma mensagem codificada, o primeiro passo é reconhecer o idioma da mensagem. Uma vez identificado, busca-se um texto legível nesse mesmo idioma, de modo que ocupe pelo menos uma lauda. O processo inicia-se contando a frequência de cada letra presente nesse texto. Em seguida, faz-se o mesmo com a mensagem codificada, ou seja, contabiliza-se a frequência de cada letra. Por fim, o método de decifragem ocorre substituindo-se a primeira letra mais frequente da mensagem codificada pela letra mais frequente do texto legível, depois troca a segunda letra mais frequente da mensagem codificada pela segunda letra mais frequente do texto legível, e assim por diante até que todos os caracteres tenham sido substituídos.

A Figura 2.8, mostra a porcentagem de frequência das letras da língua portuguesa:

Esse método, facilmente, decifra as mensagens codificadas pelo o algoritmo de Júlio César. Neste momento, qualquer um que enviasse uma mensagem codificada e ela fosse interceptada,

Figura 2.8: Análise de Frequência.

Letra	Frequência (%)	Letra	Frequência (%)
A	14,63%	N	5,05%
B	1,04%	O	10,73%
C	3,88%	P	2,52%
D	4,99%	Q	1,20%
E	12,57%	R	6,53%
F	1,02%	S	7,81%
G	1,30%	T	4,34%
H	1,28%	U	4,63%
I	6,18%	V	1,67%
J	0,40%	W	0,01%
K	0,02%	X	0,21%
L	2,78%	Y	0,01%
M	4,74%	Z	0,47%

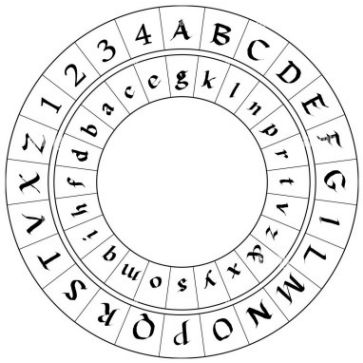
Fonte: https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html.

provavelmente teria o seu conteúdo revelado, pois, os criptoanalistas encontravam-se na vantagem da batalha.

2.1.7 Disco de Alberti e Tabela de Vigenère

Segundo Cimino (2018), em 1467, o polímata italiano Leon Battista Alberti escreveu um tratado sobre a análise de frequência. Nela continha demonstrações de como a criptografia feita por substituição de outro alfabeto desordenado era fraco. A partir disso, Alberti, percebeu que se usasse mais de um alfabeto para substituição, poderia proteger as mensagens codificadas da análise de frequência utilizada pelos criptoanalistas. Com isso, criou o Disco de Alberti, apresentado na Figura 2.9.

Figura 2.9: Disco de Alberti.



Fonte: https://www.alamy.es/disco-de-cifrado-de-alberti-obras-de-arte-este-dispositivo-fue-descrito-en-1467-por-el-criptografo-italiano-leon-battista-alberti-1404-1472-el-anillo-interior-de-lowe-image335461900.html.

Cimino (2018), descreve o disco da seguinte maneira:

> O aparelho consistia de dois discos de cobre com um eixo em comum que giravam um em relação ao outro. A borda de cada círculo era dividida em 24 células. No círculo externo, Alberti pôs as letras maiúsculas do alfabeto, uma em cada célula, omitindo “H”, “K”, “Y”. Como o alfabeto latino e italiano não tem “J”, “U” nem “W”, isso lhe dava quatro células vazias, que preencheu com os números 1 a 4. No círculo interno, pôs as letras minúsculas do alfabeto em ordem aleatória. (CIMINO, 2018, p. 38).

Para codificar a mensagem utilizando o disco de Alberti, é preciso fixar a posição inicial do disco interno na rotação estabelecida entre o remetente e o destinatário, as letras do disco externo correspondem as letras da mensagem legível, então deve-se trocá-las pelas letras correspondentes, ocasionalmente, insere-se uma letra maiúscula, indicando o novo posicionamento do disco interno. A cada giro do disco interno, obtém-se um alfabeto novo para codificar. Esse ato de utilizar mais de um alfabeto denota-se criptografia de substituição polialfabéticas, sendo as anteriores conhecidas como criptografia de substituição monoalfabéticas.

O desenvolvimento da criptografia de substituição polialfabética estava lenta, até que um diplomata francês, Blaise Vigenère, criou um sistema de 26 alfabetos para codificar as mensagens, conforme Figura 2.10.

Figura 2.10: Quadrado de Vigenère.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	**B**	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	**C**	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	**D**	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	**E**	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	**F**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	**G**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	**I**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	**J**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	**K**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	**L**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	**M**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	**N**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	**O**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	**P**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	**Q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	**R**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	**S**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	**T**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	**U**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	**V**	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	**W**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	**X**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	**Y**	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	**Z**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	**A**	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Singh (2008).

Para utilizar esse método de criptografia precisa-se de uma palavra-chave. Aqui, essa palavra será “**UFCA**”, e a mensagem a ser codificada é “**Juazeiro do Norte**”. Então, escreve-se sob a mensagem, a palavra-chave várias vezes até não restar mais letras da mensagem. A pré-codificação é apresentada na Figura 2.11.

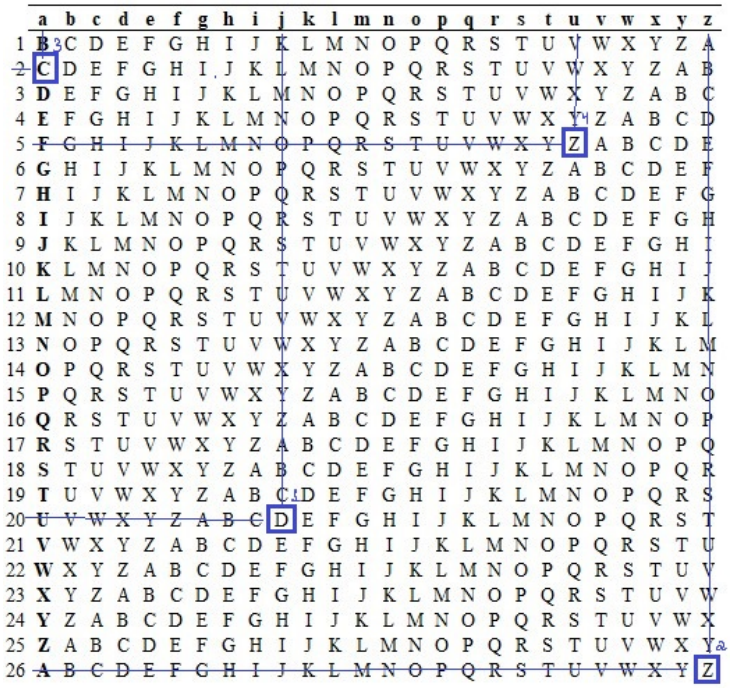
Figura 2.11: Pré-Codificação.

Mensagem:	J	U	A	Z	E	I	R	O		D	O		N	O	R	T	E							
Palavra-Chave:	**U**	**F**	**C**	**A**	**U**	**F**	**C**	**A**		**U**	**F**		**C**	**A**	**U**	**F**	**C**							

Fonte: Autor.

Depois, observa-se a primeira letra da mensagem, “J”, e a letra chave respectivamente, “**U**”, e codifica-se encontrando a letra correspondente a coluna “J” e a linha que inicia com a letra “**U**”, ou seja, a letra “D”. Análogo para as demais letras. Veja na Figura 2.12 a codificação das quatro primeiras letras da mensagem pelo quadro de Vigenère.

Figura 2.12: Codificação.



Fonte: Autor.

A mensagem completamente codificada resulta em **“DZCZYNTO XT POLYG”**. A primeira letra “E” é codificado pela letra “N”, a segunda letra “E” é codificado pela letra “G”, com isso evita-se a análise de frequência.

No entanto, seu método exigia tempo e esforço, algo negativo para a comunicação. Esse impacto fez com que exércitos em guerra continuassem utilizando a criptografia de substituição monoalfabética, a esperança estava na realização da ação do conteúdo da mensagem, antes que os criptoanalistas decifrassem, tornando-se inútil o conteúdo.

2.1.8 Cifra ADFGVX - 2 Criptografias em uma mensagem.

Durante a Primeira Guerra Mundial, os alemães já sabiam que as suas mensagens enviadas pelo rádio eram vulneráveis à interceptação, então desenvolveram novas cifras. Entre

elas, destaca-se a cifra ADFGVX.

O seu método tem duas etapas, a primeira utiliza o quadrado de Políbio que é constituído por 6 linhas e 6 colunas, designadas pelas letras ADFGVX. O quadrado é preenchido pelas 26 letras do alfabeto e os dez algarismos de 0 a 9, conforme a Figura 2.13.

Figura 2.13: O quadrado de Políbio.

	A	**D**	**F**	**G**	**V**	**X**
A	h	4	c	d	n	o
D	a	g	t	e	m	3
F	6	b	2	f	p	l
G	i	5	q	0	w	9
V	8	j	r	z	k	1
X	x	v	y	s	7	u

Fonte: Autor.

Para codificar a mensagem "*Chegaremos às 10:30*", observa-se a posição de cada caractere da mensagem em relação a linha e a coluna do quadrado de Políbio. (Figura 2.14).

Figura 2.14: Primeira codificação.

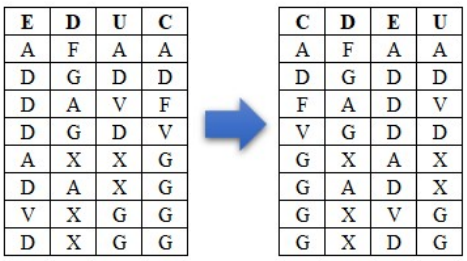
c	h	e	g	a	r	e	m	o	s	a	s	1	0	3	0
AF	**AA**	**DG**	**DD**	**DA**	**VF**	**DG**	**DV**	**AX**	**XG**	**DA**	**XG**	**VX**	**GG**	**DX**	**GG**

Fonte: Autor.

Em seguida, utiliza-se uma palavra-chave, por exemplo **EDUC**, para escrever a mensagem pré-codificada sob a mesma, no sentido horizontal, linha por linha. Esse método coincide com a Criptografia do Método Retangular já mencionado anteriormente.

Após organizar a mensagem, permuta-se as colunas em ordem alfabética da palavra-chave. (Figura 2.15).

Figura 2.15: Segunda codificação.



E	**D**	**U**	**C**
A	F	A	A
D	G	D	D
D	A	V	F
D	G	D	V
A	X	X	G
D	A	X	G
V	X	G	G
D	X	G	G

C	**D**	**E**	**U**
A	F	A	A
D	G	D	D
F	A	D	V
V	G	D	D
G	X	A	X
G	A	D	X
G	X	V	G
G	X	D	G

Fonte: Autor.

Por fim, codifica-se escrevendo a mensagem coluna por coluna.

Mensagem Codificada: ADFVGGGGFGAGXAXXADDDADVDADVDXXGG.

Cimino (2018) explica que essa cifra tem esse nome **"ADFVGX"**, porque elas são as letras mais distintas quando se coloca em código Morse, resultando em menos chance de erro ao enviar as mensagens. Posteriormente, os criptoanalistas também conseguiram decifrar.

Durante o século XIX, as comunicações expandiram-se, a invenção do telégrafo permitiu a transmissão de mensagens a longa distância, em contrapartida, pode ser interceptada facilmente. O telégrafo elétrico espalhou-se pela Europa e pelos EUA, as mensagens eram enviadas utilizando a linguagem Código Morse, criado por Samuel Morse, que se baseia na representação do alfabeto por traços e pontos, conforme Tabela 2.1. Como afirma Singh (2008), "O código Morse não é uma forma de criptografia, porque a mensagem não fica oculta. Os pontos e traços são meramente um meio de representar letras para a transmissão telegráfica. O código Morse nada mais é do que um alfabeto alternativo".

Tabela 2.1: Alfabeto e Números em Código Morse.

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

Fonte: Autor.

O motivo de utilizarem essa linguagem era por conta da facilidade de serem enviadas através de pulsos elétricos longos e curtos. Além disso, Morse criou um receptor acústico, de modo que a comunicação fosse executada através de *bips* audíveis que representavam o código Morse.

2.1.9 Máquina Enigma

Em 1918, o inventor alemão Arthur Scherbius fundou uma empresa inovadora e um de seus projetos era desenvolver os sistemas de criptografias, já que as utilizadas na Primeira Guerra Mundial se tornaram inadequadas. Então, com seus conhecimentos em engenharia elétrica, criou uma máquina para substituir o uso da codificação que utiliza lápis e papel. Pode-se dizer que era uma versão elétrica da criptografia dos discos de Alberti, sendo conhecida como Enigma, uma invenção que impactou o mundo da criptografia. (Figura 2.16).

Singh (2008), descreve a Enigma da seguinte maneira:

> [...] consiste em três elementos conectados por fios: um teclado para a entrada de cada letra do texto original, uma unidade misturadora, que cifra cada letra, transformando-a na letra correspondente da mensagem cifrada, e um mostrador consistindo em várias lâmpadas para indicar as letras do texto cifrado. (SINGH, 2008, p. 146).

Figura 2.16: A máquina Enigma.

Fonte: https://www.cryptomuseum.com/crypto/enigma/d/.

A codificação através da Enigma: O remetente tecla a letra “b”, o que envia um impulso elétrico para parte misturadora central e em seguida um sinal iluminando a letra correspondente no painel, sendo utilizada para substituição, suponha que tenha aparecido a letra “h”. Então, nesse processo, a unidade misturadora rotaciona $\frac{1}{26}$, sendo assim, ao teclar novamente a letra “b”, faz com que no final ilumine uma outra letra, diferente de “h”. Após teclar 26 letras, a unidade misturadora voltaria para sua posição inicial.

Porém, a Enigma utilizava 3 discos misturadores, cada um continha o alfabeto gravado, objetivando fazer rotações entre eles, gerando $26 \cdot 26 \cdot 26 = 17.576$ combinações possíveis. Scherbius acrescentava as possibilidades de removerem os discos e substituí-los por outros, diante de tantas combinações criadas, calcula-se mais de $10.000.000.000.000.000$ combinações.

No início da comunicação com a Enigma, o remetente ajustava as unidades misturadores, em seguida codificava a mensagem e enviava a mensagem ao destinatário que deveria ajustar a sua máquina igual a do remetente. Ao teclar as letras codificadas, o painel acenderia a letra original correspondente, assim, tornando a mensagem legível.

A Enigma foi bastante utilizada pelos alemães durante a Segunda Guerra Mundial, entre os soldados a comunicação funcionava do seguinte modo: os exércitos compartilhavam um livro que continha os reajustes dos misturadores do dia, sendo a quantidade suficiente para um mês, após isso eles receberiam um novo livro. Então, inicia-se reajustando os misturadores na posição indicada pelo livro, em seguida codifica-se a mensagem, posteriormente, era entregue ao operador de rádio, que transmitia na linguagem código Morse. O operador de rádio do outro grupo do exército recebia e escrevia a mensagem codificada, sendo entregue para a pessoa responsável pela máquina Enigma para decodificar.

A transmissão da comunicação pelo rádio era facilmente interceptada pelos inimigos, porém, ao se depararem com aquela mensagem codificada, perceberam que os alemães tinham evoluído o seu método de criptografia.

Com isso, convocaram vários criptoanalistas para ajudar a decifrar as mensagens. Todavia,

resultaram-se em dias e noites sem sucesso.

Depois de tantas tentativas em vão, surge o alemão Hans-Tilo Schimdt, que foi expulso do exército por ser considerado um soldado que não tinha valor suficiente para permanecer após cortes drásticos exigidos pelo Tratado de Versalhes. O rancor de Schimdt aumentava ainda mais ao ver seu irmão Rudolph obtendo sucesso no exército, pois continuava na Guerra. Sem conseguir sucesso na sua vida, sente-se forçado a pedir ajuda ao seu irmão, que o coloca para trabalhar no centro de comando da Enigma. Apesar de ter conseguido um novo emprego, ressentia que fora rejeitado pelo seu país e permanecia uma inveja do sucesso de seu irmão. Fato que o objetivou a vender informações sobre a máquina Enigma aos potenciais estrangeiros, resultando na criação de uma réplica pelos inimigos.

A França que comprara os documentos com informações essenciais, no entanto, sem todos os detalhes, para a criação de uma réplica, desistiu de tentar decifrar. Pois, a essência da criptografia não estava na Enigma, mas sim nos reajustes da parte misturadora, no qual presumia ser impossível conseguir um livro dos alemães.

Por outro lado, os poloneses demonstraram interesse em qualquer informação sobre a Enigma, pois se sentiam bastante ameaçados por estarem geograficamente próximo à Alemanha. Tudo isso levou à criação de um departamento de cifras, onde foram recrutados 20 matemáticos para resolverem vários testes para que no fim pudesse trabalhar com as informações sobre a Enigma, e entre eles se destacou Marian Rejewski, homem de 33 anos.

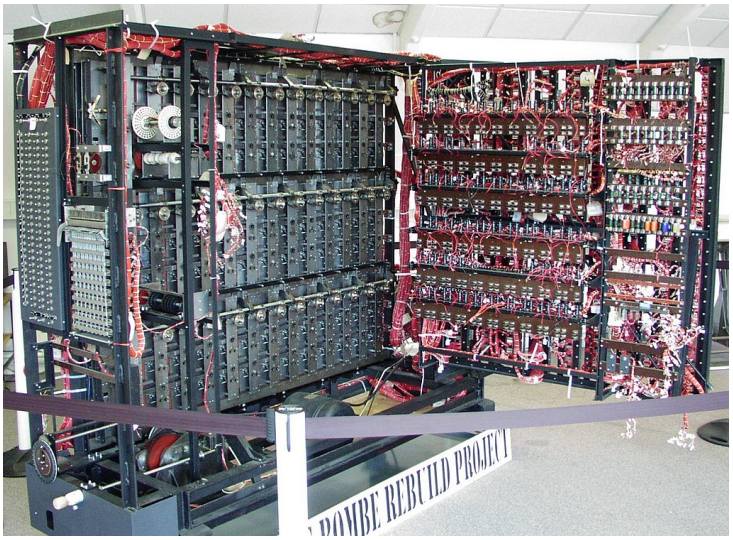
Rejewski com muito esforço conseguiu decifrar as mensagens enviadas através da Enigma, porém, aos poucos os alemães iriam melhorando a máquina, resultando em um trabalho engenhoso de Rejewski, uma máquina conhecida como *Bomba*, onde verificava todas as combinações das chaves, decifrando a mensagem em até 2 horas.

Em 1938, os alemães atualizaram a máquina, envolvendo mais 2 misturadores, resultando agora em 5 misturadores. Dessa forma, ao enviarem as mensagens, escolhia-se 3 misturadores entre os 5. Esse ato, fez com que os poloneses não conseguissem mais decifrar as mensagens. Sem recursos para atualizar a Bomba de Rejewski e o constante medo de serem atacados, já que não conseguia mais identificar os ataques dos inimigos, resolve-se passar todos os conhecimentos sobre a Enigma e a Bomba para os aliados.

Os aliados notaram a importância dos matemáticos para decifrar as mensagens, graças aos poloneses. Dentre os matemáticos recrutados, encontrava-se Alan Turing, que futuramente ficaria conhecido como o pai da informática. O mesmo, conseguiu criar uma nova bomba, que ficou conhecida como Bomba de Turing, Figura 2.17. Ele observou através das mensagens antigas, já decifradas, que os alemães sempre iniciavam a comunicação falando sobre o clima, tornando-se um padrão nas mensagens alemãs. O resultado disso é que Turing conseguiu um atalho para decifrar as mensagens.

Quando os inimigos dos alemães conseguiram decifrar novamente as mensagens, permaneceram cautelosos, planejando estratégias para vencer a Guerra. Pois, qualquer ataque brutal aos alemães, poderia fazer com que suspeitassem que sua comunicação havia sido decifrada, levando

Figura 2.17: Bomba de Turing.



Fonte: https://aventurasnahistoria.uol.com.br/noticias/reportagem/conheca-5-fatos-sobre-alan-turing-o-genio-torturado-que-inventou-computacao.phtml.

a uma nova atualização da Enigma. Dessa forma, os aliados conseguem vencer a Segunda Guerra Mundial em 1945 sobre a Alemanha.

Somente em 1970 foram divulgadas informações que a Enigma havia sido decifrada, pois antes disso ninguém estava autorizado a relatar essas informações. Notando-se a importância de manter essas informações em segredo, caso alguma nova guerra iniciasse e usassem a Enigma novamente, mantendo os criptoanalistas em vantagem.

2.2 Cifra de Chave Assimétrica

A chave assimétrica, tem esse nome porque utiliza duas chaves distintas, uma que codifica e a outra que decodifica, conhecidas respectivamente como chave pública e chave privada.

2.2.1 O Surgimento do Computador

Foram desenvolvidas outras bombas para avançar o estudo da criptologia, culminando no surgimento do primeiro computador programável em 1945, na Filadélfia. Esse computador, conhecido com ENIAC (*Electronic Numerical Integrator And Calculator*), representou um marco significativo nessa área. Segundo Viana (2020), o ENIAC era uma máquina colossal, composta por mais de 100 mil peças e ocupando um espaço de $90m^3$. Seu consumo de energia também era impressionante, ao ponto de se dizer que quando era ligado, todas as lâmpadas no estado da Pensilvânia enfraqueciam.

Após a guerra, os criptoanalistas estudaram a potência do computador, além de ser programável era altamente veloz comparados às bombas mecânicas, sendo possível simular vários tipos de cifragem.

Uma das diferenças do computador em relação às bombas mecânicas, é a utilização somente de *zeros* e *uns* para escrever a mensagem, conhecido como um sistema binário. Assemelha-se com o Código Morse que utiliza somente traços e pontos. Com isso, as letras do alfabeto são representados por 7 algarismos, veja Figura 2.18, essa conversão é dada por ASCII (*American Standard Code for Information Interchange*).

Figura 2.18: Números binários em ASCII para letras maiúsculas.

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 (2008).

Os demais caracteres como letras minúsculas e símbolos também possuem seus respectivos números binários.

Pode-se realizar cifras de transposição e substituição nos números binários. Como exemplo, considere a palavra "*PROFMAT*", inicia-se convertendo a palavra em números binários.

$$\textit{Texto Original} = \textit{PROFMAT} = 101000010100101001111100011010011011000001101010 0.$$

O algoritmo de transposição pode ser, por exemplo, a troca do primeiro e do segundo dígitos, do terceiro e do quarto dígitos, assim sucessivamente. O último dígito permanecerá, devido a quantidade de dígitos ser ímpar.

$$\begin{aligned} \textit{Texto Original} &= 101000010100101001111100011010011011000001101010 0. \\ \textit{Texto Codificado} &= 010100101000010110111100100101100111000010010101 0. \end{aligned}$$

Para decodificar, pode-se trocar novamente o primeiro e o segundo dígitos, o terceiro e o quarto dígitos, e assim por diante.

A cifra de substituição em números binários necessita a utilização de uma palavra-chave acordada entre o remetente e o destinatário, nesse caso, faz-se o método utilizando a palavra-chave "*FATORES*". O algoritmo consiste em "somar" os dígitos do texto original com a palavra-chave. A soma utilizada é feita de uma maneira simples: se os dígitos forem iguais,

então resulta em 0, caso os dígitos sejam distintos, então a soma será 1.

$$\begin{aligned}
\textit{Mensagem} &\Rightarrow \textit{PROFMAT.}\\
\textit{Mensagem em binário} &\Rightarrow 101000010100101001111100011010011011000001101010 0.\\
\textit{Chave} = \textit{FATORES} &\Rightarrow 100011010000011010100100111110100101000101101001 1.\\
\textit{Texto Codificado} &\Rightarrow 001011000100110011011000100100111110000100000011 1.
\end{aligned}$$

A mensagem codificada de 49 dígitos chegará ao destinatário, que utilizará a palavra-chave "*FATORES*" para fazer a substituição dos dígitos, voltando assim a mensagem original "*PROFMAT*".

Os computadores tornaram-se mais poderosos e baratos na década de 1960, sendo acessíveis às empresas que passaram a precisar criptografar as suas comunicações internas, transferência de dinheiro e importantes negociações comerciais. No entanto, como cada empresa tinha o seu método de criptografia, para comunicarem-se entre si, necessitavam de um novo método de criptografar. Com isso, os criptográfos procuraram uma maneira de padronizar a cifragem. Somente em 1976, obteve-se uma cifra que se chamava Lucifer de Feistel, sendo batizada como *Data Encryption Standard (DES)*, Padrão de Cifragem de Dados.

Apesar da padronização e da forte segurança da DES, tinha-se o problema da distribuição de chaves. Imaginando a situação da Segunda Guerra Mundial, os alemães tinham que distribuir para cada submarino um livro que continha as chaves de como programar a Enigma, era uma situação trabalhosa, já que os submarinos passavam longos tempos imersos. Agora, as empresas enfrentavam a mesma dificuldade, pois era preciso enviar mensageiros confiáveis para entregar as chaves a todos aqueles que receberiam a mensagem da empresa. Além disso, a dificuldade da distribuição de chaves e os custos para isso só aumentavam à medida em que essas empresas se desenvolviam e faziam mais negociações.

O problema é que na criptografia de chave privada é preciso manter a chave em segredo entre o remetente e o destinatário, caso ambos estivessem longe um do outro, deveriam se encontrar para combinar uma chave específica. Com essas dificuldades e fragilidades, surge a necessidade de criar uma criptografia de Chave Assimétrica, onde cada pessoa tem as suas chaves privada e pública, a última podendo ser divulgada publicamente, ou seja, qualquer pessoa poderia conhecê-la. Essas eram as ideias de Whitfield Diffie em 1975, apesar de não ter conseguido um exemplo prático, publicou a sua ideia no verão do mesmo ano, então vários cientistas se juntaram em busca de um método prático.

Em 1977, a equipe composta por Ronald Rivest, Adi Shamir e Leonard Adleman conseguiu criar um método, que ficou conhecido como Criptografia RSA (*Rivest, Shamir, Adleman*), sendo anunciado pela primeira vez em agosto de 1977.

De acordo com Coutinho (2014), "Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais.".

2.2.2 Criptografia RSA

Os estudos para a construção do modelo de Criptografia RSA se baseiam na Teoria dos Números.

Para poder utilizar o RSA é necessário dois parâmetros simples: dois números primos, sendo chamados de p e q. Através deles, cria-se as chaves pública e privada.

A primeira necessita do produto $p \cdot q$, que será denotado por n, o próximo elemento da chave é ϵ, um número inteiro positivo inversível módulo $\phi(n)$, ou melhor, mdc $(\epsilon, \phi(n)) = 1$. O valor de $\phi(n)$ é encontrado através dos números primos p e q:

$$\phi(n) = (p-1) \cdot (q-1).$$

Dessa forma, a *chave pública* é o par (n, ϵ).

Para enviar uma mensagem codificada utilizando a chave pública, deve-se primeiro realizar alguns passos: utilizar uma tabela com o alfabeto e seus respectivos valores numéricos para trocar as letras por esses valores, Figura 2.19, em seguida separar o números em blocos, de modo que cada bloco seja menor que n e não inicie em 0.

Segundo Coutinho (2014), "A maneira de escolher os blocos não é única, mas certos cuidados devem ser tomados. Por exemplo, é necessário evitar que o bloco comece por 0 porque isto traria problemas na hora de decodificar."

Figura 2.19: Alfabeto para Pré-Codificação.

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: Autor.

Seja b o bloco, então defini-se $C(b)$ o bloco codificado, tal que:

$C(b)$ = resto da divisão de b^ϵ por n.

Escrevendo de outra maneira, pode-se dizer que:

$b^\epsilon = n \cdot k + C(b)$, para k inteiro.

Em forma de congruência, denota-se:

$$b^\epsilon \equiv C(b) (\text{mod } n).$$

A chave privada também utiliza dois elementos, um deles sendo n e o outro d, tal que $d > 0$ e

inverso de ϵ em $\phi(n)$, ou seja, a *chave privada* é o par (n, d).

$$d \cdot \epsilon \equiv 1(mod\phi(n)).$$

Para decodificar a mensagem, necessita-se encontrar os valores dos blocos b, logo:

$$b = \text{resto da divisão de } C(b)^d \text{ por } n.$$

Exemplo 4. *Codifica-se a palavra "PROFMAT", utilizando os números primos 5 e 11, em seguida, decodifica-se retornando a palavra inicial.*

Primeiro, faz-se a pré-codificação utilizando a tabela apresentada na Figura 2.19.

Palavra pré-codificada: 25272415221029.

Sendo $p = 5$ e $q = 11$, então $n = 55$. Com isso, deve-se separar a palavra pré-codificada em blocos com valores menores que $n = 55$, evitando que o bloco inicie em 0. Portanto:

$$Blocos = 2 - 52 - 7 - 2 - 41 - 52 - 2 - 10 - 29. \tag{2.1}$$

Em seguida, calcula-se o valor de $\phi(55)$ e ϵ, tal que, mdc$(\phi(55), \epsilon) = 1$:

$$\begin{aligned} \phi(55) &= (5-1)(11-1) \\ \phi(55) &= 4 \cdot 10 \\ \phi(55) &= 40. \end{aligned}$$

Assim, pode-se atribuir o valor $\epsilon = 3$, pois, mdc$(40, 3) = 1$. Logo a Chave Pública é o par (55,3). Dessa forma, inicia-se a codificação de cada bloco:

$$\begin{aligned} 2^3 &\equiv 8(mod55), \\ 52^3 &\equiv (-3)^3 \equiv -27 \equiv 28(mod55), \\ 7^3 &\equiv 343 \equiv 13(mod55), \\ 41^3 &\equiv (-14)^3 \equiv -2744 \equiv 6(mod55), \\ 10^3 &\equiv 1000 \equiv 450 \equiv 10(mod55), \\ 29^3 &\equiv 24389 \equiv 2389 \equiv 189 \equiv 24(mod55). \end{aligned}$$

Palavra codificada = 8 - 28 - 13 - 8 - 6 - 28 - 8 - 10 - 24.

Para decodificar a palavra, necessita-se da chave privada, (n, d), ou seja, $(55, d)$. Dessa forma, tem-se que encontrar o valor de d:

$$d \cdot 3 \equiv 1(mod40) \Rightarrow d = 27.$$

Agora, com a Chave Privada em mãos, $(55, 27)$, decodifica-se cada bloco da palavra

codificada:

$$\begin{aligned} 8^{27} &\equiv X_1(mod55) \Rightarrow X_1 = 2, \\ 28^{27} &\equiv X_2(mod55) \Rightarrow X_2 = 52, \\ 13^{27} &\equiv X_3(mod55) \Rightarrow X_3 = 7, \\ 6^{27} &\equiv X_4(mod55) \Rightarrow X_4 = 41, \\ 10^{27} &\equiv X_5(mod55) \Rightarrow X_5 = 10, \\ 24^{27} &\equiv X_6(mod55) \Rightarrow X_6 = 29. \end{aligned}$$

Resultando em:

$$Blocos = 2 - 52 - 7 - 2 - 41 - 52 - 2 - 10 - 29.$$

Unindo-se todos os valores:

$$25272415221029.$$

Utilizando a tabela apresentada na Figura 2.19, retorna-se a palavra: PROFMAT.

Se o interceptador quiser decifrar a mensagem, terá que descobrir a chave privada, (n, d). O valor de n já será conhecido, pois é o mesmo utilizado na chave pública, porém, a segurança está na dificuldade de encontrar o valor de d, pois para descobrir é necessário conhecer ϵ e $\phi(n)$, consequentemente, para descobrir $\phi(n)$ é necessário conhecer os dois números primos e para isso, necessita-se fatorar n. Se n for grande, será difícil fatorá-lo, pois ainda não se tem conhecimento de algoritmos rápidos de fatoração. Segundo Coutinho (2014), recomenda-se que n tenha aproximadamente 231 algarismos para uso pessoal. Para obter esse valor de n, faz-se necessário ter dois números primos, um com 104 algarismos e o outro com 127 algarismos.

Existe outra criptografia assimétrica, *El Gamal*, desenvolvida em 1985 pelo cientista da computação egípcio Taher El Gamal.

O método da criptografia *El Gamal* fundamenta-se no estudo de grupos abelianos finitos cíclicos. Semelhante ao RSA, também utiliza o estudo da Aritmética Modular e números primos. Porém, a criptografia RSA tem a sua segurança na dificuldade na fatoração do número n, enquanto a criptografia *El Gamal* mantém a segurança devido na dificuldade de resolver o problema do logaritmo discreto em um grupo finito.

Capítulo 3

Revisão de Conceitos

Neste capítulo serão apresentados os conceitos teóricos fundamentais a serem utilizados no desenvolvimento deste trabalho e na aplicação em sala de aula. Consequentemente envolvendo a matemática e a criptologia para serem utilizados em sala de aula.

3.1 Divisibilidade

Nesta seção, será abordado o tema da divisibilidade, que desempenha um importante papel na decifragem da criptografia do Método Retangular. Recomenda-se os livros de Hefez (2022) e Santos (2010) como recursos para aprofundar ainda mais o estudo da divisibilidade.

Definição 3.1.1. *Sejam a e b números inteiros, diz-se que a divide b e denota-se $a \mid b$, se existir um inteiro c tal que $b = a \cdot c$.*

Se a não divide b, denota-se $a \nmid b$.

Proposição 3.1.1. *Se a, b e c são inteiros, $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Sabendo que $a \mid b$ e $b \mid c$, logo existem inteiros q_1 e q_2 com $b = q_1 \cdot a$ e $c = q_2 \cdot b$. Substituindo o valor de b na equação $c = q_2 \cdot b$ obtém-se $c = q_2 q_1 \cdot a$ o que implica $a \mid c$, onde $q_2 q_1$ representa um inteiro. □

Exemplo 5. *Uma vez que* $4 \mid 20$ *e* $20 \mid 140$*, tem-se* $4 \mid 140$*.*

Proposição 3.1.2. *Se a, b, c, m e n são inteiros, $a \mid b$ e $a \mid c$ então $a \mid (mb + nc)$.*

Demonstração. Se $a \mid b$ e $a \mid c$, então $b = q_1 a$ e $c = q_2 a$. Multiplicando-se estas duas equações respectivamente por m e n tem-se $m \cdot b = m \cdot q_1 a$ e $n \cdot c = n \cdot q_2 a$. Adicionando-se membro a membro, resulta em $mb + nc = (mq_1 + nq_2)a$. Concluindo que $a \mid (mb + nc)$. □

Exemplo 6. *Como* $6 \mid 18$ *e* $6 \mid 30$*, então* $6 \mid (9 \cdot 18 - 4 \cdot 30)$*.*

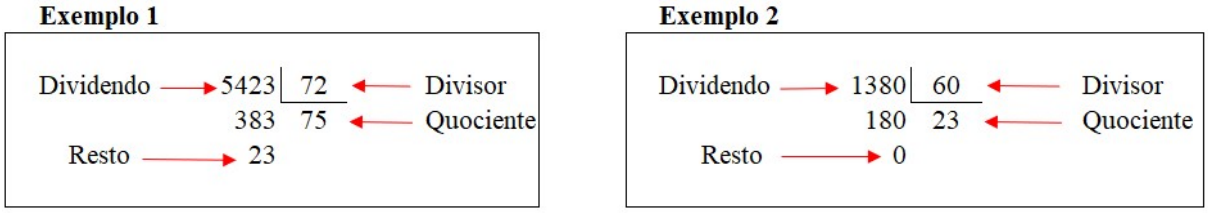
3.1.1 Algoritmo da Divisão

Um *algoritmo* é um conjunto finito de passos ordenados para concluir um objetivo.

Atualmente, o ensino do algoritmo da divisão inicia-se no Fundamental I, o qual possui quatro elementos: dividendo, divisor, quociente e resto.

Exemplo 7. *Na Figura 3.1 destacam-se dois exemplos de divisão, sendo o primeiro* 5423 *dividido* 72 *e o segundo* 1380 *dividido por* 60*.*

Figura 3.1: Algoritmo da divisão.



Fonte: Autor.

A relação do algoritmo apresentado anteriormente, pode também ser escrito da seguinte forma:

$$\textbf{Dividendo} = \textbf{Divisor} \cdot \textbf{Quociente} + \textbf{Resto}.$$

Considerando os exemplos 1 e 2 da Figura 3.1, tem-se que:

Exemplo 1: $5423 = 72 \cdot 75 + 23$.

Exemplo 2: $1380 = 60 \cdot 23 + 0$.

Definição 3.1.2. *Sejam* a *e* b *números naturais, se* a *divide* b*, de modo que o resto seja igual a* 0*, então* a *é divisor de* b*.*

Na apresentação do algoritmo da divisão (Figura 3.1) observa-se no exemplo 2, o resto é igual a zero, portanto, 60 é divisor de 1380. Consequentemente, o resultado da divisão, quociente, também é um divisor do dividendo. Ou seja, 23 também é divisor de 1380.

No exemplo 1, ao contrário, o resto é diferente de zero, portanto 72 não é divisor de 5423.

Seja n um número positivo, denomina-se $D(n)$ o seu conjunto de divisores positivos.

Exemplo 8. *Os divisores positivos dos números* $20, 36$ *e* 43 *são:*

- $D(20) = \{1, 2, 4, 5, 10, 20\}$.
- $D(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.

- $D(43) = \{1, 43\}$.

Saber os divisores de um número auxilia na determinação dos possíveis tamanhos da palavra-chave da criptografia do Método Retangular. Neste trabalho, nos estudos desenvolvidos sobre o Método Retangular, descartam-se as possibilidades das mensagens serem menores ou iguais ao tamanho da palavra-chave.

Exemplo 9. *Dada uma mensagem codificada pela criptografia do Método Retangular e uma lista de possíveis palavras-chave, identifique qual é a palavra-chave verdadeira.*

Mensagem Codificada: ***TAAAIMAARAATIEFMINREACHIREEMPDAMTE#***

Lista das possíveis palavras-chave:

PAR - *IMPARES* - *NEGATIVO* - *DIVISORES*

Resolução: Deve-se contar quantos caracteres tem a mensagem codificada, dessa forma, observa-se que há 35 caracteres. Em seguida, encontra-se os divisores positivos de 35:

$$D(35) = \{1, 5, 7, 35\}.$$

Os divisores representam a quantidade de letras das possíveis palavras-chave, com exceção do 1*, pois esse valor não torna a mensagem ilegível, e do próprio número,* 35*, por conta que foi descartado o caso da mensagem codificada ser do tamanho da palavra-chave. Com isso, a palavra-chave pode ter* 5 *ou* 7 *letras, então diante da lista dada, observa-se que não há palavra-chave de* 5 *letras, restando somente a palavra-chave de* 7 *letras, "IMPARES", sendo essa a palavra-chave para decifrar a mensagem.*

A seguir serão apresentados os critérios de divisibilidades que auxiliam a encontrar alguns divisores.

3.1.2 Critério de Divisibilidade por 2, 4 e 8

3.1.2.1 Divisibilidade por 2

Proposição 3.1.3. *Se* k *é um número inteiro e termina em 0, 2, 4, 6, ou 8, então* k *é divisível por 2.*

Demonstração. Seja k um número de n algarismos, ou seja:

$$k = n_{r-1}n_{r-2}...n_2n_1n_0$$

Pode-se escrever o número k na soma de produtos de base 10:

$$\begin{aligned} k &= 10^{r-1} \cdot n_{r-1} + 10^{r-2} \cdot n_{r-2} + ... + 10^2 \cdot n_2 + 10^1 \cdot n_1 + 10^0 \cdot n_0 \\ k &= 10 \cdot (10^{r-2} \cdot n_{r-1} + 10^{r-3} \cdot n_{r-2} + ... + 10^1 \cdot n_2 + n_1) + n_0 \end{aligned}$$

Se $2 \mid k$, então $2 \mid (10 \cdot (10^{r-2} \cdot n_{r-1} + 10^{r-3} \cdot n_{r-2} + ... + 10^1 \cdot n_2 + n_1) + n_0)$. Pela, proposição 3.1.2, nota-se que $2 \mid (10 \cdot (10^{r-2} \cdot n_{r-1} + 10^{r-3} \cdot n_{r-2} + ... + 10^1 \cdot n_2 + n_1))$ nesse caso, para k ser divisível por 2, tem-se que $2 \mid n_0$, sendo assim, $n_0 = 0, 2, 4, 6$ e 8. □

Dessa forma, os números a seguir são exemplos de números divisíveis por 2: 1.548, 24.790, 872, 236, 3.864.

3.1.2.2 Divisibilidade por 4

Para identificar um número divisível por 4, deve-se observar o número formado pelos dois últimos algarismos do número original, contados da esquerda para a direita, caso seja divisível por 4 ou forem zeros, então o número original também é divisível por 4.

Proposição 3.1.4. *Se k é um inteiro e termina em 00, 04, 08, 12, 16, ... ou 96, então k é divisível por 4.*

Demonstração. Seja k um número de n algarismos, ou seja:

$$k = n_{r-1}n_{r-2}...n_2n_1n_0$$

Escrevendo k na soma de produtos de base 10:

$$\begin{aligned} k &= 10^{r-1} \cdot n_{r-1} + 10^{r-2} \cdot n_{r-2} + ... + 10^2 \cdot n_2 + 10^1 \cdot n_1 + 10^0 \cdot n_0 \\ k &= 100 \cdot (10^{r-3} \cdot n_{r-1} + 10^{r-4} \cdot n_{r-2} + ... + n_2) + 10^1 \cdot n_1 + n_0 \\ k &= 100 \cdot (10^{r-3} \cdot n_{r-1} + 10^{r-4} \cdot n_{r-2} + ... + n_2) + n_1n_0 \end{aligned}$$

Observe que $4 \mid (100 \cdot (10^{r-3} \cdot n_{r-1} + 10^{r-4} \cdot n_{r-2} + ... + n_2))$, para que $4 \mid k$, obrigatoriamente, pela proposição 3.1.2, $4 \mid n_1n_0$, para isso, tem-se que os valores de $n_1n_0 = 00, 04, 08, 12, 16, ..., 92, 96$, múltiplos de 4. □

Exemplo 10. *Verificar se o número 5236 é divisível por 4.*

Note que o número formado pelos dois últimos algarismos de 5236, ou seja 36, é divisível por 4. Portanto, 5236 também é divisível por 4.

3.1.2.3 Divisibilidade por 8

O critério de divisibilidade por 8 assemelha-se a divisibilidade por 4, mas dessa vez, observa-se o número formado pelos três últimos algarismos do número original, caso seja divisível por 8 ou forem 000, então o número original é divisível por 8.

Proposição 3.1.5. *Se k é um inteiro e termina em 000, 008, 016, 024, ..., 984 ou 992, então k é divisível por* 8.

Demonstração. Seja k um número de n algarismos, ou seja:

$$k = n_{r-1}n_{r-2}...n_2n_1n_0$$

Escrevendo k na soma de produtos de base 10:

$$\begin{aligned} k &= 10^{r-1} \cdot n_{r-1} + 10^{r-2} \cdot n_{r-2} + ... + 10^3 \cdot n_3 + 10^2 \cdot n_2 + 10^1 \cdot n_1 + 10^0 \cdot n_0 \\ k &= 1000 \cdot (10^{r-3} \cdot n_{r-1} + 10^{r-4} \cdot n_{r-2} + ... + n_3) + 10^2 \cdot n_2 + 10^1 \cdot n_1 + n_0 \\ k &= 1000 \cdot (10^{r-3} \cdot n_{r-1} + 10^{r-4} \cdot n_{r-2} + ... + n_3) + n_2n_1n_0 \end{aligned}$$

Ocorre de maneira análoga a divisibilidade por 4. Implicando-se que para $8 \mid k$, deve-se ter $8 \mid (n_2n_1n_0)$, surgindo a necessidade de $n_2n_1n_0 = 000, 008, 016, 024, 032, ..., 984, 992$, múltiplos de 8. □

O número 352.184 é um exemplo em ser divisível por 8, pois $8 \mid 184$.

3.1.3 Critério de Divisibilidade por 3, 6 e 9

3.1.3.1 Divisibilidade por 3

Para identificar se um número é divisível por 3, deve-se observar a soma de todos os seus algarismos e verificar se o resultado é divisível por 3, caso seja, então o número original é divisível por 3.

Proposição 3.1.6. *Se k é um inteiro e a soma de seus algarismos é divisível por* 3*, então k é divisível por* 3.

Demonstração. Seja k um número de n algarismos, ou seja:

$$k = n_{r-1}n_{r-2}...n_2n_1n_0$$

Escrevendo k na soma de produtos de base 10:

$$\begin{aligned} k &= 10^{r-1} \cdot n_{r-1} + 10^{r-2} \cdot n_{r-2} + ... + 10^3 \cdot n_3 + 10^2 \cdot n_2 + 10^1 \cdot n_1 + 10^0 \cdot n_0 \\ k &= 1000...00 \cdot n_{r-1} + 100..00 \cdot n_{r-2} + ... + 1000 \cdot n_3 + 100 \cdot n_2 + 10 \cdot n_1 + n_0 \\ k &= (9999...99 + 1) \cdot n_{r-1} + (999...99 + 1) \cdot n_{r-2} + ... + (9 + 1) \cdot n_1 + n_0 \\ k &= 9999...99 \cdot n_{r-1} + 999...99 \cdot n_{r-2} + ... + 9 \cdot n_1 + n_{r-1} + n_{r-2} + ... + n_1 + n_0 \\ k &= 9[(111...11) \cdot n_{r-1} + 111...11 \cdot n_{r-2} + ... + 11 \cdot n_2 + n_1] + n_{r-1} + ... + n_1 + n_0 \end{aligned}$$

Observe que 3 divide $k = 9[(111...11) \cdot n_{r-1} + 111...11 \cdot n_{r-2} + ... + 11 \cdot n_2 + n_1]$. Então, para k ser divisível por 3, a parcela $n_{r-1} + n_{r-2} + ... + n_2 + n_1 + n_0$ deverá ser divisível por 3,

nota-se que essa parcela é a soma dos algarismos do número k. De forma análoga prova-se o critério de divisibilidade por 9. □

Exemplo 11. *Observe que os números apresentados a seguir são divisíveis por 3, utilizando o critério de divisibilidade e o algoritmo da divisão.*

- *87:*
  Utilizando o critério de divisibilidade por 3:
  $8 + 7 = 15$*, como 15 é divisível por 3, então o número 87 também é divisível por 3.*

- *4986:*
  Utilizando o critério de divisibilidade por 3:
  $4 + 9 + 8 + 6 = 27$*, como 27 é divisível por 3, então o número 4986 também é divisível por 3.*

- *857:*
  Utilizando o critério de divisibilidade por 3:
  $8 + 5 + 7 = 20$*, como 20 dividido por 3 não resulta em uma divisão exata, então o número 857 não é divisível por 3.*

3.1.3.2 Divisibilidade por 6

Se um número é divisível por 2 e 3, então ele é divisível por 6.

Exemplo 12. *Observe os números* $48, 7698, 315$ *e* 442*:*

- 48
  O número é par, portanto divisível por 2*. E note que a soma de seus algarismos é divisível por* 3*, ou seja,* $4 + 8 = 12 \Rightarrow 3 \mid 12$*. Dessa forma, 48 é divisível por* 6*.*

- 7698
  É par e tem-se que: $7 + 6 + 9 + 8 = 30 \Rightarrow 3 \mid 30$*, então* 7698 *é divisível por* 6*.*

- 315
  Não é par, portanto, 315 *não é divisível por* 6*.*

- 442
  É par, porém, $4 + 4 + 2 = 10 \Rightarrow 3 \nmid 10$*, então* 442 *não é divisível por* 6*.*

3.1.3.3 Divisibilidade por 9

O critério de divisibilidade por 9 é semelhante ao critério da divisibilidade por 3, a diferença é que a soma dos algarismos deve ser divisível por 9 para que o número original seja divisível por 9.

Exemplo 13. *Verifica-se os números* 46.872 *e* 32.846 *são divisíveis por 9.*

- 46.872 :

  Soma-se todos os algarismos, $4 + 6 + 8 + 7 + 2 = 27$*, sabe-se que* $9 \mid 27$*, logo* 46.872 *é divisível por* 9*.*

- 32.846 :

  Somando-se todos os algarismos, $3 + 2 + 8 + 4 + 6 = 23$*, como* $9 \nmid 23$*, então* 32.846 *não é divisível por* 9*.*

3.1.4 Números Primos

Definição 3.1.3. *No conjunto dos números Naturais os números primos são aqueles que tem somente dois divisores,* 1 *e o próprio número. No entanto, ao tratar do conjunto dos números Inteiros, os números primos tem exatamente quatro divisores, sendo eles:* $+1, -1$*, o próprio número e o seu oposto.*

Exemplo 14. *Observe os divisores dos números 11, 39 e 43, em relação ao Conjunto dos Naturais e Conjunto dos Inteiros:*
Conjunto dos Naturais:

- $D(11) = \{1, 11\}$.
- $D(39) = \{1, 3, 13, 39\}$.
- $D(43) = \{1, 43\}$.

Conjunto dos Inteiros:

- $D(11) = \{-11, -1, 1, 11\}$.
- $D(39) = \{-39, -13, -3, -1, 1, 3, 13, 39\}$.
- $D(43) = \{-43, -1, 1, 43\}$.

Dessa forma, conclui-se que somente os números 11 e 43 são primos.

Há uma forma antiga de encontrar números primos, desenvolvida pelo matemático Eratóstenes, que nasceu por volta de 284 a.C, o método é conhecido como *Crivo de Eratóstenes*, presente em Santos (2010).

Para utilizar o crivo, deve-se estabelecer um número natural n, que será o limite. O intervalo escolhido deve-se iniciar em 1 e terminar em n. Dessa forma, escreve-se todos os números de 1 a n, risca-se o número 1, pois, o mesmo não é primo por ter apenas um divisor no Conjunto dos Naturais. Em seguida, tem-se o número 2 que é primo, deve-se riscar todos os múltiplos de 2, com exceção do próprio número, ao terminar notará que o próximo número, que não está riscado é o 3 que é primo, então risca-se os múltiplos de 3, com exceção do próprio número, ao terminar, repete-se o processo até o último número não riscado. Os números não riscados, são os números primos.

Exemplo 15. *Utilizando o Crivo de Eratóstenes, encontre todos os números primos de* 1 *a* 40.

O número 1 *é riscado por não ser primo, assim, inicia-se a análise no próximo número, ou seja,* 2*, então risca-se os múltiplos de* 2 *com exceção do próprio número, conforme apresentado na Tabela 3.1.*

Tabela 3.1: Analisando os múltiplos de 2.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

Em seguida, analisa o número 3*. Então, risca-se todos os múltiplos de* 3*, com exceção do próprio número, conforme apresentado na Tabela 3.2.*

Tabela 3.2: Analisando os múltiplos de 3.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

O número 5 é o próximo a ser analisado, conforme apresentado na Tabela 3.3.

Tabela 3.3: Analisando os múltiplos de 5.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

Observe que ao analisar o próximo número, 7, todos os seus múltiplos já foram riscados, o mesmo vai acontecer com as análises posteriores do intervalo dado. Dessa forma, os números que sobraram são primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 e 37, conforme apresentado na Tabela 3.4.

Tabela 3.4: Números Primos no intervalo de 1 a 40.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

O crivo de Eratóstenes deu origem a outros crivos modernos. Pode-se notar a sua exatidão para encontrar números primos, porém, exige esforço para intervalos cada vez maiores.

No entanto, alguns teoremas podem facilitar o processo de identificação de números primos.

Teorema 3.1.1. *Se n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.*

Demonstração. Seja n um número composto, então $n = n_1 \cdot n_2$, onde $1 < n_1 < n$ e $1 < n_2 < n$. Suponha-se que $n_1 \leq n_2$, então:

$$\begin{aligned} n_1 \cdot n_1 &\leq n \\ (n_1)^2 &\leq n \\ \sqrt{(n_1)^2} &\leq \sqrt{n} \\ n_1 &\leq \sqrt{n}. \end{aligned}$$

Como todo número inteiro maior que 1 pode ser escrito de uma única maneira como um produto de fatores primos, desconsiderando-se a ordem posicional desses primos, garante-se que n_1 tem um fator primo p_1, tal que, $p_1 \leq n_1$. Se p_1 é fator primo de n_1, logo p_1 é fator primo de n. Sendo assim:

$$p_1 \leq n_1 \leq \sqrt{n} \Rightarrow p_1 \leq \sqrt{n}.$$

□

Ao desejar encontrar os números primos no intervalo de 1 a 100. Então, será analisado somente os números menores ou igual a $\sqrt{100} = 10$, ou seja, os primos $2, 3, 5$ e 7.

3.1.5 Fatoração

Teorema 3.1.2. *(Teorema Fundamental da Aritmética) Todo inteiro $n > 1$ pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

A demonstração desse teorema pode ser encontrada em (SANTOS, 2010, p.9).

Exemplo 16. *Números escritos como produto de fatores primos:*

- $35 = 7 \cdot 5$
- $20 = 2^2 \cdot 5$
- $693 = 3^2 \cdot 7 \cdot 11$

Para escrever um número n em produto de fatores primos, pode-se utilizar o seguinte algoritmo:

1. Traça-se uma linha vertical, escreve-se n do lado esquerdo da linha, e do lado direito coloca-se o menor divisor primo de n;
2. Divide n pelo seu menor divisor primo, em seguida, escreve-se o quociente abaixo de n;
3. Depois divide o quociente por seu menor divisor primo, repetindo esse processo até que o quociente seja igual a 1.

O produto dos números primos que estão do lado direito da linha vertical representam exatamente o produto de fatores primos de n.

Exemplo 17. *Destaca-se o uso do algoritmo de fatoração nos números $84, 180$ e 1575, por meio da Figura 3.2:*

Figura 3.2: Fatoração dos números 84, 180 e 1575.

84	2
42	2
21	3
7	7
1	

180	2
90	2
45	3
15	3
5	5
1	

1575	3
525	3
175	5
35	5
7	7
1	

Fonte: Autor.

Assim,

- $84 = 2^2 \cdot 3 \cdot 7$
- $180 = 2^2 \cdot 3^2 \cdot 5$

- $1575 = 3^2 \cdot 5^2 \cdot 7$

Existe um algoritmo para calcular o número de divisores positivos tem um número inteiro n. Primeiro fatora-se n, em seguida faz-se o produto dos expoentes dos números primos adicionado 1. Denomina-se o número de divisores positivos de n por $\#D(n)$.

Utilizando as informações do exemplo 17:

- $84 = 2^2 \cdot 3 \cdot 7$
  Desse modo, tem-se que:

$$\begin{aligned} \#D(84) &= (2+1) \cdot (1+1) \cdot (1+1) \\ &= 3 \cdot 2 \cdot 2 \\ &= 12 \end{aligned}$$

  Portanto, o número 84 tem *doze* divisores positivos.

- $180 = 2^2 \cdot 3^2 \cdot 5$
  Desse modo, tem-se que:

$$\begin{aligned} \#D(180) &= (2+1) \cdot (2+1) \cdot (1+1) \\ &= 3 \cdot 3 \cdot 2 \\ &= 18 \end{aligned}$$

  Portanto, o número 180 tem *dezoito* divisores positivos.

- $1575 = 3^2 \cdot 5^2 \cdot 7$
  Desse modo, tem-se que:

$$\begin{aligned} \#D(1575) &= (2+1) \cdot (2+1) \cdot (1+1) \\ &= 3 \cdot 3 \cdot 2 \\ &= 18 \end{aligned}$$

  Portanto, o número 1575 tem *dezoito* divisores positivos.

Saber a quantidade de divisores positivos de um número, pode nos ajudar a descobrir a quantidade de palavras-chave utilizada na criptografia do Método Retangular ao interceptar uma mensagem.

Exemplo 18. *Descubra quantos tamanhos distintos de palavras-chave pode-se analisar para decifrar a mensagem interceptada apresentada a seguir, sabendo que a criptografia utilizada é do Método Retangular:*

IANROMPSNSLTEELOEOABAROUOCSPSU

Resolução: Primeiramente, observa-se que há 30 caracteres na mensagem, então descobre-se a quantidade de divisores do número 30. Assim, fatora-se o número 30, conforme apresentado na Figura 3.3.

Figura 3.3: Fatoração do 30.

30	2
15	3
5	5
1	

Fonte: Autor.

Tem-se que: $30 = 2 \cdot 3 \cdot 5$. *Então, calcula-se* $\#D(30)$*:*

$$\#D(30) = (1+1)(1+1)(1+1) = 8.$$

Portanto, há 8 *tamanhos distintos de palavras-chave para analisar. Lembrando-se que todo número tem como divisor o número* 1 *e o próprio número, logo esses divisores são excluídos da contagem. Ou seja, pode-se analisar somente* $8 - 2 = 6$ *tamanhos de palavras-chave distintos.*

Saber a quantidade de divisores positivos permite determinar quantos divisores devem ser encontrados de um número. Ao desejar encontrar todos os divisores positivos do número 30, vê-se que é preciso encontrar 8 divisores.

3.2 Congruência

Nesta seção, serão apresentadas algumas informações sobre o estudo de Congruência, que desempenha um papel fundamental na atual criptografia RSA. Para um estudo mais aprofundado sobre Congruência, indica-se o livro Hefez (2022). Para o estudo da Congruência na Criptografia RSA, sugere-se o livro Coutinho (2014).

Antes de definir formalmente o conceito de Congruência, observe a seguir duas situações:

- $69 = 13 \cdot 5 + 4$
- $30 = 13 \cdot 2 + 4$.

Nota-se que ao dividir 69 e 30 por 13, ambos deixam resto 4. Essa relação, percebida pelo matemático Gauss, é conhecida como *Congruência*.

Dessa forma, diz-se que 69 é congruente a 4 módulo 13, e o outro, 30 é congruente a 4 módulo 13, sendo denotados da seguinte maneira:

- $69 \equiv 4 (mod 13)$
- $30 \equiv 4 (mod 13)$. (3.1)

Ainda é possível observar que os números 69 e 30 são congruentes, pois ambos deixam o mesmo resto, 4, ao serem divididos pelo mesmo número, 13. Usando a simbologia de congruência, pode-se escrever:

$$69 \equiv 30(mod 13). \tag{3.2}$$

Coutinho (2014), define a congruência da seguinte maneira:

Definição 3.2.1. *Sejam a e b números inteiros e um número n inteiro positivo, diz-se que a é congruente a b módulo n, se $(a - b)$ é divisível por n. Se a é congruente a b módulo n, então denota-se $a \equiv b$ (mod n).*

Aplicando a definição nos itens (3.1) e (3.2):

$$\begin{aligned} 69 &\equiv 4(mod 13) \Rightarrow (69 - 4) = 65 \text{ é divisível por } 13. \\ 30 &\equiv 4(mod 13) \Rightarrow (30 - 4) = 26 \text{ é divisível por } 13. \\ 69 &\equiv 30(mod 13) \Rightarrow (69 - 30) = 39 \text{ é divisível por } 13. \end{aligned}$$

Teorema 3.2.1. *Sejam a, b, c e n inteiros, sendo $n > 0$. Então:*

1. $a \equiv a$ *(mod n)*
2. *Se* $a \equiv b$ *(mod n), então* $b \equiv a$ *(mod n)*
3. *Se* $a \equiv b$ *(mod n) e* $b \equiv c$ *(mod n), então* $a \equiv c$ *(mod n)*

Demonstração. 1. Utilizando a definição, tem-se que $(a - a) = 0$ e 0 é divisível por todos os números inteiros positivos. Logo, $a \equiv a$ (mod n).

2. Se $a \equiv b$ (mod n), então $n \mid (a - b)$, sabe-se que o simétrico de $(a - b)$ também é divisível por n, ou seja:
$$n \mid -(a - b) \Rightarrow n \mid (b - a) \Rightarrow b \equiv a(\text{mod } n)$$

3. Utilizando a definição, obtém-se que $(a - b)$ e $(b - c)$ são divisíveis por n, sabe-se que a soma de ambos continuará sendo divisível por n, assim:

$$(a - b) + (b - c) = a - b + b - c = a - c$$

Logo, $a - c$ é divisível por n, ou seja, $a \equiv c$ (mod n).

□

Teorema 3.2.2. *Seja $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$, com a, b, c, d, n e q inteiros, com $n > 0$.*

1. $a + c \equiv b + d(mod\ n)$
2. $a - c \equiv b - d(mod\ n)$

3. $a \cdot c \equiv b \cdot d (mod\ n)$

4. $a^q \equiv b^q (mod\ n)$

Demonstração. 1. Tem-se que, $a \equiv b (\text{mod } n)$, implica que $n \mid (a-b)$, então existe um k_1 inteiro, tal que, $a - b = k_1 \cdot n$, o mesmo ocorre para $c \equiv d (\text{mod } n)$, ou seja, existe k_2 inteiro, que satisfaça a igualdade $c - d = k_2 \cdot n$.

Somando as duas igualdades, temos:

$$\begin{aligned} (a-b)+(c-d) &= k_1 \cdot n + k_2 \cdot n \\ a+c-b-d &= (k_1+k_2)\cdot n \\ (a+c)-(b+d) &= (k_1+k_2)\cdot n \quad \Rightarrow \quad a+c \equiv b+d (\text{mod } n) \end{aligned}$$

2. De maneira análoga, porém subtraindo as igualdades, temos:

$$\begin{aligned} (a-b)-(c-d) &= k_1 \cdot n - k_2 \cdot n \\ a-c-b+d &= (k_1-k_2)\cdot n \\ (a-c)-(b-d) &= (k_1-k_2)\cdot n \quad \Rightarrow \quad a-c \equiv b-d (\text{mod } n) \end{aligned}$$

3. Da igualdade $a - b = k_1 \cdot n$, multiplicando ambos os membros por c e da igualdade $c - d = k_2 \cdot n$, multiplicando ambos os membros por b. Assim:

$$\begin{aligned} a-b &= k_1 \cdot n \text{ , multiplica-se por } c \\ ac-bc &= k_1 \cdot n \cdot c \end{aligned} \tag{3.3}$$

$$\begin{aligned} c-d &= k_2 \cdot n \text{ , multiplica-se por } b \\ cb-bd &= k_2 \cdot n \cdot b \end{aligned} \tag{3.4}$$

Agora, somando (3.3) e (3.4):

$$\begin{aligned} ac-bc+cb-bd &= k_1 \cdot n \cdot c + k_2 \cdot n \cdot b \\ ac-bd &= (k_1 \cdot c + k_2 \cdot b)\cdot n \quad \Rightarrow \quad ac \equiv bd (\text{mod } n) \end{aligned}$$

4. A demonstração é realizada através da seguinte igualdade:

$$a^q - b^q = (a-b)\cdot(a^{q-1} + a^{q-1}\cdot b + a^{q-2}\cdot b^2 + ... + a^2 \cdot b^{q-2} + a \cdot b^{q-1} + b^q)$$

Observa-se que:

$$(a-b) \mid a^q - b^q$$

e sabe-se que:

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

Logo,

$$n \mid a^q - b^q$$

Denotando-se, $a^q \equiv b^q (\text{mod } n)$.

□

Exemplo 19. *Deseja-se descobrir qual o valor do resto ao dividir* 14^{10} *por* 12*.*

Para solucionar esse problema, pode-se encontrar uma congruência mais simples, como:

$$14 \equiv 2 (\textit{mod } 12)$$

Utiliza-se o item 4, do teorema 3.2.2, elevando-se ambos os lados a 10*:*

$$14^{10} \equiv 2^{10} (\textit{mod } 12)$$

Note que, $2^{10} = 1024$ *e* $1024 \equiv 4 (\textit{mod } 12)$*. Em resumo, têm-se as seguintes congruências:*

$$14^{10} \equiv 1024 (\textit{mod } 12) \quad \textit{e} \quad 1024 \equiv 4 (\textit{mod } 12)$$

Portanto,

$$14^{10} \equiv 4 (\textit{mod } 12)$$

Então, ao dividir 14^{10} *por* 12 *obtém-se o resto igual a* 4*.*

Congruência é de suma importância para estudos da criptografia RSA, facilitando a realização dos cálculos para encontrar o resto de divisões feito por números grandes.

3.3 Permutação

A permutação na criptografia auxilia em cálculos para descobrir o número de possibilidades de um método criptográfico. Quanto maior o número de possibilidades, conclui-se que o método criptográfico é mais seguro. Recomenda-se os livros Morgado e Carvalho (2022) e Morgado et al. (2006) para um maior aprofundamento em Probabilidade e Estatística.

Dados n objetos distintos $p_1, p_2, p_3, ..., p_n$, de quantas maneiras pode-se ordená-los?

Seja os objetos a, b e c, é possível ordená-los das seguintes maneiras: abc, acb, bac, bca, cab e cba, há 6 maneiras. Neste exemplo, tem-se no total três objetos, sendo 3 modos de escolher o objeto que ocupará o primeiro lugar, após a escolha ser feita, sobrará 2 modos de escolher o objeto que ocupará o segundo lugar, restando apenas 1 modo de escolher o último lugar. Assim, a quantidade de maneiras que se pode ordenar três objetos distintos é:

$$3 \cdot 2 \cdot 1 = 3! = 6 \text{ maneiras.}$$

Respondendo a pergunta inicial, se tem n elementos distintos, então há n modos de escolher um objeto para o primeiro lugar, $n - 1$ para escolher um objeto para o segundo lugar, $n - 2$ objetos para o terceiro lugar, assim por diante até que todos sejam preenchidos. Dessa forma, o total de maneiras de organizá-los é:

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 3 \cdot 2 \cdot 1 = n! \text{ maneiras.}$$

Chama-se **permutação simples** cada maneira de organizar esses objetos e P_n representa o número de permutação simples de n objetos distintos. Desse modo:

$$P_n = n!.$$

Exemplo 20. *Quantos números de **seis** algarismos distintos existem ao utilizarmos os algarismos 3, 4, 7, 8, 9 e 1?*

*Como são **seis** algarismos distintos, utiliza-se o cálculo de permutação simples.*

$$P_6 = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$

Portanto, existem 720 números de seis algorismos distintos.

Com o conhecimento sobre **Divisores** e **Permutação** pode-se decifrar uma mensagem codificada que utiliza o Método Retangular, sem o conhecimento da chave, além disso, calcular o máximo de tentativas que será preciso para decifrá-la.

Exemplo 21. *Um criptoanalista interceptou a seguinte mensagem:*

*Mensagem Codificada: **EINAURNOSAUAALM***

1º Passo: Conta-se a quantidade de caracteres que tem a mensagem codificada.

Resposta: 15 caracteres

2º Passo: Identifica-se os divisores do número encontrado no 1º Passo.

Resposta: $D(15) = \{1, 3, 5, 15\}$

Observação 3.3.1. *Os divisores encontrados correspondem as possíveis quantidades de letras da palavra-chave. Com isso, exclui-se o menor e o maior divisores, pois o menor não codificaria a mensagem e o maior é o caso da mensagem ser igual ao tamanho da palavra-chave. Sobrando apenas os divisores 3 e 5.*

3º Passo: Escolhe-se um dos divisores, supondo que o escolhido seja o divisor 3, então faz-se $\frac{15}{3} = 5$*, em seguida divide-se a mensagem codificada em blocos de 5 caracteres.*

EINAU - RNOSA - UAALM

Em seguida, escreve-se verticalmente cada bloco, conforme Figura 3.4.

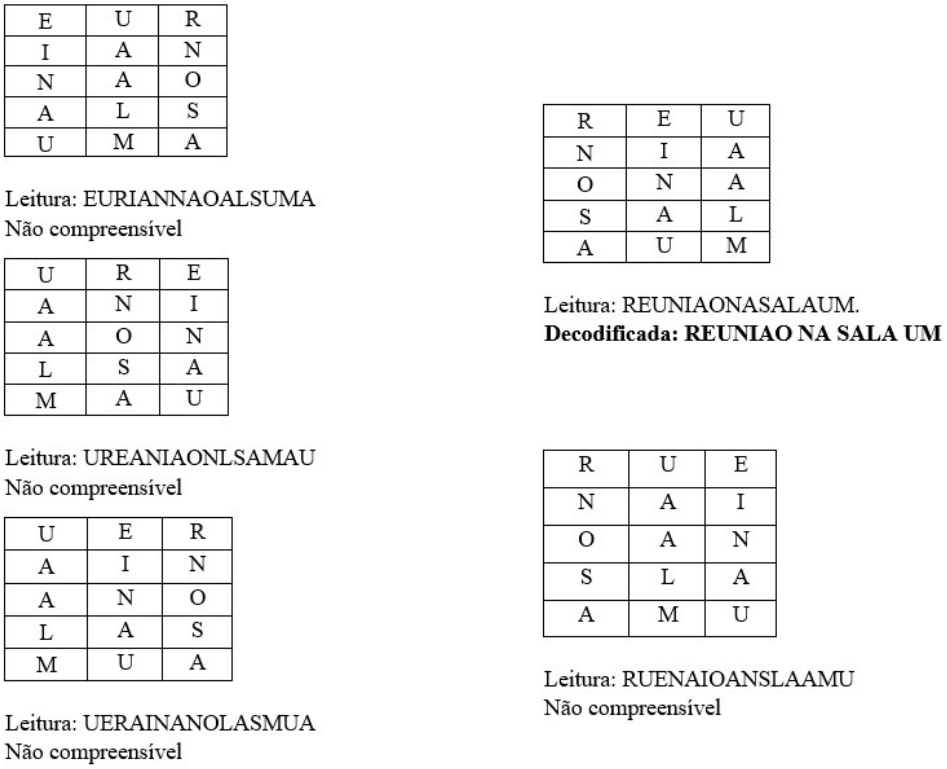
Figura 3.4: Escrito verticalmente.

E	R	U
I	N	A
N	O	A
A	S	L
U	A	M

Fonte: Autor.

*Lê-se a mensagem horizontalmente, "**ERUINANOAASLUAM**", caso não seja compreensível, deve-se permutar as colunas. Como são 3 colunas distintas, tem-se que a permutação é de 3! = 6 maneiras de organizar, conforme apresentado na Figura 3.5.*

Figura 3.5: As possibilidades.



Fonte: Autor.

*Descobre-se que a mensagem é "**REUNIÃO NA SALA UM**".*

Caso não decifrasse a mensagem com o divisor 3, passa-se para o divisor 5, $\frac{15}{5} = 3$. Dividindo a mensagem em blocos de 3 caracteres:

EIN - AUR - NOS - AUA - ALM

Nesse caso teriam-se 5 colunas, e portanto 5! = 120 maneiras de organizar. Essa quantidade pode ser feita com lápis e papel.

Como os divisores foram 3 e 5, o máximo de tentativas para decifrar a mensagem é de $3! + 5! = 126$. Um número pequeno, pois com um interceptador da mensagem disposto a usar um lápis e papel, poderia decifrar a mensagem facilmente.

Antes mesmo de tentar desvendar uma mensagem, pode-se calcular o número máximo de tentativas. Por exemplo, seja a seguinte mensagem codificada:

"SLEAALAVIOETICMEMREDGOSCROSDINSDONE"

Tem-se que o total de caracteres é 35. Sendo $D(35) = \{1, 5, 7, 35\}$, exclui-se 1 e 35, então permanece 5 e 7, dessa forma, o máximo de tentativas é de:

$$5! + 7! = 120 + 5.040 = 5.160 \text{ tentativas.}$$

Exemplo 22. *Seja a mensagem codificada:*

RVSUAAOVAGBCEMEPNDDNEENEMASEOS

Qual o máximo de tentativas para tornar a mensagem legível, sabendo que foi utilizado o método retangular?

Sabendo que o método retangular foi utilizado, então conta-se os caracteres. Observando que há 30 caracteres, calcula-se o divisor desse número.

$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

Descarta-se o menor e o maior divisor, resta o divisores $2, 3, 5, 6, 10$ *e* 15*. Portanto, o máximo de tentativas é de:*

$$\begin{aligned} 2! + 3! + 5! + 6! + 10! + 15! &= 2 + 6 + 120 + 720 + 3.628.800 + 1.307.674.368.000 + \\ &= 1.307.677.997.648. \end{aligned}$$

Devido ao aumento de divisores, faz com que o interceptor da mensagem tenha mais dificuldade de decifrar.

3.4 Função

O estudo de funções é um dos assuntos mais presentes no ensino médio e, por meio dele, é possível criar um sistema de criptografia de chave simétrica. Para um maior aprofundamento no conteúdo de funções, sugere-se os livros Lima (2023) e Iezzi e Murakami (2013).

Definição 3.4.1. *Dados dois conjuntos A e B, não vazios, uma relação f de A em B recebe o nome de aplicação de A em B se, e somente se, para todo x ∈ A existe um único y ∈ B tal que (x,y) ∈ f.*

3.4.1 Função Afim

Definição 3.4.2. *Seja uma aplicação de* $f : \mathbb{R} \to \mathbb{R}$*, tal que para cada* $x \in \mathbb{R}$*,* f *associa o elemento ax + b* $\in \mathbb{R}$*, em que* $a \neq 0$ *e b é um número real dado. Ou seja,*

$$\boxed{f(x) = ax + b}, \quad (a \neq 0)$$

ou

$$\boxed{y = ax + b}, \quad (a \neq 0)$$

Exemplo 23. *Função Afim:*

- $f(x) = 15x + 2$, *sendo* $a = 15$ *e* $b = 2$.
- $f(x) = -2x + 5$, *sendo* $a = -2$ *e* $b = 5$.
- $y = 8x - 13$, *sendo* $a = 8$ *e* $b = -13$.

Exemplo 24. *Seja uma aplicação de* $f : \mathbb{R} \to \mathbb{R}$ *definida por* $f(x) = 14x - 8$. *Calcule* $f(5)$ *e* $f(-3)$.

$$f(5) \quad = 14 \cdot 5 - 8 = 70 - 8 = 62 \Rightarrow f(5) = 62.$$

$$f(-3) \quad = 14 \cdot (-3) - 8 = -42 - 8 = -50 \Rightarrow f(-3) = -50.$$

Exemplo 25. *Através da Figura 3.6, que estabelece o alfabeto pré-codificação, pode-se codificar uma mensagem utilizando o conteúdo de* ***Função****. Dessa forma, seja a função* $y = 12x - 7$ *e a mensagem* ***"METODOLOGIA ATIVA"****.*

Figura 3.6: Tabela de Pré-Codificação.

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

Fonte: Autor.

Faz-se a pré-codificação, substituindo as letras da mensagem pelos números da tabela: ***Pré-Codificação:*** $13-5-20-15-4-15-12-15-7-9-1-1-20-9-22-1$.

Utiliza-se a função $y = 12x - 7$ *para codificar cada valor da pré-codificação.*

$$\begin{aligned}
f(13) &= 12(13) - 7 = 149 \\
f(5) &= 12(5) - 7 = 53 \\
f(20) &= 12(20) - 7 = 233 \\
f(15) &= 12(15) - 7 = 173 \\
f(4) &= 12(4) - 7 = 41 \\
f(12) &= 12(12) - 7 = 137 \\
f(7) &= 12(7) - 7 = 77 \\
f(9) &= 12(9) - 7 = 101 \\
f(1) &= 12(1) - 7 = 5 \\
f(22) &= 12(22) - 7 = 257
\end{aligned}$$

Em seguida substitui cada valor da pré-codificação pelo o seu resultado correspondente ao passar pela função $y = 12x - 7$.

Mensagem Codificada: $149 - 53 - 233 - 173 - 41 - 173 - 137 - 173 - 77 - 101 - 5 - 5 - 233 - 101 - 257 - 5$.

Então, o destinatário utilizará uma chave para tornar a mensagem legível. Para compreender a criação da chave do mesmo, precisa-se compreender o assunto de *Função Inversa*.

3.4.2 Função Inversa

Definição 3.4.3. *Se f é uma função bijetora de A em B, a relação inversa de f é uma função de B em A que denominamos função inversa de f e indicamos por f^{-1}.*

Exemplo 26. *Decodificar a mensagem codificada no Exemplo 25.*

O destinatário deve ter a função inversa da função da codificação, que é encontrada a partir de $y = 12x - 7$ para encontrar a sua função inversa:

Primeiro, invertem-se as variáveis x e y:

$$x = 12y - 7.$$

Em seguida, deve-se isolar a variável y:

$$\begin{aligned} x &= 12y - 7 \\ 12y - 7 &= x \\ 12y &= x + 7 \\ y &= \frac{x+7}{12} \end{aligned}$$

Portanto, a chave do destinatário é:

$$\boxed{f^{-1}(x) = \frac{x+7}{12}}$$

Decodificando a mensagem recebida:

$$f^{-1}(149) = \frac{149+7}{12} = \frac{156}{12} = 13, \textit{corresponde a letra } \boldsymbol{M}.$$

$$f^{-1}(53) = \frac{53+7}{12} = \frac{60}{12} = 5, \textit{corresponde a letra } \boldsymbol{E}.$$

$$f^{-1}(233) = \frac{233+7}{12} = \frac{240}{12} = 20, \textit{corresponde a letra } \boldsymbol{T}.$$

$$f^{-1}(173) = \frac{173+7}{12} = \frac{180}{12} = 15, \textit{corresponde a letra } \boldsymbol{O}.$$

$$f^{-1}(41) = \frac{41+7}{12} = \frac{48}{12} = 4, \textit{corresponde a letra } \boldsymbol{D}.$$

$$f^{-1}(137) = \frac{137+7}{12} = \frac{144}{12} = 12, \textit{corresponde a letra } \boldsymbol{L}.$$

$$f^{-1}(77) = \frac{77+7}{12} = \frac{84}{12} = 7, \textit{corresponde a letra } \boldsymbol{G}.$$

$$f^{-1}(101) = \frac{101+7}{12} = \frac{108}{12} = 9, \textit{corresponde a letra } \boldsymbol{I}.$$

$$f^{-1}(5) = \frac{5+7}{12} = \frac{12}{12} = 1, \textit{corresponde a letra } \boldsymbol{A}.$$

$$f^{-1}(257) = \frac{257+7}{12} = \frac{264}{12} = 22, \textit{corresponde a letra } \boldsymbol{V}.$$

Dessa forma, a Figura 3.7 representa a decodificação da mensagem.

Figura 3.7: Mensagem decodificada.

Mensagem Codificada	149	53	233	173	41	173	137	173	77	101	5	5	233	101	257	5
Mensagem Pré-Decodificada	13	5	20	15	4	15	12	15	7	9	1	1	20	9	22	1
Mensagem Decoficada	M	E	T	O	D	O	L	O	G	I	A	A	T	I	V	A

Fonte: Autor.

Capítulo 4

Atividades para Sala de Aula

Esse capítulo tem como objetivo apresentar propostas de atividades de matemática que envolvem a criptografia, para serem trabalhadas em salas de aulas.

4.1 Atividade 1 - Codificadores, Decodificadores e Espiões

Para essa atividade é preciso separar os alunos em três tipos de grupos, *Codificadores*, *Decodificadores* e *Espiões*, Figura 4.1.

Figura 4.1: Grupos.

Fonte: Autor

Cada grupo será responsável por uma função específica e receberá as informações iniciais necessárias para desempenhá-la. É de extrema importância que essas informações não sejam compartilhadas entre os grupos

Essa dinâmica será apresentada em três tipos de criptografias: *Método Retangular*, *Cifra de César* e *Função Afim, e Função Inversa*.

4.1.1 Dinâmica - Método Retangular

Conteúdo: Método retangular e divisores positivos de um número natural.
Público alvo: Fundamental II e Ensino Médio.
Organização: Grupo de 3 a 6 alunos.
Duração: 100 minutos.
Objetivos: Trabalhar em equipe; Codificar e decodificar uma mensagem pela criptografia do método Retangular; Decifrar uma mensagem codificada pela criptografia do método Retangular utilizando o estudo de divisores positivos de um número natural.
Recursos: Anexados no Apêndice, Seção A.1.

Caso a sala de aula tenha mais alunos, pode-se fazer novos grupos de *codificadores*, *decodificadores* e *espiões*.

Antes da atividade ser entregue aos alunos, o professor pode explicar a importância de uma comunicação segura, em seguida os orientar com um exemplo do dever de cada grupo, para isso utiliza-se a Seção 2.1.3 e o Exemplo 9 da Seção 3.1.1.

Logo depois, apresentam-se as informações iniciais de cada grupo, de forma isolada, sem que os outros grupos possam ouvir ou ver.

- *Codificadores* - Possuirá uma mensagem e a chave de codificação.

  Mensagem: Quanto é quinze mais dezenove
  Chave: MARTE

  Observação 4.1.1. *Não colocar "?" na frase, pois facilitaria o processo dos espiões.*

- *Decodificadores* - Terá a chave de decodificação.

  Chave: MARTE

- *Espiões* - Possuirá uma lista de possíveis palavras-chave.

  PLUTÃO - MARTE - JÚPITER - SATURNO - NETUNO - VÊNUS

Depois que todos os grupos estiverem com suas informações iniciais, o grupo dos codificadores irá codificar a mensagem utilizando a sua palavra-chave. Em seguida, escreve-se a mensagem codificada em dois pedaços de papel, pois uma será entregue ao grupo dos decodificadores e outro para os espiões, simulando a interceptação (material disponível no Apêndice A.1).

O grupo dos decodificadores tornará a mensagem legível utilizando a palavra-chave.

O grupo dos espiões utilizará o estudo de divisores para descobrir quais palavras-chave da lista deverá usar para decifrar a mensagem.

Por fim, o grupo dos decodificadores e espiões entregam a resposta da mensagem ao docente, após terem decifrado.

Resolução dos codificadores: Eles irão iniciar escrevendo a palavra-chave na tabela dada pelo professor, anexado na Seção A.1. Em seguida, enumeram-se as letras da palavra-chave de acordo com a ordem alfabética e depois escreve a mensagem horizontalmente, abaixo da palavra-chave, linha por linha, resultando na Figura 4.2.

Figura 4.2: Codificando.

ORDEM	3	1	4	5	2
CHAVE	**M**	**A**	**R**	**T**	**E**
MENSAGEM	Q	U	A	N	T
	O	E	Q	U	I
	N	Z	E	M	A
	I	S	D	E	Z
	E	N	O	V	E

Fonte: Autor.

Finalizando o processo de codificação, escreve-se as letras da mensagem da coluna 1, em seguida a coluna 2 e assim por diante até finalizar, Figura 4.3.

Figura 4.3: Mensagem codificada.

MENSAGEM CODIFICADA (Ser entregue aos Decodificadores)
UEZSNTIAZEQONIEAQEDONUMEV

MENSAGEM CODIFICADA (Ser entregue aos Espiões)
UEZSNTIAZEQONIEAQEDONUMEV

Fonte: Autor.

Agora, com a mensagem codificada, um dos integrantes do grupo entrega para os grupos dos decodificadores e dos espiões.

Resolução dos decodificadores: com a mensagem codificada, Figura 4.3, e com a palavra-chave em mãos, inicia-se o processo de decodificação.

Os decodificadores contabilizam a quantidade de caracteres da mensagem recebida, neste caso, 25 caracteres e divide pela quantidade de letras da palavra-chave, 5 letras.

$$\frac{25}{5} = 5.$$

Depois, eles separam a mensagem recebida em blocos de 5 caracteres.

UEZSN - TIAZE - QONIE - AQEDO - NUMEV

Em seguida, decodificam a mensagem utilizando a palavra-chave, Figura 4.4.

Figura 4.4: Decodificando.

ORDEM	3	1	4	5	2
CHAVE	**M**	**A**	**R**	**T**	**E**
MENSAGEM	Q	U	A	N	T
	O	E	Q	U	I
	N	Z	E	M	A
	I	S	D	E	Z
	E	N	O	V	E

Fonte: Autor.

Por fim, a mensagem decodificada, Tabela 4.1.

Tabela 4.1: Mensagem decodificada.

Mensagem Legível
QUANTO É QUINZE MAIS DEZENOVE

Resolução dos espiões: os membros desse grupo irão primeiro contar o número de caracteres, neste caso, 25 caracteres, em seguida, calcularão os seus divisores.

$$D(25) = \{1, 5, 25\}$$

Dessa forma, o tamanho da palavra-chave é de 5 letras, pois descarta-se o menor e o maior divisor. Observando a lista de palavras-chave dada:

PLUTÃO - MARTE - JÚPITER - SATURNO - NETUNO - VÊNUS

Nota-se que somente as palavras MARTE e VÊNUS tem 5 letras. Então os espiões devem usar as duas para decifrar a mensagem.

Como as palavras-chave encontradas tem 5 letras, divide-se a quantidade de caracteres da mensagem interceptada por 5.

$$\frac{25}{5} = 5.$$

Assim, eles irão separar a mensagem recebida em blocos de 5 caracteres.

UEZSN - TIAZE - QONIE - AQEDO - NUMEV

Em seguida, decifram a mensagem utilizando as palavras-chave, Figura 4.5:

Figura 4.5: Decifrando.

ORDEM	3	1	4	5	2
CHAVE	**M**	**A**	**R**	**T**	**E**
MENSAGEM	Q	U	A	N	T
	O	E	Q	U	I
	N	Z	E	M	A
	I	S	D	E	Z
	E	N	O	V	E

Mensagem
QUANTOEQUINZEMAISDEZENOVE

ORDEM	5	1	2	4	3
CHAVE	**V**	**E**	**N**	**U**	**S**
MENSAGEM	N	U	T	A	Q
	U	E	I	Q	O
	M	Z	A	E	N
	E	S	Z	D	I
	V	N	E	O	E

Mensagem
NUTAQUEIQOMZAENESZDIVNEOE

Fonte: Autor.

Eles irão observar que a palavra-chave VENUS não tornou a mensagem legível e a palavra-chave MARTE exibe uma mensagem legível:

QUANTO É QUINZE MAIS DEZENOVE

Por fim, o grupo informa ao professor a resposta da mensagem.

$$15 + 19 = 34.$$

O grupo dos espiões efetua mais cálculos comparado aos demais grupos e aplicam o estudo de divisores, com isso, propõe-se uma atividade extra a seguir, para que todos os grupos possam efetuar o estudo sobre os divisores.

4.1.1.1 Atividade Extra - Todos são Espiões

Após a dinâmica, pode-se trabalhar a questão de divisores com todos os grupos. A seguir é dada a mensagem codificada e uma lista das possíveis palavras-chave, de modo que os grupos tentem decifrar a mensagem, conforme Figuras 4.6 e 4.7.

Figura 4.6: Mensagem Codificada.

MENSAGEM
ASNIASSRMQRISREVIOCTCDEEUEOOUNEVDON

Fonte: Autor.

Figura 4.7: Lista das Possíveis Chaves.

LISTA DAS POSSÍVEIS CHAVES					
CADERNO	ESTOJO	PROFESSORA	LAPIS	PAPEL	COLA
ESCOLA	QUADRO	TESOURA	RÉGUA	COMPUTADOR	APAGADOR
GEOGRAFIA	PINCEL	QUADRA	BOLA	MATEMATICA	FÍSICA

Fonte: Autor.

Resolução:

A mensagem "ASNIASSRMQRISREVIOCTCDEEUEOOUNEVDON" possui 35 *caracteres, sabendo disso, calcula-se os seus divisores.*

$$D(35) = \{1, 5, 7, 35\}.$$

Em seguida, observa-se a lista de palavras-chaves com essas quantidades de caracteres, 5 *ou* 7 *letras, como apresentado na Figura 4.8.*

Figura 4.8: As palavras-chave para tentar decifrar.

LISTA DAS POSSÍVEIS CHAVES					
CADERNO	ESTOJO	PROFESSORA	LAPIS	PAPEL	COLA
ESCOLA	QUADRO	TESOURA	RÉGUA	COMPUTADOR	APAGADOR
GEOGRAFIA	PINCEL	QUADRA	BOLA	MATEMATICA	FÍSICA

Fonte: Autor.

Os grupos tentarão descobrir qual das palavras-chave decifrará a mensagem. Por fim, encontrará que a palavra-chave correta é "TESOURA".

Como há 7 letras, efetua-se a divisão $\frac{35}{7} = 5$*, portanto, a mensagem é separada em blocos de 5 letras.*

ASNIA - SSRMQ - RISRE - VIOCT - CDEEU - EOOUN - EVDON

Em seguida, decifrando a mensagem, conforme Figura 4.9.

Figura 4.9: Mensagem Decifrada.

ORDEM	6	2	5	3	7	4	1
CHAVE	**T**	**E**	**S**	**O**	**U**	**R**	**A**
MENSAGEM	E	S	C	R	E	V	A
	O	S	D	I	V	I	S
	O	R	E	S	D	O	N
	U	M	E	R	O	C	I
	N	Q	U	E	N	T	A

Fonte: Autor.

Dessa forma, a mensagem encontrada é "Escreva os divisores do número cinquenta". Respondendo a pergunta:

$$D(50) = \{1, 2, 5, 10, 25, 50\}.$$

4.1.2 Dinâmica - Cifra de César

Conteúdo: Cifra de César.
Público alvo: Fundamental II e Ensino Médio.
Organização: Grupo de 4 a 5 alunos.
Duração: 90 minutos.
Objetivos: Codificar, Decodificar e Decifrar a Cifra de César.
Recursos: Anexados no Apêndice, Seção A.2.

O professor pode começar a aula abordando a importância de manter uma comunicação segura e discutir as possíveis consequências caso a comunicação de pessoas influentes seja comprometida. Em seguida, pode explicar como César garantia a segurança de suas mensagens, consultando a Seção 2.1.5 para obter mais informações.

Recomenda-se que os grupos dos codificadores e decodificadores tenham até 5 alunos e o grupo dos espiões podem ter mais alunos, devido o esforço para tentar descobrir a chave. Itens iniciais de cada grupo:

- *Codificadores* - Possuem uma mensagem e a chave de codificação, conforme Figura 4.10.

Figura 4.10: Informações - Codificadores.

MENSAGEM
Informe qual é o menor número primo ímpar

CHAVE																									
Alfabeto Original	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Fonte: Autor.

- *Decodificadores* - Tem a chave de decodificação, conforme Figura 4.11.

Figura 4.11: Informações - Decodificadores.

CHAVE																									
Alfabeto Original	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Fonte: Autor.

- *Espiões* - Possuem uma lista de possíveis chaves, Figura 4.12.

Figura 4.12: Informações - Espiões.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Fonte: Autor.

O professor entrega as informações de cada grupo, de forma isolada, sem que os outros grupos possam ouvir ou ver.

Em seguida, o processo inicia-se pelo grupo dos codificadores, codificando a mensagem duas vezes em um pedaço de papel. Depois, um dos integrantes do grupo entregará a mensagem aos grupos dos decodificadores (destinatário) e dos espiões (interceptadores).

Os decodificadores utilizam a chave para decodificar a mensagem, enquanto os espiões utilizam as possíveis chaves para decifrar a mensagem, por meio de tentativa e erro.

Quando ambos tornarem a mensagem legível, um integrante de cada grupo entrega a resposta ao professor da sala.

Resolução dos codificadores: codificando a mensagem utilizando a chave, Figura 4.13.

Figura 4.13: Mensagem e a Chave de Codificação.

MENSAGEM
Informe qual é o menor número primo ímpar

CHAVE																										
Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Fonte: Autor.

Substituindo cada letra, obtém-se:

Mensagem Codificada: SXPYBWO AEKV O Y WOXYB XEWOBY ZBSWY SWZKB

Escreve-se a mensagem codificada em dois pedaços de papel, Figura 4.14.

Figura 4.14: Mensagem codificada.

MENSAGEM CODIFICADA (Ser entregue aos Decodificadores)
SXPYBWO AEKV O Y WOXYB XEWOBY ZBSWY SWZKB

MENSAGEM CODIFICADA (Ser entregue aos Espiões)
SXPYBWO AEKV O Y WOXYB XEWOBY ZBSWY SWZKB

Fonte: Autor.

Em seguida, um dos integrantes da equipe entregará a mensagem aos grupos decodificadores e espiões.

Resolução dos decodificadores: decodificando a mensagem utilizando a chave, Figura 4.15.

Figura 4.15: Chave dos Decodificadores.

CHAVE																									
Alfabeto Original	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Fonte: Autor.

Substituindo cada letra, obtém-se:

Mensagem Decodificada: INFORME QUAL E O MENOR NUMERO PRIMO IMPAR

Organizando a mensagem:

INFORME QUAL É O MENOR NÚMERO PRIMO ÍMPAR

Sendo a resposta correta da mensagem o número 3*. Ao responder, um dos integrantes do grupo entrega a resposta ao professor.*

Resolução dos espiões: decifrando a mensagem utilizando a lista de chaves, Figura 4.16.

Figura 4.16: Lista de Chaves.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Fonte: Autor.

O grupo tem que dividir todas as chaves entre os membros para realizar a atividade com mais rapidez, em seguida eles tentam decifrar a mensagem testando cada chave. Até que encontre a chave correta, Figura 4.17.

Figura 4.17: Chave Correta.

CHAVE																										
Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Fonte: Autor.

Substituindo cada letra, obtém-se:

Mensagem Decifrada: INFORME QUAL E O MENOR NUMERO PRIMO IMPAR

Organizando a mensagem:

INFORME QUAL É O MENOR NÚMERO PRIMO ÍMPAR

Um dos integrantes do grupo entrega a resposta ao professor, sendo a resposta correta da mensagem o número 3*.*

Observação 4.1.2. *Após todos concluírem, o professor pode compartilhar o método utilizado pelo grupo dos espiões para conseguir decifrar a mensagem.*

Um dos métodos que facilitaria o processo de decifração é tentar decifrar uma das palavras da mensagem para observar se há algo legível.

Observe a primeira palavra da mensagem codificada, ***SXPYBWO****, sendo substituída por cada chave.*

1ª Chave: QVNWZUM - *Não legível.*

2ª Chave: OTLUXSK - *Não legível.*

3ª Chave: MRJSYQI - *Não legível.*

4ª Chave: KPHQTOG - *Não legível.*

5ª Chave: INFORME - *Legível, possível chave.*

6ª Chave: FKCLOJB - *Não legível.*

7ª Chave: DIAJMHZ - *Não legível.*

8ª Chave: XCUDGBT - *Não legível.*

9ª Chave: BGYHKFX - *Não legível.*

10ª Chave: AFXGJEW - *Não legível.*

Dessa forma, encontrará que a 5ª chave decifrará a mensagem codificada.

4.1.2.1 Atividade Extra - Todos são espiões

Após a dinâmica, o professor pode realizar o processo dos espiões com todos os grupos. De acordo com a dificuldade do grupo dos espiões durante a primeira dinâmica, o professor pode permanecer com os grupos ou alterar a quantidade de alunos por grupo. O processo ocorrerá da mesma maneira, com uma mensagem codificada e dez chaves aleatórias, Figura 4.18, dentre elas a chave que decodifica a mensagem.

Figura 4.18: Lista das possíveis chaves.

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

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

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

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

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

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

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

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

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

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

Fonte: Autor.

A seguir, tem-se a mensagem codificada, Figura 4.19.

Figura 4.19: Mensagem codificada.

MENSAGEM CODIFICADA
KOUHNI Y PCHNY GUCM NLCHNU Y XICM

Fonte: Autor.

Na mensagem codificada há uma pergunta, os alunos devem entregar a resposta ao professor.

Resolução:

Dada a lista de chaves, Figura 4.18:
Decifra-se a mensagem "KOUHNI Y PCHNY GUCM NLCHNU Y XICM" utilizando o método de substituir a primeira palavra com cada chave:

1ª Chave: LPVIOJ - *Não legível.*
2ª Chave: OSULRM - *Não legível.*
3ª Chave: EIOBHC - *Não legível.*
4ª Chave: SWCPVQ - *Não legível.*
5ª Chave: IMSFLG - *Não legível.*
6ª Chave: XBHUAV - *Não legível.*
7ª Chave: QUANTO - *Legível, possível chave.*
8ª Chave: JNTGMH - *Não legível.*
9ª Chave: PTZMSN - *Não legível.*
10ª Chave: ZDJWCX - *Não legível.*

Substituindo o restante da mensagem utilizando a 7ª Chave, Figura 4.20.

Figura 4.20: 7ª Chave.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Fonte: Autor.

Mensagem Decifrada: QUANTO E VINTE MAIS TRINTA E DOIS

Organizando a mensagem, tem-se "Quanto é vinte mais trinta e dois?", então um integrante da equipe entregará a resposta ao professor, sendo a resposta 52.

4.1.3 Dinâmica - Função Afim e Função Inversa

Conteúdo: Criptografia com Função Afim e Função Inversa.
Público alvo: 1º Ano do Ensino Médio.
Organização: Grupos de até 6 alunos.
Duração: 100 minutos.
Objetivos: Praticar o conceito de Função Afim e Função Inversa através de Criptografia.
Recursos: Anexados no Apêndice, Seção A.3.

Nessa atividade, o professor pode falar a respeito da importância da criptografia para manter uma comunicação segura, com isso, cita que o objetivo da aula é criptografar mensagens através de função. É importante que o professor apresente um exemplo de codificação e decodificação no quadro, em seguida de como decifrar uma mensagem conhecendo a função que foi utilizada para codificar. Alguns exemplos são apresentados na Seção 3.4.

Os grupos podem ser formados por até 6 alunos, nesse assunto abordado, todos os grupos terão que realizar cálculos para finalizar o processo. Importante ressaltar, que as informações dadas de cada grupo a seguir, devem ser entregues de forma isolada para cada equipe, de modo que os outros grupos não possam ver.

- *Codificadores* - Possuem uma mensagem, a tabela de conversão de letra para números e a chave de codificação, Figura 4.21.

Figura 4.21: Informações - Codificadores.

MENSAGEM
Qual é a raiz quadrada de dezesseis

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

CHAVE dos Codificadores
$\mathbf{f(x) = 2x + 3}$

Fonte: Autor.

- *Decodificadores* - Tem a tabela de conversão de letra para números e a chave de decodificação, Figura 4.22.

Figura 4.22: Informações - Decodificadores.

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

CHAVE dos Decodificadores
$\mathbf{f(x) = \dfrac{x - 3}{2}}$

Fonte: Autor.

- *Espiões* - Possuem a tabela de conversão de letra para números e a chave utilizada para codificar, Figura 4.23.

Figura 4.23: Informações - Espiões.

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

CHAVE dos Codificadores
$\mathbf{f(x) = 2x + 3}$

Fonte: Autor.

O grupo dos codificadores inicia o processo para codificar a mensagem, ao terminar, um dos integrantes do grupo entregará a mensagem ao grupo dos decodificadores e ao grupo dos espiões, simulando a interceptação.

O grupo dos decodificadores possui a chave de decodificação e a tabela de conversão, com isso, decodificará a mensagem.

O grupo dos espiões tem a chave que foi utilizada para codificar a mensagem, com isso, eles terão que encontrar a sua função inversa, que será a chave de decodificação, ao encontrá-la deve utilizá-la para decifrar a mensagem.

Ao terminar todos os processos, os grupos respondem a pergunta da mensagem e entrega ao professor.

Resolução dos codificadores:

Codificando a mensagem:

Primeiro, converte-se as letras da mensagem "Qual é a raiz quadrada de dezesseis" em números, utilizando a Figura 4.24.

Figura 4.24: Substituição de letras para números.

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

Fonte: Autor.

Conversão de letra para números:

$$17 - 21 - 1 - 12 - 5 - 1 - 18 - 1 - 9 - 26 - 17 - 21 - 1 - 4 - 18 - 1 - 4 - 1 - 4 - 5 - 4 - 5 - 26 - 5 - 19 - 19 - 5 - 9 - 19.$$

Em seguida, utiliza-se a chave de codificação, conforme a Figura 4.25.

Figura 4.25: Chave de codificação.

CHAVE
$\mathbf{f(x) = 2x + 3}$

Fonte: Autor.

Codificando:

$$\begin{aligned} f(17) &= 2(17) + 3 = 37 \\ f(21) &= 2(21) + 3 = 45 \\ f(1) &= 2(1) + 3 = 5 \\ f(12) &= 2(12) + 3 = 27 \\ f(5) &= 2(5) + 3 = 13 \\ f(18) &= 2(18) + 3 = 39 \\ f(9) &= 2(9) + 3 = 21 \\ f(26) &= 2(26) + 3 = 55 \\ f(4) &= 2(4) + 3 = 11 \\ f(19) &= 2(19) + 3 = 41 \end{aligned}$$

Depois, substituem-se os números que representam as letras pelos respectivos valores encontrados ao usarem a chave.

Mensagem Codificada: $37 - 45 - 5 - 17 - 13 - 5 - 39 - 5 - 21 - 55 - 37 - 45 - 5 - 1 - 39 - 5 - 11 - 5 - 11 - 13 - 11 - 13 - 55 - 13 - 41 - 41 - 13 - 21 - 41$

Por fim, escreve-se a mensagem codificada em dois pedaços de papel, Figura 4.26, e um dos integrantes do grupo entrega a mensagem aos grupos dos decodificadores e espiões.

Figura 4.26: Mensagem codificada.

MENSAGEM CODIFICADA (Ser entregue aos Decodificadores)
37 - 45 - 5 - 17 - 13 - 5 - 39 - 5 - 21 - 55 - 37 - 45 - 5 - 1 - 39 - 5 -
11 - 5 - 11 - 13 - 11 - 13 - 55 - 13 - 41 - 41 - 13 - 21 - 41

MENSAGEM CODIFICADA (Ser entregue aos Espiões)
37 - 45 - 5 - 17 - 13 - 5 - 39 - 5 - 21 - 55 - 37 - 45 - 5 - 1 - 39 - 5 -
11 - 5 - 11 - 13 - 11 - 13 - 55 - 13 - 41 - 41 - 13 - 21 - 41

Fonte: Autor.

Resolução dos decodificadores:

Para decodificar a mensagem:

$37 - 45 - 5 - 17 - 13 - 5 - 39 - 5 - 21 - 55 - 37 - 45 - 5 - 1 - 39 - 5 - 11 - 5 - 11 - 13 - 11 - 13 - 55 - 13 - 41 - 41 - 13 - 21 - 41.$

O grupo terá que utilizar a sua chave, Figura 4.27:

Figura 4.27: Chave de decodificação.

CHAVE dos Decodificadores
$\mathbf{f(x) = \frac{x-3}{2}}$

Fonte: Autor

Decodificando:

$$\begin{aligned} f(37) &= \frac{37-3}{2} = 17 \\ f(45) &= \frac{45-3}{2} = 21 \\ f(5) &= \frac{5-3}{2} = 1 \\ f(29) &= \frac{29-3}{2} = 13 \\ f(13) &= \frac{13-3}{2} = 5 \\ f(39) &= \frac{39-3}{2} = 18 \\ f(21) &= \frac{21-3}{2} = 9 \\ f(55) &= \frac{55-3}{2} = 26 \\ f(11) &= \frac{11-3}{2} = 4 \\ f(41) &= \frac{41-3}{2} = 19. \end{aligned}$$

Substituindo os valores, tem-se a seguinte mensagem: $17-21-1-12-5-1-18-1-9-26-17-21-1-4-18-1-4-1-4-5-4-5-26-5-19-19-5-9-19.$

Depois utiliza a tabela de conversão de números para letras, Figura 4.28:

Figura 4.28: Conversão de letra para números.

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

Fonte: Autor.

Mensagem Decodificada: QUALEARAIZQUADRADADEDEZESSEIS

Organizando a mensagem, tem-se "Qual é a raiz quadrada de dezesseis", com isso, os alunos levarão a resposta ao professor, sendo ela o número 4.

Resolução dos espiões: para decifrar a mensagem, os espiões precisam encontrar a função inversa de $f(x) = 2x + 3$. *Dessa forma, substitui* $f(x)$ *por* y*:*

$$y = 2x + 3.$$

Depois, invertem-se as variáveis x *e* y*:*

$$x = 2y + 3.$$

Em seguida, eles calcularão a função inversa, isolando a variável y*:*

$$\begin{aligned} x &= 2y + 3 \\ 2y + 3 &= x \\ 2y &= x - 3 \\ y &= \frac{x-3}{2} \end{aligned}$$

Assim, eles encontrarão a chave para decifrar a mensagem:

$$\boxed{f^{-1}(x) = \frac{x-3}{2}}$$

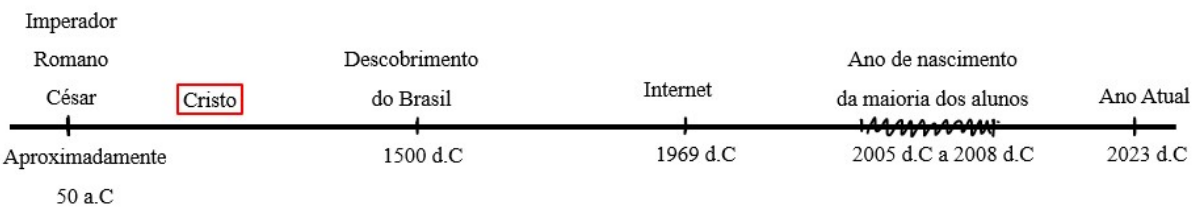
O restante do processo ocorre de maneira análoga à resolução do grupo dos decodificadores, calculando os valores da mensagem codificada na função inversa, em seguida substituindo os resultados por letras na tabela de conversão de número para letras.

4.2 Atividade 2 - Cifra de César

Conteúdo: Cifra de César.
Público alvo: Fundamental II e Ensino Médio.
Organização: Grupo de 3 a 5 alunos.
Duração: 90 minutos.
Objetivos: Codificar, Decodificar e Decifrar a Cifra de César.
Anexo: Atividade sem resolução, Seção A.4.

Fica como sugestão fazer uma linha do tempo voltando até a época de César. (Figura 4.29).

Figura 4.29: Linha do tempo.



Fonte: Autor.

Iniciando pelo contexto atual, estamos no ano de 2023. Agora, vamos retroceder no tempo e calcular o intervalo de nascimento da maioria dos alunos, que geralmente é de 15 a 18 anos antes do ano atual. Viajando até 1969, ano do surgimento da internet, podemos perceber que antes disso, a internet como os alunos conhecem não existia. Era um mundo diferente, onde não existia essa comunicação que os alunos conhecem hoje.

Vamos agora fazer uma viagem ainda mais distante, até o ano de 1500, quando o Brasil foi descoberto. Nessa época, o ambiente que os alunos conhecem hoje era habitado apenas por indígenas. É importante ressaltar que todos esses anos são relatados como depois de Cristo. Pois, agora, voltando para tempo antes de Cristo, aproximadamente 50 a.C, vamos nos concentrar no período do Imperador Romano César. César tinha legiões distantes de seu império e precisava se comunicar com elas. Você sabe como ele fazia isso?

Espera-se que os alunos respondam "através de cartas" ou algo semelhante. Em seguida, podemos perguntar como as cartas eram transportadas, e a resposta mais comum é "por mensageiros". Agora, podemos informar aos alunos sobre um problema que ocorria na época: alguns mensageiros eram emboscados por inimigos, que interceptavam as cartas de César.

Assim, surge a pergunta: como César poderia enviar mensagens para suas legiões, de forma que os inimigos não descobrissem o conteúdo caso os mensageiros fossem emboscados?

Com base nas respostas dos alunos, o professor pode fazer considerações e, em seguida, explicar o método utilizado por César. Recomenda-se que o professor faça um exemplo de codificação e depois decodificação. Então, informa-se aos alunos que esse processo de elaborar uma escrita secreta é conhecido como *criptografia*.

Em seguida, os alunos podem ser divididos em grupos de 3 a 5 alunos para praticar o método utilizado por César. Eles devem utilizar a tabela criada por César para responder as questões 1 e 2, Figura 4.30. É importante prestar atenção na questão 3 para que os alunos escrevam o alfabeto codificado no modo correto de translação, evitando preenchê-lo com letras de forma aleatória.

Figura 4.30: Tabela de César.

Alfabeto Original	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Alfabeto Codificado	D	E	F	G	H	I	J	K	L	M	N	O	P

Alfabeto Original	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto Codificado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: Autor.

Questão 1: Utilizando a tabela de cifra de César, codifique a seguinte mensagem: "*Reforce a proteção dos mensageiros, pois tem suspeita de emboscada na estrada*".

Resolução: Utilizando a tabela de Cifra de César substituindo cada letra, obterá a seguinte mensagem codificada:

UHIRUFH D SURWHFDR GRV PHQVDJHLURV SRLV WHP VXVSHLWD GH HPERVFDGD QD HVWUDGD

Questão 2: César enviou a seguinte mensagem para a legião do Oeste:

"**WUDQVSRUWH RV DOLPHQWRV SDUD D OHJLDR GR VXO**"

Decodifique-o utilizando a tabela de César.

Resolução: Utilizando a tabela de Cifra de César faz o processo inverso para poder tornar a mensagem legível, com isso, obtém a mensagem:

TRANSPORTE OS ALIMENTOS PARA A LEGIÃO DO SUL

Questão 3: César criou o alfabeto codificador transladando o alfabeto três posições a frente. Dessa forma, crie seu próprio alfabeto codificador transladando-o uma quantidade de posições diferente de César.

Figura 4.31: Cifra em branco.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfabeto Codificado													

Alfabeto Original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado													

Fonte: Autor.

Resolução: Resposta pessoal.

Observação 4.2.1. *A tabela tem que ser preenchida de forma a transladar o alfabeto, ou seja, não pode distribuir as letras de forma aleatória na tabela.*

Questão 4: De quantas maneiras César poderia transladar o alfabeto, de modo que a mensagem fique codificada?

Resolução: 25 maneiras, pois o alfabeto codificador pode iniciar com a letra B ou C ou D ou ... ou Z. Descarta-se somente o início com a letra A, pois é o alfabeto original.

Questão 5: Elabore uma pergunta pedindo para calcular a soma de dois números e codifique-a utilizando a tabela da questão 3.

Observação 4.2.2. *Outro grupo irá decodificar o que você escreveu e responder. (Escreva a mesma frase codificada e a primeira letra do seu alfabeto codificado em um pedaço de papel para entregar a outra equipe)*

Mensagem Legível:

Mensagem Codificada:

Figura 4.32: Mensagem codificada e a 1º Letra do alfabeto codificado.

MENSAGEM CODIFICADA	1ª Letra do Alfabeto Codificado

Fonte: Autor.

Resolução: Resposta Pessoal

Questão 6: Tente decodificar e responder a mensagem da outra equipe.

Resolução: Resposta Pessoal

4.3 Atividade 3 - Método Retangular

Conteúdo: Método retangular e divisores positivos de um número natural.
Público alvo: Alunos do Ensino Fundamental II.
Organização: Grupo de 3 a 5 alunos.
Duração: 90 minutos.
Objetivo: Resolver problemas envolvendo divisores positivos de um número natural.
Anexo: Atividade sem resolução, Seção A.5.

Inicialmente, o professor deve explicar a criptografia do Método Retangular, os modos de codificar, decodificar e decifrar a partir de uma lista de palavras-chave. O assunto do Método Retangular encontra-se na Seção 2.1.3.

O Exemplo 9, da Seção 3.1.1, mostra como identificar os possíveis tamanhos da palavra-chave.

Questão 1: Sendo a palavra-chave SOMAR, utilize o método retangular para codificar a mensagem "*Os divisores podem quebrar a criptografia do método retangular*".

Resolução:

Preenchendo a tabela do método retangular, Figura 4.33:

Figura 4.33: Codificando a mensagem.

ORDEM	5	3	2	1	4
CHAVE	**S**	**O**	**M**	**A**	**R**
MENSAGEM	O	S	D	I	V
	I	S	O	R	E
	S	P	O	D	E
	M	Q	U	E	B
	R	A	R	A	C
	R	I	P	T	O
	G	R	A	F	I
	A	D	O	M	E
	T	O	D	O	R
	E	T	A	N	G
	U	L	A	R	#

Fonte: Autor.

Unindo as colunas da mensagem de acordo com a ordem alfabética da palavra-chave.

Mensagem Codificada: IRDEATFMONRDOOURPAODAASSPQAIRDOTLVEEBCOIERG#OISMRRGATEU

Questão 2: Desvende a mensagem secreta a seguir, sabendo que foi utilizado o método Retangular e a palavra-chave é NÚMERO.

LPEMIAIMURQTDROOOOROELNEMURONP

Resolução:

Note que a mensagem tem 30 *caracteres e a palavra-chave "NÚMERO" tem* 6 *letras, portanto, divide* 30 *por* 6*, que resultará em* 5*. Dessa forma, cada bloco terá* 5 *caracteres.*

LPEMI - AIMUR - QTDRO - OOORO - ELNEM - URONP

Depois, enumeram-se as letras da palavra-chave em ordem alfabética, Tabela 4.2:

Tabela 4.2: Letras da palavra-chave enumerada em ordem alfabética.

3	6	2	1	5	4
N	**U**	**M**	**E**	**R**	**O**

Em seguida, escreve-se o primeiro bloco verticalmente abaixo da primeira letra em ordem alfabética da palavra-chave, o segundo bloco abaixo da segunda letra em ordem alfabética, assim sucessivamente até terminar todos os blocos, Tabela 4.3.

Tabela 4.3: Mensagem decodificada.

3	6	2	1	5	4
N	**U**	**M**	**E**	**R**	**O**
Q	U	A	L	E	O
T	R	I	P	L	O
D	O	M	E	N	O
R	N	U	M	E	R
O	P	R	I	M	O

Por fim, lê-se a mensagem horizontalmente, "QUAL É O TRIPLO DO MENOR NÚMERO PRIMO", respondendo a pergunta, $3 \cdot 2 = 6$.

Questão 3: Os alunos do 8º ano estão utilizando a criptografia do método retangular para comunicar-se secretamente. Carlos, interceptou uma das mensagens de seus colegas:

SNAISRIOUUNAOOVSNAPIDORRIESENIDCSATMEQULHNARAMASA

Sabe-se que uma das palavras a seguir é a palavra-chave, então descubra através dos divisores qual delas é a palavra-chave e torne a mensagem legível.

ESCOLA - VÔLEI - ATO - FUTEBOL - DATE

Resolução:

Deve-se contar a quantidade de caracteres da mensagem " SNAISRIOUUNAOOVSNAPIDORRIESENIDCSATMEQULHNARAMASA", sendo assim, observa-se 49 *caracteres. Agora, encontra-se os divisores positivos de* 49*:*

$$D(49) = \{1, 7, 49\}$$

Ao descartar os divisores 1 *e* 49*, sobrará o divisor* 7*. Portanto, dentre as alternativas, a palavra-chave é FUTEBOL.*

Agora, deve-se dividir 49 *por* 7*, resultando em* 7*, então a mensagem tem que ser separadas em blocos de 7 caracteres.*

SNAISRI - OUUNAOO - VSNAPID - ORRIESE - NIDCSAT - MEQULHN - ARAMASA

Aplicando na criptografia do método retangular, obtém-se, Figura 4.34

Figura 4.34: Decifrando a mensagem.

ORDEM	3	7	6	2	1	5	4
CHAVE	**F**	**U**	**T**	**E**	**B**	**O**	**L**
MENSAGEM	V	A	M	O	S	N	O
	S	R	E	U	N	I	R
	N	A	Q	U	A	D	R
	A	M	U	N	I	C	I
	P	A	L	A	S	S	E
	I	S	H	O	R	A	S
	D	A	N	O	I	T	E

Fonte: Autor.

Dessa forma, a mensagem decifrada é "Vamos nos reunir na quadra municipal as seis horas da noite".

Questão 4: Duas mensagens foram interceptadas, sabe-se que o algoritmo utilizado é do método retangular. Com isso, descubra os possíveis tamanhos da palavra-chave.

Mensagem 1: "OCIEADET#NSNOTNTPSSAUÇSENEAASMAESICDSOCSOORA#"

Mensagem 2: "EEADAASSULMASVMROCDNNCASMOESOCIOEEOMNECDOHA-FAMGREUTIMLRIÇSAPRGAT#"

Resolução:

A primeira mensagem tem 45 caracteres e a segunda mensagem tem 65 caracteres. Calcula-se os divisores de ambos:

$$\begin{aligned} D(45) &= \{1, 3, 5, 9, 15, 45\}. \\ D(65) &= \{1, 5, 13, 65\}. \end{aligned}$$

Note que o divisor 1 *e* 5 *são os termos comuns, mas descarta-se o divisor* 1*, dessa forma, a palavra-chave tem* 5 *letras.*

Ao final da atividade, o professor pode questionar por que os divisores podem acelerar o processo de decifragem. A resposta está relacionada ao fato de que a quantidade de caracteres da mensagem será um múltiplo do tamanho da palavra-chave. Portanto, o tamanho da palavra-chave é um dos divisores da quantidade de caracteres da mensagem.

Por exemplo, na questão 1, a palavra-chave é "SOMAR", com 5 letras, e a mensagem codificada possui 55 caracteres. É importante observar que 55 é um múltiplo de 5, ou seja, 5 é um divisor de 55.

4.4 Atividade 4 - Criptografia com Função Afim e Função Inversa

Conteúdo: Criptografia com Função Afim e Função Inversa.
Público alvo: 1º Ano do Ensino Médio.
Organização: Grupos de até 5 alunos.
Duração: 100 minutos.
Objetivo: Praticar o conceito de Função Afim e Função Inversa através de Criptografia.
Anexo: Atividade sem resolução, Seção A.6.

O professor pode começar a aula destacando a importância da segurança na comunicação e mencionar que os alunos aprenderão a codificar uma mensagem usando funções, enfatizando a relevância de manter certos dados privados para evitar que terceiros possam decifrar as mensagens. Para ilustrar esses conceitos, pode-se utilizar o conteúdo e exemplos da Seção 3.4 como referência durante a aula.

Questão 1: Dado a tabela de pré-codificação, Tabela 4.4, utilize a função $f(x) = 6x - 4$, para codificar a mensagem *"Amanhã vamos estudar somente matemática"*.

Tabela 4.4: Alfabeto.

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

Resolução:

Primeiramente, converte-se a mensagem em valores numéricos de acordo com a Tabela 4.4:

$$\begin{aligned} \textit{Mensagem Original} &= \textit{Amanhã vamos estudar somente matemática} \\ \textit{Mensagem Pré-Codificada} &= 1-13-1-14-8-1-22-1-13-15-19- \\ &\quad 5-19-20-21-4-1-18-19-15-13- \\ &\quad 5-14-20-5-13-1-20-5-13-1-20- \\ &\quad 9-3-1 \end{aligned}$$

Agora, utiliza-se a função $f(x) = 6x - 4$, para codificar cada número.

$$
\begin{aligned}
f(1) &= 6(1) - 4 = 2 \\
f(13) &= 6(13) - 4 = 74 \\
f(14) &= 6(14) - 4 = 80 \\
f(8) &= 6(8) - 4 = 44 \\
f(22) &= 6(22) - 4 = 128 \\
f(15) &= 6(15) - 4 = 86 \\
f(19) &= 6(19) - 4 = 110 \\
f(5) &= 6(5) - 4 = 26 \\
f(20) &= 6(20) - 4 = 116 \\
f(21) &= 6(21) - 4 = 122 \\
f(4) &= 6(4) - 4 = 20 \\
f(18) &= 6(18) - 4 = 104 \\
f(9) &= 6(9) - 4 = 50 \\
f(3) &= 6(3) - 4 = 14
\end{aligned}
$$

Dessa forma, tem-se a mensagem codificada:

$$2 - 74 - 2 - 80 - 44 - 2 - 128 - 2 - 74 - 86 - 110 - 26 - 110 - 116 - 122 - 20 - 2 - 104 - 110 - 86 - 74 - 26 - 80 - 116 - 26 - 74 - 2 - 116 - 26 - 74 - 2 - 116 - 50 - 14 - 2.$$

Questão 2: Seu amigo te enviou a seguinte mensagem secreta:

$$18 - 54 - 18 - 57 - 39 - 18 - 75 - 30 - 69 - 18 - 78 - 54 - 18 - 33 - 30 - 72 - 75 - 18 - 57 - 18 - 54 - 42 - 57 - 39 - 18 - 24 - 18 - 72 - 18.$$

Sabendo que a sua chave de decodificação é $y = \dfrac{x-15}{3}$, torne a mensagem legível. Utilize a Tabela 4.4.

Resolução:

Deve-se substituir os valores da mensagem codificada na função $f(x) = \dfrac{x-15}{3}$.

$$f(18) = \frac{18-15}{3} = \frac{3}{3} = 1$$

$$f(54) = \frac{54-15}{3} = \frac{39}{3} = 13$$

$$f(57) = \frac{57-15}{3} = \frac{42}{3} = 14$$

$$f(39) = \frac{39-15}{3} = \frac{24}{3} = 8$$

$$f(75) = \frac{75-15}{3} = \frac{60}{3} = 20$$

$$f(30) = \frac{30-15}{3} = \frac{15}{3} = 5$$

$$f(69) = \frac{69-15}{3} = \frac{54}{3} = 18$$

$$f(78) = \frac{78-15}{3} = \frac{63}{3} = 21$$

$$f(33) = \frac{33-15}{3} = \frac{18}{3} = 6$$

$$f(72) = \frac{72-15}{3} = \frac{57}{3} = 19$$

$$f(42) = \frac{42-15}{3} = \frac{27}{3} = 9$$

$$f(24) = \frac{24-15}{3} = \frac{9}{3} = 3.$$

Portanto, utiliza-se a tabela dada na questão para substituir os valores às letras correspondentes. Finalizando na Figura 4.35.

Figura 4.35: Decodificação.

Mensagem Codificada	18	54	18	57	39	18	75	30	69	18	78	54	18	33	30	72	75	18	57	18	54	42	57	39	18	24	18	72	18
Pré-Codificação	1	13	1	14	8	1	20	5	18	1	21	13	1	6	5	19	20	1	14	1	13	9	14	8	1	3	1	19	1
Mensagem Decodificada	**A**	**M**	**A**	**N**	**H**	**A**	**T**	**E**	**R**	**A**	**U**	**M**	**A**	**F**	**E**	**S**	**T**	**A**	**N**	**A**	**M**	**I**	**N**	**H**	**A**	**C**	**A**	**S**	**A**

Fonte: Autor.

A mensagem recebida é "Amanhã terá uma festa na minha casa".

Questão 3: Ana, Beatriz e Carla enviam mensagens secretas para seus respectivos melhores amigos, Daniel, Elias e Fábio, cada uma tem sua chave, sabendo que as chaves são funções afim, destacadas na Tabela 4.5, descubra a chave de cada um dos seus melhores amigos.

Tabela 4.5: Chaves.

Ana	Daniel
$y = 4x - 7$	

Beatriz	Elias
$y = 5x + 9$	

Carla	Fábio
$y = \frac{2x+5}{15}$	

Resolução: Deve-se calcular a função inversa de cada um dos melhores amigos, então:

- *Daniel*

$$\begin{aligned} x &= 4y - 7 \\ 4y - 7 &= x \\ 4y &= x + 7 \\ y &= \frac{x+7}{4} \end{aligned}$$

- *Elias*

$$\begin{aligned} x &= 5y + 9 \\ 5y + 9 &= x \\ 5y &= x - 9 \\ y &= \frac{x-9}{5} \end{aligned}$$

- *Fábio*

$$\begin{aligned} x &= \frac{2y+5}{15} \\ \frac{2y+5}{15} &= x \\ 2y + 5 &= 15x \\ 2y &= 15x - 5 \\ y &= \frac{15x-5}{2} \end{aligned}$$

Assim, preenche-se a Tabela 4.6:

Tabela 4.6: Resposta.

Ana	Daniel
$y = 4x - 7$	$y = \frac{x+7}{4}$

Beatriz	Elias
$y = 5x + 9$	$y = \frac{x-9}{5}$

Carla	Fábio
$y = \frac{2x+5}{15}$	$y = \frac{15x-5}{2}$

Questão 4: Em relação à questão 3, uma das pessoas recebeu a seguinte mensagem "$119 - 14 - 74 - 84 - 104 - 14 - 84 - 24 - 54 - 79 - 34 - 74 - 14$", tente tornar a mensagem legível. Utilize a Figura 4.36.

Figura 4.36: Conversão de letra $\Leftrightarrow$ número.

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

Fonte: Autor.

Resolução: Como deve realizar um processo de decodificação com as funções da questão 3, os resultados encontrados devem ser um número natural e pertencer ao intervalo de 1 *a* 26*, pois são valores que podem ser substituído por letras.*

- *Testando a chave de Ana:*

  $f(119) = 4 \cdot 119 - 7 = 483$*, o resultado não pertence ao intervalo de* 1 *a* 26*, logo, chave incorreta.*

- Testando a chave de Daniel:
  $f(119) = \dfrac{119+7}{4} = \dfrac{126}{4} = 31,5$*, o resultado não pertence ao intervalo de* 1 *a* 26*, logo, chave incorreta.*

- *Testando a chave de Beatriz:*

  $f(119) = 5 \cdot 119 + 9 = 604$*, o resultado não pertence ao intervalo de* 1 *a* 26*, logo, chave incorreta.*

- *Testando a chave de Elias:*

$$
\begin{aligned}
f(119) &= \frac{119-9}{5} = \frac{110}{5} = 22\text{, o resultado representa a letra V.} \\
f(14) &= \frac{14-9}{5} = \frac{5}{5} = 1\text{, o resultado representa a letra A.} \\
f(74) &= \frac{74-9}{5} = \frac{65}{5} = 13\text{, o resultado representa a letra M.} \\
f(84) &= \frac{84-9}{5} = \frac{75}{5} = 15\text{, o resultado representa a letra O.} \\
f(104) &= \frac{104-9}{5} = \frac{95}{5} = 19\text{, o resultado representa a letra S.} \\
f(24) &= \frac{24-9}{5} = \frac{15}{5} = 3\text{, o resultado representa a letra C.} \\
f(54) &= \frac{54-9}{5} = \frac{45}{5} = 9\text{, o resultado representa a letra I.} \\
f(79) &= \frac{79-9}{5} = \frac{70}{5} = 14\text{, o resultado representa a letra N.} \\
f(34) &= \frac{34-9}{5} = \frac{25}{5} = 5\text{, o resultado representa a letra E.}
\end{aligned}
$$

Substituindo todas as letras nos valores correspondente, obtém, Figura 4.37.

Figura 4.37: Mensagem decodificada.

Mensagem Codificada	119	14	74	84	104	14	84	24	54	79	34	74	14
Pré-Codificação	22	1	13	15	19	1	15	3	9	14	5	13	1
Mensagem Decodificada	**V**	**A**	**M**	**O**	**S**	**A**	**O**	**C**	**I**	**N**	**E**	**M**	**A**

Fonte: Autor.

Atribuindo espaços na mensagem, obtém-se "Vamos ao cinema".

- *Testando a chave de Carla:*

  $f(119) = \dfrac{2 \cdot 119 + 5}{15} = \dfrac{243}{15} = 16,2$, *o resultado não é um número inteiro, logo, chave incorreta.*

- *Testando a chave de Fábio:*

  $f(119) = \dfrac{15 \cdot 119 - 5}{2} = \dfrac{1780}{2} = 890$, *o resultado não pertence ao intervalo de* 1 *a* 26*, logo, chave incorreta.*

Concluindo que Elias recebeu a mensagem.

Questão 5: Marque a alternativa que representa o remetente da mensagem enviada na questão 4.

a) Ana

b) Beatriz

c) Carla

d) Daniel

e) Elias

f) Fábio

Resolução: Se Elias recebeu a mensagem, então Beatriz que é a remetente da mensagem. Alternativa B.

4.5 Atividade 5 - Criptografia, Fatoração e Permutação

Conteúdo: Criptografia, Fatoração e Permutação.
Público alvo: 3º Ano do Ensino Médio.
Organização: Individual ou Grupo.
Duração: 90 minutos.
Objetivos: Resolver problemas envolvendo agrupamentos ordenáveis; Identificar e descrever o espaço amostral, Calcular a quantidade de divisores positivos de um número natural e identificá-los.
Anexo: Atividade sem resolução, Seção A.7.

Nessa atividade, o professor deve explicar inicialmente a codificação do Método Retangular, Seção 2.1.3, em seguida, mencionar que a atividade é focada em cálculos para decifrar a mensagem codificada pelo Método Retangular. Dessa forma, os focos principais são:

- Exemplificar quantos tamanhos distintos pode ter a palavra-chave de acordo com a mensagem codificada, Exemplo 18 da Seção 3.1.5.
- Saber os tamanhos de cada possível palavra-chave e identificar de quantas maneiras pode-se organizar as colunas de acordo com a possível palavra-chave, Exemplos 9 da Seção 3.1.1 e 21 da Seção 3.3.
- Calcular o máximo de tentativas para decifrar a mensagem, Exemplo 22 da Seção 3.3.

Questão 1: Maria recebeu uma mensagem codificada com o método retangular, porém, esqueceu da sua palavra-chave, só lembra que tinha 3 letras. Abaixo, têm-se a mensagem separado em três blocos, pois, sabe-se que a palavra-chave tem 3 letras.

AOURARL - QNEAOTI - UTQTFOA

Sabendo que os blocos são colunas, responda os seguintes itens:

a) De quantas maneiras diferente pode-se organizar essas colunas?

Resolução: Deve-se utilizar o estudo de permutação, como há 3 *colunas, então:*

$$P_3 = 3 \cdot 2 \cdot 1 = 6.$$

Logo, há 6 maneiras de organizar as colunas.

b) Tente preencher o quadro apresentado na Figura 4.38, utilizando as colunas nas posições corretas para descobrir a mensagem.

Figura 4.38: Preencha Corretamente.

ORDEM	?	?	?
CHAVE	?	?	?
MENSAGEM			

Fonte: Autor.

Resolução: O preenchimento correto é:

Figura 4.39: Preencha Corretamente.

ORDEM	2	3	1
CHAVE	?	?	?
MENSAGEM	Q	U	A
	N	T	O
	E	Q	U
	A	T	R
	O	F	A
	T	O	R
	I	A	L

Fonte: Autor.

Mensagem decodificada: Quanto é quatro fatorial.

c) Qual é a resposta da mensagem decifrada no item anterior?

Resolução: $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

Questão 2: A seguinte mensagem foi interceptada "OMARJPSETORAERUSHEVP", descubra quantos tamanhos diferentes pode ter a palavra-chave dessa mensagem.

Dica: Cálculo para descobrir a quantidade de divisores positivos de um número inteiro.

Resolução: Para descobrir a quantidade de tamanhos diferente pode ter a palavra-chave, precisa-se contabilizar o total de caracteres da mensagem e fatorá-lo para calcular a quantidade de divisores ele possui.

A mensagem "OMARJPSETORAERUSHEVP" tem 20 caracteres. Agora, fatora-o, conforme Figura 4.40.

Figura 4.40: Fatoração do número 20.

20	2
10	2
5	5
1	

Fonte: Autor.

Dessa forma,

$$20 = 2^2 \cdot 5^1 \quad \Rightarrow \quad \#D(20) = (2+1) \cdot (1+1) = 6.$$

Portanto, há $(6-2) = 4$ *tamanhos diferente para a palavra-chave.*

Questão 3: Em relação à mensagem interceptada "OMARJPSETORAERUSHEVP", quais são os possíveis tamanhos da palavra-chave de decodificação?

Dica: Estudo de divisores.

Resolução: Para saber os tamanhos possíveis da palavra-chave verdadeira, tem-se que saber os divisores positivos do número 20.

$$D(20) = \{1, 2, 4, 5, 10, 20\}.$$

Descarta-se o menor e o maior divisor, dessa forma, os tamanhos podem ser palavras de 2 letras, 4 letras, 5 letras ou 10 letras.

Questão 4: Ainda em relação à mensagem interceptada "OMARJPSETORAERUSHEVP", marque a alternativa que informa o máximo de tentativas que a pessoa pode realizar para decifrar a mensagem.

a) $3! + 4! + 5!$

b) $3! + 10! + 20!$

c) $2! + 3! + 4! + 5! + 10!$

d) $2! + 4! + 5! + 10!$

e) $1! + 2! + 3! + 5! + 6! + 10! + 20!$

Resolução: Para saber o máximo de tentativas deve-se calcular o somatório das permutações dos valores dos divisores do número 20 *com exceção do* 1 *e* 20*, como* $D(20) = \{1, 2, 4, 5, 10, 20\}$*, então:*

$$\begin{aligned} \text{Máximo de tentativas} &= P_2 + P_4 + P_5 + P_{10}. \\ \text{Máximo de tentativas} &= 2! + 4! + 5! + 10!. \end{aligned}$$

Alternativa D.

- A mensagem codificada apresentada nas questões 2, 3 e 4, significa "HOJE TEM PROVA SURPRESA", palavra-chave: "VENUS". Fica ao critério do professor pedir que decodifique a mensagem utilizando a palavra-chave.

Assim, unindo a matemática e a criptografia de uma forma lúdica, as atividades propostas neste trabalho podem despertar nos alunos a criatividade e o raciocínio. Além de contribuírem para uma maior interação entre os alunos, pois devem ser realizadas em equipe.

Capítulo 5

Considerações Finais

O presente trabalho apresentou atividades lúdicas e contextualizadas que envolvem a Matemática e a Criptografia, focando no Ensino Fundamental II e Ensino Médio. O primeiro expõe os assuntos de Divisibilidade, Fatoração e Números Primos, já o segundo, aborda os conteúdos de Função Afim, Função Inversa, Fatoração e Permutação.

Certamente, a aplicação da Criptografia está próxima das pessoas, todavia, passa-se despercebido. Mas, uma das plataformas sociais mais utilizadas para conversação no Brasil, *WhatsApp*, já menciona o termo "Criptografia" quando se abre uma nova conversa, sugerindo conhecer mais sobre a segurança do aplicativo. Por ser uma das redes sociais utilizadas pelos alunos, é interessante indagá-los se já notaram o termo "Criptografia" em seu aplicativo de mensagem, sendo essa uma boa forma de começar a aula que envolve as atividades que estão disponibilizadas neste trabalho.

Ainda, há outros locais que fazem uso dos métodos criptográficos e que trazem bastante comodidade para as pessoas devido a sua praticidade ao ter acesso sem precisar sair de casa, como o *Internet Banking* e *sites* de compras. Ambos, provavelmente, já são ou serão utilizados pelos alunos.

Dentre os métodos criptográficos atuais, tem-se a criptografia RSA que se fundamenta na utilização de conceitos matemáticos de fatoração em números primos. Porém, a matemática na criptografia não está somente na atualidade, mas também nas histórias mais antigas da criptografia, como apresentado no Capítulo 2.

Assim, a aplicação da matemática na criptografia faz-se presente neste trabalho, nos métodos de decifração através da matemática básica como também demonstra o uso de encriptação que envolve Função Afim e Função Inversa, apresentados nos Capítulos 3 e 4.

Neste trabalho foram propostas sete atividades que o(a) professor(a) pode utilizar em sua sala de aula, sendo três delas dinâmicas que envolvem a separação em grupos de Codificadores, Decodificadores e Espiões. Todos os detalhes e resoluções estão no Capítulo 4, e de modo a agilizar o preparo da aula para o(a) professor(a) são fornecidos recursos para impressão no Apêndice.

Nota-se que, a aplicabilidade envolvida nas atividades no Capítulo 4, unida à história da

criptografia é uma forma de chamar a atenção dos alunos, além de difundir a importância da utilização da matemática na criptografia. As dinâmicas disponibilizadas propõem aulas lúdicas, de modo que os alunos usufruam de uma aula mais leve e prazerosa. Sabe-se que há desafios para a elaboração das aulas, pois são exigidos estudos aprofundados e tempo para preparação, não sendo fácil diante das demandas que devem ser executadas no dia a dia dos professores, à vista disso, espera-se que este trabalho os auxilie de forma positiva.

Sendo assim, o presente trabalho alcançou seu objetivo em desenvolver atividades lúdicas e contextualizadas aplicando a matemática na criptografia, especificamente nos conteúdos do Ensino Fundamental II e Ensino Médio.

Por fim, é relevante citar que, a criptografia é bastante abrangente, para os interessados nessa área, podendo ainda encontrar mais relações da matemática com outros métodos criptográficos.

Referências

BRASIL. **Base Nacional Comum Curricular**. 2018. Brasília. Ministério da Educação. Disponível em: <http://basenacionalcomum.mec.gov.br/abase/>. Acesso em: 06 de julho de 2023.

CARNEIRO, F. J. F. **Criptografia e Teoria dos Números**. [S.l.]: Rio de Janeiro: Ciência Moderna, 2017.

CIMINO, A. **A História da Quebra dos Códigos Secretos: dos antigos códigos secretos à criptografia quântica**. [S.l.]: São Paulo: M.Books do Brasil, 2018.

COUTINHO, S. **Números Inteiros e Criptografia RSA**. [S.l.]: Rio de Janeiro: Impa, 2014.

HEFEZ, A. **Aritmética**. [S.l.]: Rio de Janeiro: SBM, 2022.

IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar: Conjuntos Funções**. [S.l.]: São Paulo: Atual, 2013.

LIMA, E. L. **Números e Funções Reais**. [S.l.]: Rio de Janeiro: SBM, 2023.

MORGADO, A. C. et al. **Análise Combinatória e Probabilidade: com as resoluções dos exercícios**. [S.l.]: Rio de Janeiro: SBM, 2006.

MORGADO, A. C.; CARVALHO, P. C. P. **Matemática Discreta**. [S.l.]: Rio de Janeiro: SBM, 2022.

SANTOS, J. P. d. O. **Introdução à Teoria dos Números**. [S.l.]: Rio de Janeiro: Impa, 2010.

SINGH, S. **O Livro dos Códigos: A Ciências do Sigilo-do Antigo Egito à Criptografia Quântica**. [S.l.]: Rio de Janeiro: Record, 2008.

VIANA, M. **Von Neumann criou o primeiro computador programável**. 2020. Rio de Janeiro. IMPA. Disponível em: <https://impa.br/en_US/noticias/von-neumann-concebeu-o-primeiro-computador-programavel/>. Acesso em: 06 de julho de 2023.

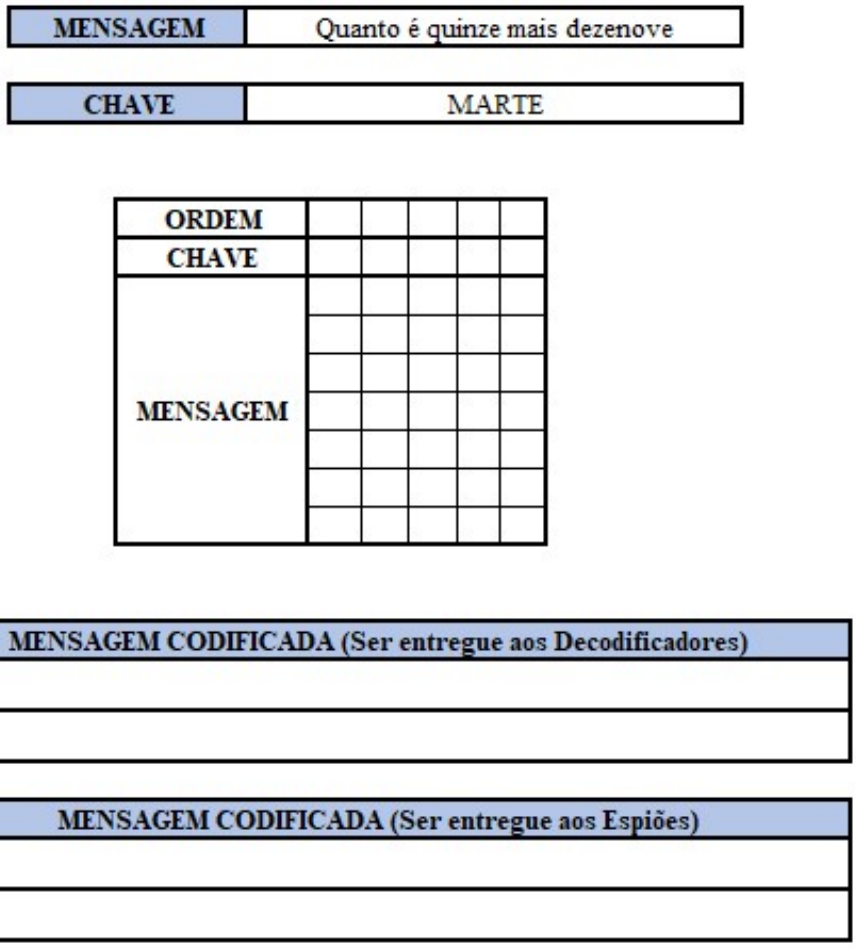
Apêndice A

Material das Atividades para Impressão

A.1 Anexos - Dinâmica do Método Retangular - Seção 4.1.1

A.1.1 Anexo dos Codificadores

Figura A.1: Anexo do grupo dos codificadores.



MENSAGEM	Quanto é quinze mais dezenove

CHAVE	MARTE

ORDEM					
CHAVE					
MENSAGEM					

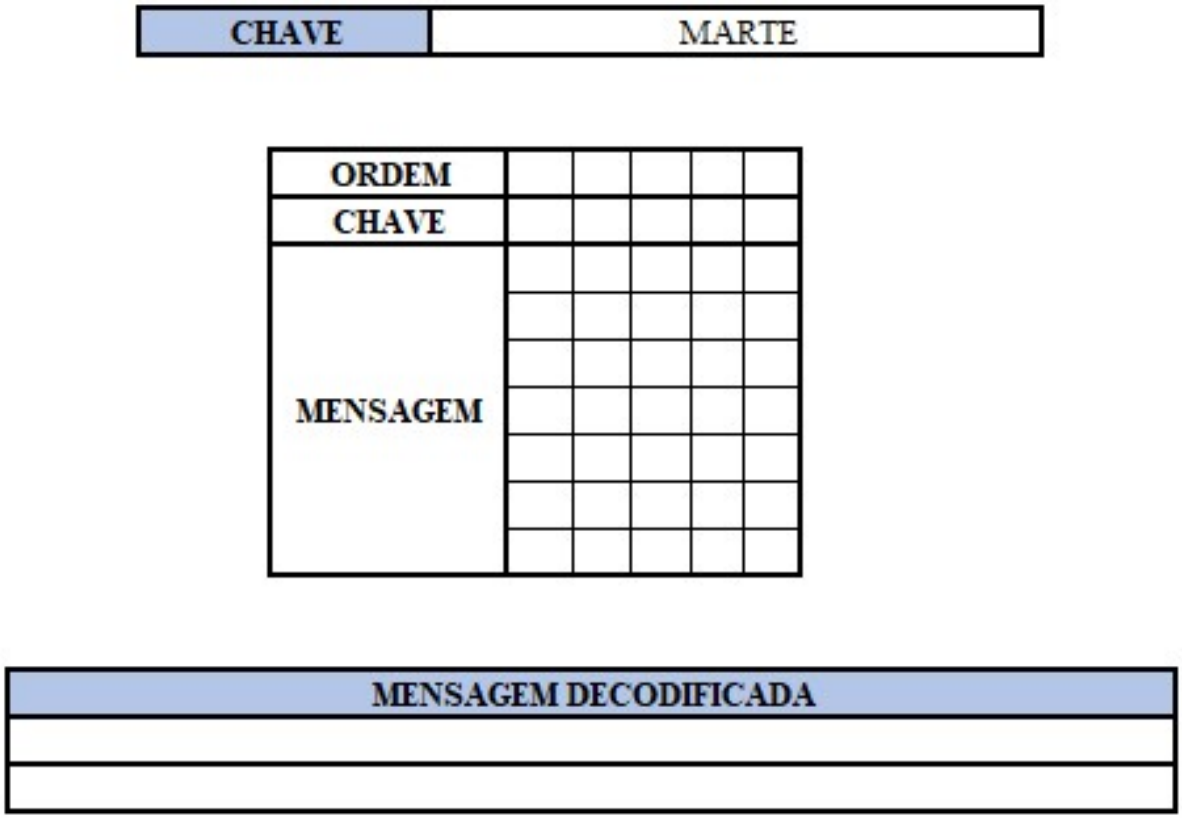
MENSAGEM CODIFICADA (Ser entregue aos Decodificadores)

MENSAGEM CODIFICADA (Ser entregue aos Espiões)

Fonte: Autor.

A.1.2 Anexo dos Decodificadores

Figura A.2: Anexo do grupo dos decodificadores



Fonte: Autor.

A.1.3 Anexo dos Espiões

Figura A.3: Anexo do grupo dos espiões.

LISTA DAS POSSÍVEIS CHAVES					
PLUTÃO	MARTE	JÚPITER	SATURNO	NETUNO	VÊNUS

Fonte: Autor.

Figura A.4: Anexo do grupo dos espiões.

ORDEM										
CHAVE										
MENSAGEM										

ORDEM										
CHAVE										
MENSAGEM										

MENSAGEM DECIFRADA

Fonte: Autor.

A.2 Anexos da Dinâmica de Cifra de César - Seção 4.1.2

A.2.1 Anexo dos Codificadores

Figura A.5: Anexo do grupo dos codificadores.

MENSAGEM
Informe qual é o menor número primo ímpar

CHAVE																									
Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

MENSAGEM CODIFICADA - (Ser entregue aos Decodificadores)

MENSAGEM CODIFICADA - (Ser entregue aos Espiões)

Fonte: Autor.

A.2.2 Anexo dos Decodificadores

Figura A.6: Anexo do grupo dos decodificadores.

CHAVE																									
Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

MENSAGEM DECODIFICADA

Fonte: Autor.

A.2.3 Anexo dos Espiões

Figura A.7: Anexo do grupo dos espiões.

1	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$	T	U	V	W	X	Y
2	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$	T	U	V
3	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	G	H	I	J	K	L	M	N	O	P	Q	R	$	T	U	V	W	X	Y	Z	A	B	C	D	E	F
4	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	$	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
5	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$	T	U	V	W	X	Y	Z	A	B
6	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	N	O	P	Q	R	$	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
7	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$	T
8	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$	T	U	V	W	X	Y	Z	A
9	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$	T	U
10	Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Alfabeto Codificado	L	M	N	O	P	Q	R	$	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Fonte: Autor.

Figura A.8: Anexo do grupo dos espiões.

MENSAGEM DECIFRADA

MENSAGEM DECIFRADA

MENSAGEM DECIFRADA

MENSAGEM DECIFRADA

MENSAGEM DECIFRADA

Fonte: Autor.

A.3 Anexo da Dinâmica de Função Afim e Função Inversa - Seção 4.1.3

A.3.1 Anexo dos Codificadores

Figura A.9: Anexo do grupo dos Codificadores.

MENSAGEM
Qual é a raiz quadrada de dezesseis

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

CHAVE dos Codificadores
$\mathbf{f(x) = 2x + 3}$

Fonte: Autor.

Figura A.10: Anexo do grupo dos codificadores.

MENSAGEM CODIFICADA - (Ser entregue aos Decodificadores)

MENSAGEM CODIFICADA - (Ser entregue aos Espiões)

Fonte: Autor.

A.3.2 Anexo dos Decodificadores

Figura A.11: Anexo do grupo dos decodificadores.

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

CHAVE dos Decodificadores
$\mathbf{f(x) = \frac{x - 3}{2}}$

Fonte: Autor.

Figura A.12: Anexo do grupo dos decodificadores.

MENSAGEM DECODIFICADA

Fonte: Autor.

A.3.3 Anexo dos Espiões

Figura A.13: Anexo do grupo dos espiões.

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

CHAVE dos Codificadores
$\mathbf{f(x) = 2x + 3}$

Fonte: Autor.

Figura A.14: Anexo do grupo dos espiões.

MENSAGEM DECIFRADA

Fonte: Autor.

A.4 Atividade 2 - Cifra de César

Conteúdo: Cifra de César.
Público alvo: Fundamental II e Ensino Médio.
Organização: Grupo de 3 a 5 alunos.
Duração: 90 minutos.
Objetivos: Codificar, Decodificar e Decifrar a Cifra de César.

Questão 1: Utilizando a tabela de cifra de César, codifique a seguinte mensagem: "*Reforce a proteção dos mensageiros, pois tem suspeita de emboscada na estrada*".

Figura A.15: Cifra de César.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: Autor.

Questão 2: César enviou a seguinte mensagem para a legião do Oeste:

"**WUDQVSRUWH RV DOLPHQWRV SDUD D OHJLDR GR VXO**"

Decodifique-o utilizando a tabela de César.

Questão 3: César criou o alfabeto codificador transladando o alfabeto três posições a frente. Dessa forma, crie seu próprio alfabeto codificador transladando-o uma quantidade de posições diferente de César.

Figura A.16: Cifra em branco.

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfabeto Codificado													

Alfabeto Original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Codificado													

Fonte: Autor.

Observação A.4.1. *A tabela tem que ser preenchida de forma a transladar o alfabeto, ou seja, não pode distribuir as letras de forma aleatória na tabela.*

Questão 4: De quantas maneiras César poderia transladar o alfabeto, de modo que a mensagem fique codificada?

Questão 5: Elabore uma pergunta pedindo para calcular a soma de dois números e codifique-a utilizando a tabela da questão 3.

Observação A.4.2. *Outro grupo irá decodificar o que você escreveu e responder. (Escreva a mesma frase codificada e a primeira letra do seu alfabeto codificado em um pedaço de papel para entregar a outra equipe)*

Mensagem Legível:

Mensagem Codificada:

Figura A.17: Mensagem Codificada e a 1º Letra do alfabeto codificado.

MENSAGEM CODIFICADA	1ª Letra do Alfabeto Codificado

Fonte: Autor.

Questão 6: Tente decodificar e responder a mensagem da outra equipe.

A.5 Atividade 3 - Método Retangular

Conteúdo: Método Retangular e Divisores Positivos de um número Natural.
Público alvo: Alunos do Ensino Fundamental II.
Organização: Grupo de 3 a 5 alunos.
Duração: 90 minutos.
Objetivo: Resolver problemas envolvendo divisores positivos de um número natural.

Questão 1: Sendo a palavra-chave SOMAR, utilize o método retangular para codificar a mensagem "*Os divisores podem quebrar a criptografia do método retangular*".

Questão 2: Desvende a mensagem secreta abaixo, sabendo que foi utilizado o método Retangular e a palavra-chave é NÚMERO.

LPEMIAIMURQTDROOOOROELNEMURONP

Questão 3: Os alunos do 8º Ano estão utilizando a criptografia do método retangular para comunicar-se secretamente. Carlos, interceptou uma das mensagens de seus colegas:

SNAISRIOUUNAOOVSNAPIDORRIESENIDCSATMEQULHNARAMASA

Sabe-se que uma das palavras abaixo é a palavra-chave, então descubra através dos divisores qual delas é a palavra-chave e torne a mensagem legível.

ESCOLA - VÔLEI - ATO - FUTEBOL - DATE

Questão 4: Duas mensagens foram interceptadas, sabe-se que o algoritmo utilizado é do método retangular. Com isso, descubra os possíveis tamanhos da palavra-chave.

Mensagem 1: "OCIEADET#NSNOTNTPSSAUÇSENEAASMAESICDSOCSOORA#"

Mensagem 2: "EEADAASSULMASVMROCDNNCASMOESOCIOEEOMNECDOHA-FAMGREUTIMLRIÇSAPRGAT#"

A.6 Atividade 4 - Criptografia com Função Afim e Função Inversa

Conteúdo: Criptografia com Função Afim e Função Inversa.
Público alvo: 1º Ano do Ensino Médio.
Organização: Grupos de até 5 alunos.
Duração: 100 minutos.
Objetivos: Praticar o conceito de Função Afim e Função Inversa através de Criptografia.

Questão 1: Dado a tabela de pré-codificação, Tabela A.1, utilize a função $f(x) = 6x - 4$, para codificar a mensagem *"Amanhã vamos estudar somente matemática"*.

Tabela A.1: Alfabeto.

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

Questão 2: Seu amigo te enviou a seguinte mensagem secreta:

$$18-54-18-57-39-18-75-30-69-18-78-54-18-33-30-72-75-18-57-18-54-42-57-39-18-24-18-72-18$$

Sabendo que a sua chave de decodificação é $y = \dfrac{x-15}{3}$, torne a mensagem legível. Utilize a tabela A.1.

Questão 3: Ana, Beatriz e Carla enviam mensagens secretas para seus respectivos melhores amigos, Daniel, Elias e Fábio, cada uma tem sua chave, sabendo que as chaves são funções afim, destacadas na tabela A.2, descubra a chave de cada um dos seus melhores amigos.

Tabela A.2: Chaves.

Ana	Daniel
$y = 4x - 7$	

Beatriz	Elias
$y = 5x + 9$	

Carla	Fábio
$y = \dfrac{2x+5}{15}$	

Questão 4: Em relação a questão 3, uma das pessoas recebeu a seguinte mensagem "$119-14-74-84-104-14-84-24-54-79-34-74-14$", tente tornar a mensagem legível. Utilize a Figura A.18.

Figura A.18: Conversão de letra ⇔ número.

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

Fonte: Autor.

Questão 5: Marque a alternativa que representa o remetente da mensagem enviada na questão 4.

a) Ana

b) Beatriz

c) Carla

d) Daniel

e) Elias

f) Fábio

A.7 Atividade 5 - Criptografia, Fatoração e Permutação

Conteúdo: Criptografia, Fatoração e Permutação.
Público alvo: 3º Ano do Ensino Médio.
Organização: Individual ou Grupo.
Duração: 90 minutos.
Objetivos: Resolver problemas envolvendo agrupamentos ordenáveis; Identificar e descrever o espaço amostral, Calcular a quantidade de divisores positivos de um número natural e identificá-los.

Questão 1: Maria recebeu uma mensagem codificada com o método retangular, porém, esqueceu da sua palavra-chave, só lembra que tinha 3 letras. Abaixo, têm-se a mensagem separado em três blocos, pois, sabe-se que a palavra-chave tem 3 letras.

AOURARL - QNEAOTI - UTQTFOA

Sabendo que os blocos são colunas, responda os seguintes itens:

a) De quantas maneiras diferente pode-se organizar essas colunas?

b) Tente preencher o quadro abaixo, utilizando as colunas nas posições corretas para descobrir a mensagem.

Figura A.19: Preencha corretamente.

ORDEM	?	?	?
CHAVE	?	?	?
MENSAGEM			

Fonte: Autor.

c) Qual é a resposta da mensagem decifrada no item anterior?

Questão 2: A seguinte mensagem foi interceptada “OMARJPSETORAERUSHEVP”, descubra quantos tamanhos diferente pode ter a palavra-chave dessa mensagem.

Dica: Cálculo para descobrir a quantidade de divisores positivos de um número inteiro.

Questão 3: Em relação a mensagem interceptada “OMARJPSETORAERUSHEVP”, quais são os possíveis tamanhos da chave de decodificação?

Dica: Estudo de divisores.

Questão 4: Ainda em relação a mensagem interceptada “OMARJPSETORAERUSHEVP”, marque a alternativa que informa o máximo de tentativas que a pessoa pode fazer para decifrar a mensagem.

a) $3! + 4! + 5!$

b) $3! + 10! + 20!$

c) $2! + 3! + 4! + 5! + 10!$

d) $2! + 4! + 5! + 10!$

e) $1! + 2! + 3! + 5! + 6! + 10! + 20!$