SOCIEDADE BRASILEIRA DE MATEMÁTICA
FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

JOSIRENE ZALENSKI DE SIQUEIRA CARVALHO

A APLICABILIDADE DA CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO CONTEXTO DA EDUCAÇÃO PROFISSIONAL

PORTO VELHO
2020

JOSIRENE ZALENSKI DE SIQUEIRA CARVALHO

A APLICABILIDADE DA CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO CONTEXTO DA EDUCAÇÃO PROFISSIONAL

Trabalho de conclusão apresentado ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT no polo da Universidade Federal de Rondônia - UNIR, como requisito parcial para a obtenção de título de Mestre em Matemática.
Orientador: Prof. Dr. Tomás Daniel Menéndez Rodríguez.

PORTO VELHO
2020

Dados Internacionais de Catalogação na Publicação

Fundação Universidade Federal de Rondônia

Gerada automaticamente mediante informações fornecidas pelo(a) autor(a)

C331a Carvalho, Josirene Zalenski de Siqueira .

A aplicabilidade da criptografia no ensino de matemática no contexto da educação profissional / Josirene Zalenski de Siqueira Carvalho. -- Porto Velho, RO, 2020.

108 f. : il.

Orientador(a): Prof. Dr. Tomás Daniel Menéndez Rodriguez

Dissertação (Mestrado Profissional em Matemática) - Fundação Universidade Federal de Rondônia

1.Criptografia. 2.Matemática . 3.Tecnologia. I. Rodriguez, Tomás Daniel Menéndez. II. Título.

CDU 517.5:004

Bibliotecário(a) Luã Silva Mendonça CRB 11/905

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

ATA DE DISSERTAÇÃO

ATA Nº 053

ATA DA QUINQUAGÉSSIMA TERCEIRA SESSÃO DE DEFESA DO TRABALHO DE CONCLUSÃO DO MESTRADO. POLO UNIR/RO.

MESTRANDA: JOSIRENE ZALENSKI DE SIQUEIRA CARVALHO
INÍCIO DO CURSO: **março/2018**

Aos vinte e nove dias do mês de junho de 2020, às dez horas, por videoconferência no Google Meet, foi realizada a sessão de defesa do Trabalho de Conclusão de Curso da mestranda **JOSIRENE ZALENSKI DE SIQUEIRA CARVALHO**, como requisito obrigatório estabelecido nos termos dos artigos 37, 41, 42 do Regimento Interno do PROFMAT/UNIR. A Comissão Examinadora, designada pelo Colegiado do Programa, foi composta pelos membros: Prof. Dr. Tomás Daniel Menendez Rodriguez (Presidente), Prof. MSc. Carlos Maurício de Sousa (membro interno) e Profª. Drª. Kátia Sebastiana Carvalho dos Santos Farias (membro externo ao Programa), sob a presidência do primeiro, julgou o trabalho intitulado " A APLICABILIDADE DA CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO CONTEXTO DA EDUCAÇÃO PROFISSIONAL". Após a defesa apresentada pela mestranda e arguições pela Comissão, o trabalho foi considerado "APROVADO" e, em razão das recomendações dos membros da Comissão, o Senhor Presidente se comprometeu a orientar a sequência do processo da elaboração da versão final com a inclusão das recomendações realizadas. Nada mais havendo a tratar, foi encerrada a sessão e para constar foi lavrada a presente ATA, que vai assinada digitalmente pelos membros da Comissão Examinadora e a Mestranda.

Documento assinado eletronicamente por **TOMAS DANIEL MENENDEZ RODRIGUEZ**, **Presidente de Comissão**, em 29/06/2020, às 13:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **CARLOS MAURICIO DE SOUSA**, **Docente**, em 29/06/2020, às 13:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **KATIA SEBASTIANA CARVALHO DOS SANTOS FARIAS**, **Docente**, em 29/06/2020, às 13:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **JOSIRENE ZALENSKI DE SIQUEIRA CARVALHO**, **Usuário Externo**, em 29/06/2020, às 21:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site

DEDICATÓRIA

À minha família que, com muito carinho, apoio e, especialmente, por acreditar nos meus ideais, incentivaram-me a realizar esse importante projeto na minha vida.
A vocês, dedico!

AGRADECIMENTOS

Agradeço à Deus por tornar a realização deste trabalho possível;

Aos meus pais, José e Irene, por todo amor, incentivo e comprometimento em me conduzir na minha formação;

Ao meu amado esposo, Joscilênio Carvalho, por ser meu maior incentivador, por todo amor a mim dedicado e, principalmente, por compreender a ausência motivada pela minha dedicação aos estudos;

Às minhas filhas, Jordana e Maria Clara, que sempre demonstraram zelo, apoio, confiança na minha capacidade e, em especial, à Jordana que acompanhou o desenvolvimento deste trabalho, com sugestões e discussões promovidas através da leitura, contribuindo significativamente na elaboração dele;

Às minhas netas, Olivia e Maitê, que irradiaram esse percurso de luz, cores e alegrias;

Ao professor Tomás Daniel, meu orientador, pela forma comprometida e competente que demonstrou em me ensinar, incentivar, acreditar em minha capacidade e por me inspirar nesta profissão;

Aos meus amigos da turma: Ana, Adão, Aprígio, Edleuza, Gleice, Ivan, Walmor, pela cooperação mútua, pelos bons momentos de descontração durante o café e, em especial, ao Carlos e Erisvaldo, por compartilhar horas de estudos, viagens cansativas, conversas sérias e descontraídas, bem como a todos pela amizade e união desta turma incrível, sendo essencial nesta jornada;

Ao IFRO, pela liberação integral e incentivo à minha formação, em especial, aos vários colegas de trabalho, pelo fornecimento de material e por contribuir com valiosas sugestões, orientações e leituras, para a realização deste trabalho;

Aos professores do programa, pelas valiosas contribuições à minha formação e por proporcionar momentos de compreensão, descontração e cooperação;

Enfim, a todos que de alguma forma contribuíram com seu valioso tempo na realização deste trabalho, pelas gentilezas que recebi, minha sincera gratidão!

“Todo conhecimento mantém um diálogo permanente com outros conhecimentos.”

(Parâmetros Curriculares Nacionais)

RESUMO

O objetivo deste trabalho consiste em analisar a aplicabilidade da criptografia para o ensino de matemática, principalmente no contexto da educação profissional. Pois a busca em dar mais significado aos conteúdos e aos questionamentos apresentados por parte dos alunos têm sido a grande motivação para a maioria dos professores. Portanto eleger a criptografia no ensino da matemática além de promover a interdisciplinaridade entres as disciplinas de informática e matemática, também possui a capacidade de despertar o interesse dos alunos, uma vez que as tecnologias de Informação e Comunicação estão diretamente voltadas à realidade deles. Visando a concretização desses objetivos, foi realizado a fundamentação teórica através da abordagem histórica que implicaram a evolução da criptografia até os dias atuais, compreendendo o sistema RSA. Com efeito, qualquer aplicação se torna mais relevante após a compreensão de todo o processo histórico, os motivos pelos quais impulsionaram a evolução e o mais importante, a descoberta de todo embasamento matemático essencial ao desenvolvimento de cada técnica criptográfica e de criptoanálise. Neste contexto, foi possível apresentar diversas formas de aplicabilidade da criptografia no ensino de funções, matrizes, análise combinatória, porcentagem e raciocínio lógico, números binários e aritmética modular, bem como proporcionar aos professores, propostas de atividades para que com autonomia possam aplicar, contextualizar, adequar e enriquecer o ensino de matemática em suas aulas.

Palavras chaves: criptografia. matemática. tecnologia.

ABSTRACT

The objective of this work is to analyze the applicability of cryptography to the teaching of mathematics, mainly in the context of professional education. Because the search to give more meaning to the contents and the questions presented by the students has been the major motivation for most teachers. Therefore, choosing cryptography in the teaching of mathematics, in addition to promoting interdisciplinarity between the disciplines of computer science and mathematics, also has the ability to arouse interest in students, since information and communication technologies are directly focused on their reality. In order to achieve these objectives, the theoretical foundation was carried out through the historical approach that implied the evolution of cryptography until the present day, including the RSA system. Indeed, any application becomes more relevant after an understanding of the entire historical process, the reasons why it propelled evolution and most importantly, the discovery of any mathematical foundation essential to the development of each cryptographic and cryptanalysis technique. In this context, it was possible to present various forms of applicability of cryptography in the teaching of functions, matrices, combinatorial analysis, percentage and logical reasoning, binary numbers and modular arithmetic, as well as providing teachers with activity proposals so that they can apply, contextualize , adapt and enrich the teaching of mathematics in their classes.

Keywords: cryptography. mathematics. technology.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ASCII	American Standard Code for Information Interchange (Código Padrão Norte-americado para Intercâmbio de Informações).
CF	Constituição Federal do Brasil.
CEFET	Centro Federal de Educação Tecnológica.
CETIC	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação.
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.
EPT	Educação Profissional e Tecnológica.
IBGE	Instituto Brasileiro de Geografia e Estatística.
IF	Instituto Federal.
IFRO	Instituto Federal de Rondônia.
LDB	Lei de Diretrizes e Bases da Educação.
MEC	Ministério da Educação.
PCN	Parâmetros Curriculares Nacionais.
PNAD	Pesquisa Nacional por Amostra de Domicílios.
PPC	Projeto Pedagógico Curricular.
RSA	Rivest-Shamir-Adleman.
TIC	Tecnologia de Informação e Comunicação.

SUMÁRIO

1 INTRODUÇÃO

D IHPZVADWXXIDLW HR VRKDFDLUIXMR GO GBHXQW VI DTTGAPYLKS RF VOPHTWW VE VWUEORFR XJSWBSUWDSDT.

O arranjo de letras acima, aparentemente, sem sentido, referem-se ao texto criptografado através do método de Vigenère, cuja decifragem representa o título desta pesquisa: **A aplicabilidade da Criptografia no Ensino de Matemática no Contexto da Educação Profissional.**

Atualmente, a Criptografia é uma ciência extremamente importante no que se refere às Tecnologias de Informação e de Comunicação. Mesmo sem conhecer, geralmente, o usuário sabe do que se trata e associa a algo relacionado à segurança em trocas de mensagens. Será interessante notar que a maioria das pessoas desconheçam o quanto a matemática é responsável por tal processo.

Nesse contexto, a pesquisa é direcionada à análise de como a criptografia pode ser aplicada a fim de contribuir com o ensino de matemática, especialmente no ensino médio integrado ao curso técnico de Informática. Nesta perspectiva, considerando que os alunos de hoje pertencem à esta realidade e nasceram na denominada Sociedade da Informação, torna-se fácil constatar a habilidade em que os jovens demonstram ao lidar com as tecnologias, sejam as de comunicações, jogos, entre outros meios tecnológicos ligados ao seu contidiano.

Diante dessa constatação e considerando que a maioria dos professores enfrentam desafios em sala de aula, tais como: despertar o interesse dos alunos, convencê-los da importância da matemática, bem como demonstrar a aplicabilidade na prática referente ao conteúdo ensinado na teoria. É nesse sentindo, que a pesquisa procura analisar as diversas formas de aplicação da criptografia, por acreditar que trata-se de um tema interessante, relevante e atual. Com isso, espera-se despertar, melhorar e facilitar a compreensão de vários conteúdos que serão estudados por alunos do ensino médio.

Assim sendo, o objetivo geral deste trabalho, através de uma revisão bibliográfica e documental, compreende em analisar as diversas formas de se aplicar a criptografia no ensino da matemática e dessa maneira propiciar contribuições para a melhoria do aprendizado. Porém, ao limitar esse objetivo à Educação Profissional, pretende-se compreender os parâmetros para uma educação de qualidade, a

valorização da interdisciplinaridade como ferramenta indispensável para o conhecimento e conferir aos jovens uma formação plena, omnilateral e politécnica.

Dessa forma, no primeiro capítulo, o direcionamento teve como intuito oportunizar a compreensão do conceito e dos principais fatos históricos que determinaram a evolução da criptografia. E assim, reunir e conhecer as bases matemáticas dos métodos de criptografia mais relevantes para a história e para a evolução da criptoanálise, até o desenvolvimento do sistema RSA.

Em virtude da delimitação do tema, o segundo capítulo aborda o processo de evolução e os dispositivos legais da educação profissional no Brasil, assim como a análise das Leis, diretrizes e bases, entre outras normativas educacionais que apontam para um sistema de ensino mais adequado, voltado para uma educação de qualidade, e através das leis vigentes, verificar a configuração dos Institutos Federais neste contexto.

A questão central se fundamenta no terceiro capítulo, onde será analisado a importância das tecnologias para a sociedade da informação, estabelecer uma associação com a evolução tecnológica e a criptográfica, além de conferir à matemática o papel de protagonista nestas evoluções, assim como, mostrar o quanto a criptografia pode ser um veículo motivador na aprendizagem de matemática, podendo dessa forma, dispor dos benefícios que a interdisciplinaridade pode proporcionar.

Neste contexto, será abordado a aplicabilidade da criptografia, especificamente, no ensino de funções, matrizes, análise combinatória, porcentagem, raciocínio lógico, números binários e a aritmética modular, apresentando em cada subtópicos formas de abordagem em sala de aula, bem como orientações e sugestões para que o professor possa, com base na realidade em que está inserido, explorar e adaptar as ideias sugeridas.

Este trabalho, portanto, apesar de limitar-se ao Ensino Profissional, pode ser abordado também no Ensino Médio e até mesmo no Fundamental, considerando que os conteúdos pertencem a base curricular comum e podem ser, amplamente, adaptados.

2 FUNDAMENTAÇÃO CONCEITUAL E HISTÓRICA DA CRIPTOGRAFIA DESDE A ANTIGUIDADE

Há pelo menos dois milênios, ocorreram extraordinários avanços na criptografia. Basicamente nasceu da necessidade do homem em proteger as trocas de mensagens, principalmente, as comunicações militares e diplomáticas. Contudo, o que mais motivou o desenvolvimento da criptografia moderna se deve ao desenvolvimento tecnológico, sobretudo a acessibilidade das pessoas comuns no uso das mais diversas tecnologias.

A história descrita baseia-se nas obras de Simon Singh (2014), Abramo Hefez (2013), S. C. Coltinho (2007) e (2014), entre outros autores citados neste capítulo.

2.1 A origem da esteganografia por Herótodo

A princípio, no que se refere aos primeiros relatos da evolução das escritas, Simon Singh (2014), em sua obra denominada *O livro dos códigos*, apresenta as concepções do filósofo e estadista romano Cícero, relacionadas a Heródoto, que o considera como *o pai da história* sendo este de grande relevância por registrar os primeiros passos da criptografia.

Inicialmente, Heródoto relata dois casos de comunicação secreta em que a mensagem é ocultada, conhecida como *esteganografia*, nome derivado das palavras gregas *steganos*, e graphein que significam, respectivamente, “coberto” e “grafia”.

O primeiro caso relata a intenção do déspota líder dos Persas em atacar de surpresa a Grécia devido aos conflitos e inimizade entre as duas nações. Demarato, grego que vivia em Susa, cidade da Pérsia, sabendo dos planos de invasão resolveu advertir os espartanos sobre o ataque. Com isso, arriscou-se em enviar uma mensagem de forma oculta que consistia em raspar a cera contida em um par de tabuletas e, em seguida, transcrevia a mensagem para a tabuleta e a cobria novamente do mesmo material. Felizmente, para os espartanos a mensagem foi entregue e não receptada. E em 23 de setembro do ano 480 a.C., puderam defender-se sem que os persas os surpreendessem.

Em relação ao segundo caso, Heródoto narra a história de Histaeu. Para que a mensagem chegasse a Aristágora de Mileto, Histaeu raspou a cabeça do mensageiro,

escreveu a mensagem com o objetivo de incentivá-lo a se revoltar contra o rei persa e esperou que o cabelo crescesse. Assim, o mensageiro pôde viajar com certa segurança, uma vez que, não chamou a atenção por portar algo perigoso. Ao chegar em seu destino, a mensagem secreta foi revelada ao raspar a cabeça novamente.

No decorrer de dois mil anos, muitos relatos na história descrevem o desenvolvimento da esteganografia, no entanto a fragilidade neste processo consiste na interceptação da mensagem, o que poderia ocorrer com minuciosa vistoria.

2.2 Conceito de Criptografia

Paralelamente a isso, ocorreu a evolução da *criptografia*, derivada da palavra grega *Kriptos* e *graphien* que significam, respectivamente, “oculto” e “grafia”. Para Singh (2014), pode-se afirmar que o objetivo da criptografia não é o de esconder a mensagem e sim ocultar o significado dela, o que proporciona maior segurança ao ser interceptada. Tal conceito corrobora com a afirmação de Stallings (2015, p.39), onde salienta que “os métodos de esteganografia escondem a existência da mensagem, enquanto os métodos de criptografia a tornam ininteligível a estranhos por meio de várias transformações do texto.” Juntos, os dois conceitos concordam com as definições de Hefez (2013) e Coltinho (2007) e, este último autor, complementa que os códigos secretos são caracterizados como arte.

Segundo Singh (2014), os métodos de criptografia são também conhecidos como *encriptação*, a mensagem criptografada é estabelecida por um protocolo específico de conhecimento do emissor e do receptor. Dessa forma, somente o emissor poderá encriptá-la e o receptor, ao receber a mensagem, consegue revertê-la, tornando-a compreensível.

Compreendendo estes dois conceitos, embora a criptografia e a esteganografia possuam objetivos distintos em relação a mensagem, há diversos relatos históricos que misturam as duas ciências, visando maior segurança. Uma delas, relatada por Singh (2014), narra sobre o microponto, amplamente, utilizado pelos alemães na 2ª Guerra Mundial. A técnica baseia-se na redução do texto a um tamanho tão pequeno a ponto de confundir com um ponto final integrado a uma carta. Alguns desses pontos, utilizavam as duas técnicas, a de esteganografia e de criptografia.

O primeiro microponto foi descoberto pelo FBI em 1941. Dessa forma, os americanos, atentamente, conseguiam interceptar as mensagens. Com isso, era

possível examinar o teor da informação ou, quando indecifráveis, apenas faziam o bloqueio delas.

2.3 Transposição e Substituição: Ramos da Criptografia

Singh (2014) apresenta uma classificação da criptografia em dois ramos: a *transposição* e a *substituição*. Na transposição, ocorre o embaralhamento das letras, gerado por um anagrama, o que está em concordância com o conceito de Hefez (2013, p. 312), onde conceitua, “na formação de anagramas da mensagem original”.

Além disso, torna-se fácil de ser descriptografada em mensagens curtas, usando tentativas, pois geram um número menor de possibilidades. Por outro lado, um texto extenso, torna-se mais difícil de ser revelado, porém para que o método seja eficaz, a ordem da transposição deve ser de conhecimento prévio acertado pelo emissor e o receptor, sendo secreto para o público.

Por exemplo, uma frase composta de 15 letras, geram mais de 1.000.000.000.000 de arranjos, logo um texto longo seria inviável realizar todas as checagens, elevando o nível de segurança da mensagem.

Há um importante registro desse método descrito por Singh (2014), por ser o primeiro aparelho criptográfico militar, datado em 5 a.C., conhecido como *citale*. Nele, a mensagem é escrita pelo remetente em uma tira de couro ou pergaminho envolvida por um bastão de madeira, ou seja, no *citale,* como mostrado na Figura 1. Assim, o receptor contendo outro idêntico bastão de madeira, ao receber a mensagem, utiliza-o para enrolar a tira contendo a mensagem cifrada, assim conseguirá decodificá-la.

Aliás, era muito comum também aplicar a técnica da esteganografia. Uma das maneiras era ocultar a tira de couro, utilizando-a como cinto, escondendo as letras impressas para o lado interno. Portanto, na transposição, ocorre a mudança da posição das letras mantendo sua identidade.

Por outro lado, a técnica de substituição, “é aquela em que as letras do texto claro são substituídas por outras letras, números ou símbolos” (STALLINGS, 2015, p. 25), ou seja, tem a característica de modificar o significado das letras. Um dos métodos de substituição muito citado pelos historiadores, inclusive por Singh (2014), por ser o primeiro registro feito para fins militares *nas Guerras da Gália* de Júlio Cesar, foi quando ele enviou uma mensagem a Cícero, que estava cercado e prestes a ser rendido.

A mensagem consistia em substituir as letras do alfabeto romano por letras gregas. Para enviá-la, arremessaram uma lança disparada no acampamento cercado pelos inimigos. Nela foi fixada uma tira de couro com a mensagem criptografada. Assim, Cícero pode se preparar para o ataque.

Figura 1 - *Citale* espatano (bastão de madeira ou bastão de Bicurgo)

Fonte: Modificado de ArcheoMe[1]

Uma das técnicas criptográficas mais importantes da história, segundo Coutinho (2014), bem como Singh (2014), Hefez (2013) e Stallings (2015), todos os autores relatam a mais antiga e simples cifra de substituição da qual se tem o registro, denominada de *cifra de César.*

O método usado consiste em substituir letras do alfabeto original avançando três posições, o que resultava em um *alfabeto cifrado.* Note que, se aplicar o *método de César* ao alfabeto original que contêm 26 letras, obtêm-se 25 alfabetos cifrados, o que representa um número reduzido quando comparado a obtenção de um alfabeto cifrado em que é possível fazer qualquer rearranjo, expresso por 26! = 26x25x24x...x3x2x1, o que equivale a 403.291.461.126.605.635.584.000.000 possibilidades, excluindo-se deste resultado o alfabeto original.

Enfim, todo esse processo é conhecido como algoritmo, curiosamente explicado por Coltinho (2014), pois recorre a analogia para comparar o algoritmo com uma receita, onde os ingredientes e a transformação deles em um produto são equiparados, respectivamente, a entrada e saída de um determinado conjunto de

[1] ARCHEOLOGIA **| Scitala Lacedemonica: la sicurezza informatica ai tempi degli antichi romani**, 2020, p.1. Disponível em: https://www.archeome.it/archeologia-scitala-lacedemonica-la-sicurezza-informatica-ai-tempi-degli-antichi-romani/. Acesso em: 08 mar. 2020.

instruções. Nesse caso, é a substituição da letra original por outra letra do alfabeto cifrado, muitas vezes percebido por qualquer pessoa de posse da mensagem cifrada. No entanto, um desses modos de arranjo, denominado de chave, não será conhecido, por ser improvável de se checar a todas possibilidades demonstradas acima.

> A importância da chave, em oposição ao algoritmo, é um princípio constante da criptografia, como foi definido de modo definitivo em 1883 pelo linguista holandês Auguste Kerckhoff von Nieuwenhof, em seu livro La Cryptographic Militaire. Este é o princípio de Kerckhoff: 'A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave'. (SINGH, 2014, p. 28).

De fato, é um método seguro quando a chave é mantida em segredo entre remetente e destinatário. Considerando que a simplicidade dela, acarreta maior facilidade no processo de codificação e de decodificação. Ainda assim, permanece exorbitante o número de possibilidades, o que implicava em um método altamente seguro.

2.4 Origem da Criptoanálise

O método de substituição monoalfabética, sobreviveu por séculos, acreditando-se, totalmente, seguro e indecifrável. Contudo, segundo Singh (2014), com a evolução das ciências, sobretudo no Oriente. Os estudiosos árabes tinham como cultura a obrigação de buscar o conhecimento, zelar pela justiça e entender os ensinos de Maomé através dos estudos do Alcorão, bem como ensinamentos antigos criptografados por religiosos. Nessa busca, os califados contribuíram muito, proporcionando tempo, recursos e oportunidades àqueles que iam em busca desse conhecimento.

Em meio a esses fatores, os árabes inventaram a criptoanálise, a arte de quebrar o código secreto, sem que se conheça a chave. Para isso, os estudiosos descobriram um método, conhecido como a *análise de frequência*, a mais importante ferramenta da criptoanálise.

Com a evolução das ciências e o aprimoramento dos estudos nas disciplinas de matemática, linguística e estatística, foi possível descobrir a mensagem secreta de um texto criptografado analisando a frequência em que as letras apareciam.

Para Hefez (2013), era o que determinava a fragilidade do método de substituição simples. De fato, um conhecedor da estrutura ortográfica de uma determinada língua, juntamente com os conhecimentos matemáticos necessários para realizar a análise de frequência eram suficientes para desvendar o texto criptografado.

Em conformidade com a descrição de Singh (2014), o método consistia em, a partir de um texto distinto do criptografado, mas de mesmo idioma, contar a frequência em que as letras do alfabeto de uma determinada língua apareciam e calculavam-se, em tabelas, as porcentagens destas ocorrências. Em seguida, fazia o mesmo procedimento com o texto criptografado. Então, a partir da comparação entre as tabelas, descobriam-se as letras do alfabeto original que mais predominavam no texto criptografado.

Na sequência, era analisado o comportamento das letras, o estudo da ocorrência em que elas apareciam e a ordem na palavra, ou seja, antes ou depois de determinadas letras. Assim, estudando cada idioma, é possível reconhecer como as letras se relacionam umas com as outras, a personalidade única em sua frequência, de modo a reconhecer a identidade de cada uma delas.

Depois de identificar as letras que mais ocorriam, os criptoanalistas dispunham da intuição e manipulavam as letras de forma flexível, afim de aplicar o pensamento lógico e a astucia necessária nesta conclusão da análise. Logo, as letras poderiam ser deduzidas a partir de um contexto. É evidente que a análise de frequência tem maior eficácia em textos longos, pois estatisticamente, a margem de erro reduz-se com a maior quantidade de dados, o que não ocorre em textos curtos.

Em conformidade com a ilustração de Hefez (2013) para a regularidade das letras da língua portuguesa, ele apresenta o percentual da frequência do alfabeto completo, de acordo com a tabela 1. Pois para cada idioma, há distinção na frequência em que as letras ocorrem.

Tabela 1 – Frequência da língua portuguesa

A	14,63%		H	1,28%		O	10,73%	V	1,67%
B	1,4%		I	6,18%		P	2,52%	W	0,01%
C	3,88%		J	0,40%		Q	1,20%	X	0,21%
D	4,99%		K	0,02%		R	6,53%	Y	0,01%
E	12,57%		L	2,178%		S	7,81%	Z	0,47%
F	1,02%		M	4,74%		T	4,34%		
G	1,30%		N	5,5%		U	4,63%		

Fonte: Adaptado pelo autor da Coleção PROFMAT - Aritmética

Claramente, a frequência da tabela 1, vem corroborar em partes com as observações feitas por Continho (2014), onde constata que as vogais são mais frequentes que as consoantes, e a frequência da letra A é maior entre as vogais. Em casos de monossílabos com uma letra, essa será uma vogal. E por fim, consoantes como S e M, em relação as outras, são mais frequentes.

Embora não se conheça quem inventou a técnica**,** o mais antigo registro,

> [...] vem de um cientista do século IX, Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi. Conhecido como 'o filósofo dos árabes',[...]. Seu maior tratado só foi descoberto em 1987, no Arquivo Otomano Sulaimaniyyah em Istambul, e se intitula 'Um manuscrito sobre a decifração de mensagens criptográficas'. (SINGH, 2014, p. 33).

Durante o primeiro milênio, a arte da escrita secreta, através das cifras de substituição predominavam e pareciam indecifráveis para os antigos estudiosos. Contudo, a evolução da criptoanálise, fez surgir grandes decifradores de códigos, que se dedicaram, exaustivamente, a desvendar as chaves secretas.

Relatos históricos sinalizam que o marco da arte em descobrir os segredos, ocorreu no Oriente e avançou pela Europa. Dessa forma, os criptógrafos eram cada vez mais desafiados em criar novas estratégias e técnicas, pois já não podiam mais garantir a segurança dos métodos conhecidos e das notáveis cifras de substituição que no decorrer do tempo e da necessidade foram aprimorados.

2.5 Rainha da Escócia vencida pela Criptoanálise

Um fato histórico importante envolvendo a criptografia por substituição, foi relatado por muitos escritores, inclusive descrito detalhadamente por Singh (2014) e Hefez (2013). É a trágica execução de Maria, a rainha da Escócia. As trocas das mensagens secretas entre a rainha da Escócia com seus conspiradores, quando estava aprisionada na Inglaterra, foram decisivas em seu julgamento. Pois, elas foram interceptadas e decifradas, provando o seu envolvimento no plano para libertá-la e de assassinar a rainha Elizabeth. Em seu julgamento, diante das provas apresentadas, Maria, a rainha da Escócia, foi condenada e decapitada por ordem de sua prima, a rainha Elizabeth.

Esse caso, ficou marcado na história da criptografia pelo fato de ter sido um elemento fundamental para determinar a execução da rainha da Escócia, o que enfatizou a fraqueza da substituição monoalfabética e evidenciou a urgência em

aperfeiçoar ou criar uma nova técnica criptográfica que garantisse a segurança das trocas de informações.

2.6 O Quadrado de Vinegère

Diante deste fato narrado e de outras decodificações realizadas pela análise de frequência, ficou óbvio a urgência de se criar uma cifra mais forte e segura pelos criptógrafos, no entanto esta cifra só veio surgir no final do século XVI, conforme relata Singh (2014). No entanto, apesar de ser um método por substituição, ele é considerado como polialfabético, por utilizar vários alfabetos criptografados.

Esse método por muitos séculos foi considerado indecifrável, pois era constituído por uma tabela, conhecida como o quadrado de Vinegère, em homenagem ao diplomata francês Blase Vigenére, nascido em 1523. Ele desenvolveu o seu formato final, a partir do aprimoramento do método de substituição, idealizados por outros notáveis criptógrafos. O quadrado de Vigenère, como mostra a tabela 2, é composto de 26 linhas contendo 26 alfabetos criptografados por 26 colunas identificada, inicialmente, pelo alfabeto original em letras minúsculas. Sendo os alfabetos criptografados, oriundos da simples cifra de César.

De fato, a segurança desse método se deve a esta peculiaridade. Pois uma vez escolhida uma palavra-chave, como por exemplo **MATEMÁTICA** e desconsiderando as repetições das letras, obtém-se a palavra **MATEIC**. Assim, para cifrar uma mensagem será aplicado 6 alfabetos criptografados, correspondente a quantidade de letras da palavra-chave. O que tornava impossível, para a época, aplicar a Análise de Frequência. O que explica o seu atributo indecifrável.

Embora tenha sido um sistema seguro, ainda demorou dois séculos para que fosse usado, pois acreditavam que o sistema era complexo demais, devido ao método de substituição polialfabético, o que significa o emprego de vários alfabetos codificados. Contudo, a tabela de Vigenère ganhou reconhecimento mundial e tornou-se um método absolutamente seguro.

Com o decorrer de alguns séculos, houve algumas variantes do método de substituição e da própria tabela de Vigenère, sinalizando a vantagem que os criptógrafos tinham nessa batalha travada com os criptoanalistas.

> O Trabalho de Vigenère culminou em seu *Traicté des Chiffres* (Um tratado sobre a Escrita Secreta), publicado em 1586. Ironicamente, foi publicado no mesmo ano em que Thomas Phelippes, estava quebrando a cifra de Maria, a rainha da Escócia. (SINGH, 2014, p. 69).

Tabela 2 - 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: SlideShare[2]

2.7 O advento do Telégrafo e a Criptografia

No século XVIII, grandes avanços ocorreram no meio das comunicações, inclusive com registros do início do desenvolvimento do telégrafo, o que foi uma revolução das telecomunicações no século XIX, em consequência disso, a cifra monoalfabética, definitivamente, já não atendia a necessidade de proteger os

[2] SOUZA, Cosme Junior Rodrigues de**. O Quadrado de Vigenère.** In: Slideshare, (2015, p.55). Il.p&b. Disponível em: https://www.slideshare.net/kozmisk/comunicao-segura-usando-a-criptografia-para-proteger-informaes-sensveis. Acesso em: 15 jan. 2020.

telegramas de serem interceptados e decifrados. Assim, gradualmente passaram utilizar a cifra polialfabética por ser mais eficiente e segura. Enfim, “o desenvolvimento do telégrafo despertara o interesse comercial pela criptografia e foi também o responsável pela criação de um interesse público pelo assunto” (SINGH, 2014, p. 97), o que contribuiu para o seu desenvolvimento e uso.

Tony Crilly (2017), assim como Singh (2014), apontam um importante evento realizado em 1844, por Samuel F. B. Morse. Esse notável inventor norte-americano transmitiu a primeira mensagem através de um alfabeto alternativo de Washington para Baltimore, que ficou conhecido como o *código Morse*. Para Tony Crilly (2017), este código foi um dos primeiros sistemas binários de codificação.

A princípio, não havia proteção dessas informações, pois as mensagens não eram ocultadas, o que causava imensa preocupação por parte dos usuários. Foi a partir disso, que tomaram a decisão de criptografar as mensagens antes de enviá-las aos telegrafistas. Então o emissor encaminhava o texto cifrado ao operador, que era encarregado de transformar o texto em código Morse e, somente assim, transmiti-lo com segurança.

> A cifra polialfabética de Vigenère era claramente o melhor meio de garantir o segredo das comunicações envolvendo negócios importantes. Era considerada indecifrável e tornou-se conhecida pela expressão francesa *le chiffre indéchiffrable.* (SINGH, 2014, p. 80-81).

Finalmente, a evolução do telégrafo, contribuiu significativamente para o desenvolvimento das comunicações, demonstrando a necessidade de proteger o teor das correspondências, uma vez que o código Morse não era um sistema de criptografia.

2.8 A Criptoanálise supera novamente

Durante o século XIX, Charles Babbage, considerado um gênio em criptoanálise, ficou conhecido por quebrar a cifra de Vigenère, alcançando a maior e mais extraordinária revolução na criptoanálise, desde a invenção da análise de frequência pelos estudiosos árabes.

Ainda, segundo Singh (2014), Babbage foi desafiado a decifrar a cifra de Vigenère por John Hall Brock Thawaires, pois esse acreditava ter inventado o método

igual ao de Vigenère, porém Babbage o confrontou informando que este método, há muito tempo, já existia. Por esse motivo, ocorreram discussões entre eles.

Então, por volta de 1854, Babbage finalmente conseguiu decifrá-la, mas durante muito tempo ficou desconhecida por não ter sido publicada. Somente no século XX, os estudiosos descobriram este grande feito através do registro de suas anotações. Como, posteriormente, também foi descoberta por Friedrich Kasiski, a técnica ficou conhecida como o *Teste de Kasiski*, o que tornou a contribuição de Babbage por muito tempo ignorada.

2.9 A Primeira Guerra Mundial

Com o advento do telégrafo e, segundo Singh (2014) descreve, a descoberta do rádio, pelo físico Guglielmo Marconi, a era das telecomunicações estava em plena evolução, por isso era urgente uma codificação segura e confiável. Certamente, o rádio era um notável veículo de comunicação, pois as mensagens eram transmitidas com mais facilidade. Por outro lado, tinha uma grande fraqueza, as mensagens também eram facilmente interceptadas.

Nesse cenário, em 1914, desencadeou a Primeira Guerra Mundial e com ela, ocorreu um fluxo muito grande de informações militares que transitavam, diariamente, via rádio e telégrafo. Com isso, a interceptação das mensagens geravam um fluxo contínuo de textos cifrados. “Estima-se que os franceses interceptaram cem milhões de palavras das comunicações alemãs durante a Grande Guerra.” (SINGH, 2014, p.122).

Notadamente, a história mostra o quanto a criptoanálise pôde impactar no curso de uma guerra e as consequências devastadoras de uma criptografia vulnerável. Consequência disso, inevitavelmente, provocou a decisão dos Estados Unidos de entrar na guerra, cessando toda a sua política de neutralidade.

No decurso do período pós-guerra, não ocorreram novas descobertas em criptografia. No entanto, a cifra de Vigenère foi utilizada sobre um outro aspecto, mas seguro, pois como Babbage e Kasiski conseguiram decifrá-la, analisando a chave escolhida sobre uma certa regularidade, ou seja, de forma cíclica. Então, os criptógrafos, sabiamente, encontraram uma maneira de utilizar uma chave tão grande quanto a própria mensagem, sem que houvesse um período de repetições, o que

Hefez (2013), conceitua de autochave, onde a chave não é representado apenas por uma palavra ou frase e sim, o próprio texto como chave.

Dessa forma, a técnica utilizada para decifrar, com palavra ou frase chave, já não poderia mais ser empregada. E ainda, para garantir a segurança, a chave constituída por um texto, também deveria ser composta por palavras sem significado.

Então, em 1918, os criptógrafos começaram a experimentar essa chave desprovida de um padrão aparente, conforme ressalta Stallings (2015), contidas em blocos de uma única vez como era conhecido por ser descartável, isto é, a segurança estava no fato de se usar uma única vez, o que implicava em uma cifra indecifrável. Contudo, criar uma chave aleatória exigia tempo, esforço e sobretudo, recursos financeiros.

> O bloco de uma única vez é prático apenas para pessoas que necessitam de comunicações ultra-seguras e que podem se permitir arcar com o custo enorme de produzir e distribuir as chaves em segurança. Por exemplo, o telefone vermelho entre os presidentes da Rússia e dos Estados Unidos é codificado usando-se um bloco de cifras de uma única vez. (SINGH, 2014, p.143).

Muitos autores corroboram com esta ideia, um deles afirma que: “a principal defesa contra a técnica criptoanalítica descrita é escolher uma palavra-chave que seja tão longa quanto o texto claro e que não possua relacionamento estatístico com ele.” (STALLINGS, 2015, p.35). Ainda, reitera como uma técnica estrutural dos princípios de muitas cifras simétricas modernas, como a mais utilizada: o data encryption standard (DES), um algoritmo de grande importância para os estudos atuais.

2.10 O poder da Enigma

Nos anos seguintes ao término da Primeira Guerra Mundial, a batalha entre os criptógrafos e criptoanalistas, foi impulsionada a explorar a tecnologia mais avançada para enviar textos criptografados. Segundo Hefez (2013) e de acordo com Singh (2014), a nova tecnologia surge a partir da invenção do arquiteto italiano Leon Alberti, do século XV. Esta invenção foi a primeira máquina de criptografia, conhecida como o *disco de cifras* ou *o disco de Alberti*, que consistia em dois discos de cobres de tamanhos diferentes unidos por um pino central, ambos com o alfabeto gravado em suas bordas, o menor sobre o maior, conforme ilustrado na figura 2.

Para criptografar a mensagem, posicionava uma letra do disco menor, previamente programado, sobre a letra A do disco maior, representado pelo alfabeto original. A posição dos discos era o que determinava o alfabeto criptografado pelo disco menor, ou seja, a chave secreta. Assim bastava substituir as letras da mensagem original por letras que correspondiam ao alfabeto criptografado, indicado pelo disco menor.

Figura 2 - Um disco de cifra dos confederados utilizados na Guerra Civil americana.

Fonte: Timeline created by nidiacortez In Science and Technology[3]

Quinhentos anos após a invenção de Alberti, segundo Hefez (2013), Arthur Scherbius, inventor alemão e engenheiro elétrico, a partir da ideia dos discos de cifras, inventou uma máquina criptográfica que, basicamente, era uma versão elétrica dos discos de Alberti. Esta máquina era conhecida como *Enigma* e foi considerada o mais terrível projeto de cifragem da história.

A Enigma, conforme apresentada na figura 3, era uma máquina eletromecânica, composta, primeiramente, por um teclado onde era realizada a entrada de dados ao digitar o texto a ser criptografado. Em seguida, através de fios elétricos conectados a três componentes, desempenhando a função de um misturador, as letras do texto original convertiam-se em letras do alfabeto cifrado.

[3] TIMELINE CREATED BY NIDIACORTEZ . **Um disco de cifra dos confederados utilizados na Guerra Civil americana**. In Science and Technology[3]Il.color. Disponível em: https://media.timetoast.com/timelines/criptografia-2e44fa7d-5526-4f2f-9b5b-acd17dd9797f. Acessado em 08 jan. 2020.

Como cada um desses componentes eram compostos do alfabeto completo, ao realizar esses arranjos, o movimento dos misturadores fornecia 26x26x26 o que equivale a 17.576 combinações. Além dessa complexidade, Scherbius, ainda conseguiu que estes misturadores também fossem removíveis, logo essa opção fornecia mais 6 formas de arranjos, aumentando a potencialidade de obter um alfabeto criptografado. Finalmente, todas essas partes se conectavam e produziam um resultado através de sinais luminosos, sinalizados por lâmpadas, que tinham a finalidade de indicar as letras do texto cifrado.

Figura 3 - A máquina Enigma

Fonte: Universidade Federal do Rio Grande do Sul – UFRS[4]

Essa tecnologia inovadora, permitia que todo esse processo fosse feito com grande eficiência e exatidão, devido ao movimento automático dos misturadores e à velocidade da eletricidade.

Scherbius, acrescentou outros elementos a Enigma, tornando-a mais eficiente e funcional. Um desses, foi a introdução de um refletor capaz de reverter o processo, ou seja, o emissor digitava uma letra do texto original e através dos sinais enviados aos misturadores eram transmitidos ao refletor. Quando este recebia os sinais, os enviavam de volta, novamente, através dos misturadores, mas ao longo de uma rota diferente, resultando em letras do alfabeto cifrado.

[4] UFRS. **A máquina Enigma**, 2013. Il. color. Disponível em: http://www.ufrgs.br/prorext-siteantigo/news/museu-da-ufrgs-apresenta-ao-publico-maquina-enigma-original-da-segunda-guerra-mundial. Acesso em: 12 mar. 2020.

.

Quando a mensagem criptografada era enviada ao operador de rádio para realizar a transmissão da mensagem, o receptor, ao recebê-la introduzia o texto cifrado e o mesmo processo dos conectores elétricos percorriam o caminho de volta, fornecendo a mensagem original.

Certamente, o destinatário haveria de trazer consigo outra máquina Enigma, juntamente com uma cópia do livro de códigos contendo a regulagem inicial dos misturadores para aquele dia específico, isto é, a chave. Essa programação prévia era definida diariamente por esse livro que era entregue com segurança aos postos onde se operavam as Enigmas.

Em outras palavras, a Enigma, funcionava como um espelho, cuja mensagem entrava original e saia criptografada, da mesma forma que entrava criptografada e saia original. Finalmente, todo esse processo de decriptação só era possível pela funcionalidade do refletor.

Como as máquinas também eram destinadas para fins militares e governamentais, além de comerciais, Scherbius, a fim de tornar a Enigma ainda mais complexa e segura, inseriu um painel de tomadas, que tinha a função de realizar trocas de 6 pares de letras escolhidos a partir das 26 letras do alfabeto, o que resultavam em 100.391.791.500 combinações.

Portanto, a Enigma excedeu a todas as expectativas e sua capacidade de gerar chaves equivalia ao produto dos elementos que compunham a máquina, ou seja, 17576 x 6 x 100.391.791.500, cujo resultado do produto corresponde a 10.586.916.764.424.000 opções de chaves.

Em 1918, Scherbius conseguiu patentear sua poderosa invenção e em 1925, deu início a produção em grande escala das máquinas adquiridas, principalmente, pelo governo alemão e por empresas estatais, como as ferrovias.

> Nas duas décadas seguintes os militares alemães compraram 30 mil máquinas Enigma. E a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo. Com ele, no início da Segunda Guerra Mundial, as comunicações estavam protegidas por um nível sem igual de decifragem. Naquela época parecia que a máquina Enigma desempenharia um papel vital na vitória nazista, mas ela acabou ajudando na queda de Hitler. (SINGH, 2014, p. 161).

De acordo com Stallings (2015), a Enigma usada pelos Alemães assim como a Purple, pelos Japoneses, eram definidas como máquinas de rotor, onde “a máquina consiste em um conjunto de cilindros rotativos independentes, através dos quais

pulsos elétricos podem fluir.” (STALLINGS, 2015, p. 38). Contudo, possuem as mesmas estruturas básicas descritas, anteriormente, na composição da Enigma.

2.11 A inacreditável conquista da Polônia

Com efetivo uso da máquina Enigma, no período pós-guerra, os americanos, britânicos e franceses realizaram várias tentativas de desvendar a Enigma, porém frustradas.

Como a Alemanha foi vencida por eles na Primeira Guerra Mundial, os aliados, sem motivação e confiantes pela segurança da vitória, aos poucos, diminuíam a esperança em vencê-la. Conforme evidencia Singh (2014, p. 163), “Parece que o medo era a principal força impulsionadora e que a adversidade é um dos fundamentos de uma decifração bem-sucedida.” Ainda, segundo o autor, a Polônia se superou em matéria de criptoanálise e detalha a sua incrível participação no desafio de vencer a Enigma.

Inicialmente, o que motivou a Polônia no enfrentamento à Enigma, foi o fato de sentir-se ameaçada pelas nações: Rússia e Alemanha. Por questões de segurança, ela decidiu continuar a luta contra a poderosa máquina de cifragem alemã, e produzir meios de defesa diante de uma possível investida. Então, criaram um departamento de cifras, conhecido como Biuro Szyfrów.

Enquanto isso, os franceses tiveram acesso a documentos secretos que foram vendidos por um informante alemão, chamado de Hans-Thilo Schmidt. Esses documentos vieram diretamente do centro de comando da Enigma e tinham informações secretas sobre o uso dela, assim como também informações a respeito do livro de códigos e a disposição da fiação de cada misturador.

Como havia uma década que a França tinha assinado um acordo de cooperação militar com os poloneses, então eles entregaram todas as informações obtidas pela espionagem através de Schmidt. Com estas informações, o departamento de cifras da Polônia conseguiu construir uma réplica da Enigma. Contudo, era apenas um ponto de partida, pois sabia-se que a segurança do sistema não estava em ter a posse da máquina e sim em obter a chave, ou seja, o ajuste inicial da máquina em segredo. Pois para um criptoanalista decifrar uma mensagem interceptada, além de possuir uma réplica da Enigma, teria que descobrir qual seria a chave utilizada pelos alemães para cifrar as mensagens.

Convencidos da complexidade da Enigma por ser uma cifra mecânica, porém sem perder a motivação e a esperança, provavelmente movidos pelo medo de uma nova invasão alemã. O departamento de Cifras Biuro constatou a necessidade de se formar um grupo de pessoas com formação mais científica. Então realizou um curso de criptografia e convidou 20 matemáticos que falavam fluentemente alemão, entre eles, felizmente, estava Marian Rejewski, um dos matemáticos que conseguiu desvendar as primeiras versões da Enigma.

Os poloneses acreditavam que as mensagens interceptadas e cifradas poderiam levar a um caminho para identificação da chave. Como já conheciam o funcionamento da máquina e sabiam dos ajustes diários realizados pelos operadores delas, Rejewski começou a investigar um padrão nos textos cifrados. Logo, percebeu que os alemães, astuciosamente, usavam a chave diária para transmitir uma nova chave que seria encarregada de cifrar e decifrar a mensagem enviada.

Prudentemente, para que não ocorresse incertezas no envio da nova chave, convencionou-se a transmiti-la replicada. Por exemplo, se fosse DMB a chave para enviar a mensagem, então usava o ajuste inicial, definida pelo livro dos códigos, para criptografar DMBDMB.

Analisando todo o processo de funcionamento da Enigma, Rejewski estrategicamente buscava encontrar padrões, assim ele se concentrou em examinar a duplicidade das chaves enviadas. Então, esse foi o caminho que o levou a estudar um tipo específico de padrão, onde eram geradas correntes de letras e com isso, começou a catalogadas.

Seguindo esse raciocínio, Rejewski conseguiu identificar esse padrão e constatou que eram diretamente refletidos pelos ajustes dos misturadores, o que reduziu, consideravelmente, o número de possibilidades. Pois apesar dos misturadores produzirem uma combinação de 105.456 possibilidades, resultado do produto de 6 arranjos entre eles por 17.576 orientações dos mesmos, ainda assim, eram cem bilhões de vezes menor comparado com todas as chaves que a Enigma podia gerar. Dessa forma, era humanamente possível que as equipes do departamento de cifras fizessem a checagem.

Após um ano de estudos dos padrões observados e catalogados, de extraordinário empenho e dedicação, Rejewski conseguiu desvendar o padrão das correntes analisadas. E utilizando de meios de natureza igual a Enigma, também mecanizara o processo ao projetar e construir 6 máquinas que representavam os

arranjos dos misturadores, formando uma unidade de aproximadamente um metro de altura, denominada por ele de bomba.

> O sucesso polonês na quebra da Enigma pode ser atribuído a três fatores: medo, matemática e espionagem. Sem o medo de uma invasão, os poloneses poderiam ter se sentido desencorajados pela aparente invulnerabilidade da cifra da Enigma. Sem a matemática, Rejewski não teria sido capaz de analisar as correntes. E sem Schmidt, [...], a fiação dos misturadores não teria sido descoberta e a criptoanálise não teria nem mesmo começado. (SINGH, 2014, p. 176).

Embora Rejewski tivesse descoberto o padrão das correntes, muito trabalho, detalhes técnicos e testes foram executados para que a Enigma fosse vencida, inclusive usando a própria réplica para analisar a disposição dos fios no quadro de tomadas e, finalmente, após incansáveis tentativas, produzir chaves que fizessem sentido.

Porém, em 1938, os alemães aumentaram, consideravelmente, a segurança da Enigma. Com isso, todos os avanços conquistados por Rejewski já não podiam ser aplicados, pois foi introduzido à máquina mais 2 misturadores, aumentando de 6 para 60 formas de ajustes e alteraram o quadro de tomadas, passando de 12 trocas de letras para 20.

Essas novas medidas adotadas pelos alemães foram responsáveis pelo declínio do trabalho do departamento de cifras. Primeiro, porque o investimento necessário para adequar essas novas alterações das bombas, estourariam em quinze vezes mais o orçamento anual e, em segundo, a corrida contra o tempo era uma preocupação causada pela iminência de uma nova guerra.

Portanto, para não deixar perder todos os avanços criptoanáliticos conquistados pelo Biuro, até então desconhecido pelos aliados, o departamento tomou a decisão de convidar os aliados franceses e britânicos, revelar tudo que foi descoberto sobre a Enigma e transferir todo o conhecimento adquiridos, as réplicas da Enigma, plantas e diagramas das bombas de Rejewski, a fim de que estas informações não fossem perdidas em caso de uma possível invasão.

Dessa forma, garantiria que o trabalho fosse continuado nos países aliados. Duas semanas após tomar todas essas sábias providências, no primeiro dia de setembro, a Alemanha invadiu a Polônia.

2.12 Evolução da Enigma e a Segunda Guerra Mundial

Os aliados ficaram surpresos com o progresso da criptoanálise desenvolvida pelos poloneses, particularmente, os franceses, pois parte desse sucesso se devia a espionagem de Schmidt. Contudo, a admiração maior devia-se ao fato de terem julgado sem valor as informações obtidas e que, nas mãos dos poloneses, surtiram efeitos que os colocaram a uma década a frente do mundo.

Com essa experiência, os franceses avaliaram a importância de se empregar matemáticos e cientistas na formação de equipes de criptoanalistas e ainda, constataram que a Enigma não era mais o que julgavam ser uma cifra perfeita.

Na Inglaterra, conforme os relatos de Singh (2014), uma nova organização de criptoanalistas se concentrou em Bletchley Park, em Buckinghamshire, onde situava a sede da Escola de Cifras e Códigos do Governo. Este local tinha capacidade de atender um grande número de equipes, assim como tinham à disposição recursos financeiros destinados a dar continuidade as descobertas de Rejewski.

Considerando a disponibilidade dos meios de comunicação, como o rádio, Bletchley previa e estava preparada para um fluxo de dois milhões de palavras criptografadas por dia o que correspondia a quantidade mensal durante a Primeira Guerra Mundial.

Diante das incursões alemãs tomadas em 1939, as grandes mentes de Bletchley, rapidamente, dominaram as técnicas polonesas. No entanto, estavam diante de uma Enigma muito mais difícil de decifrar e apesar de uma numerosa e organizada equipe, diariamente, à meia noite, encerrava o uso da chave utilizada para cifrar as mensagens do dia. E no dia seguinte, iniciava-se todo trabalho novamente.

> A busca por novos atalhos criptoanalíticos era necessária porque a máquina Enigma continuou a evoluir ao longo da guerra. Os criptoanalistas eram continuamente forçados a inovar, a reprojetar e melhorar as bombas e a criar estratégias inteiramente novas. Parte do motivo para seu sucesso era a combinação bizarra de matemáticos, cientistas, linguistas, especialistas na cultura clássica, mestres do xadrez e viciados em palavras cruzadas dentro de cada casa. (SINGH, 2014, p. 186).

Certamente a busca por vencer a Enigma revelou notáveis criptógrafos, onde cada um contribuiu significativamente, mesmo por partes, nesse processo. Entretanto, nessa época, Alan Turing destacou-se, grandiosamente, pois ele conseguiu identificar as maiores fraquezas e desvendou novas possibilidades de quebrar a cifra da Enigma.

Antes de Alan Turing ir para Bletchley, ainda no período escolar em Sherborne, em companhia de seu único amigo, Christopher Morcom, ambos se destacaram pelo interesse em ciências da qual compartilhavam ideias, descobertas e experiências científicas. Após, 4 anos de convivência, em 1930, a fatalidade causada por uma súbita tuberculose levou seu amigo, provocando um forte impacto na vida afetiva e profissional de Turing. Devido ao sentimento que tinha em relação a Morcom e arrasado pela perda, Turing resolveu se dedicar aos estudos científicos e seguir os passos idealizados por seu amigo.

Então, em 1931 ele foi admitido no King's College em Cambridge. E por intermédio dos seus trabalhos acadêmicos como professor e seu destaque no meio científicos realizados em Cambridge, Turing foi convidado a tornar-se criptoanalista de Bletchley.

Já como membro de Bletchley, tomando conhecimento de todas as técnicas de criptoanálise desenvolvida pelos poloneses e, a partir delas, apropriando-se das novas adaptações da Enigma, Turing dedicou seu trabalho, particularmente, em prever modificações no sistema das chaves que pudessem ser feitas pelos alemães e em consequência disso, comprometer todo avanço conquistado pelos criptoanalistas.

Com esse propósito, procurou uma forma alternativa de ataque a Enigma, algo que não dependesse da repetição dos ajustes diários, pois os alemães, a qualquer momento, poderiam perceber que esse procedimento comprometeria o seu sistema de segurança.

Durante seu trabalho na universidade em Cambridge, Turing já desenvolvia teorias que "fornecera uma sólida base teórica para a computação, dando ao computador um potencial até então não imaginado." (SINGH, 2014, p. 190). Ainda que limitada a tecnologia para a década de 1930. A partir dessas teorias, juntamente com algumas observações feitas sobre a rotina dos operadores da Enigma, foi possível desenvolver uma máquina que fizesse a checagem humanamente impossível para um dia.

Inicialmente, Turing observou que havia sempre um padrão seguido para escrever a primeira mensagem do dia, ou seja, sempre no começo da mensagem fazia-se a previsão do tempo. Posteriormente, a partir de uma coleção de mensagens decifradas, resultado do trabalho realizado pelas equipes de Bletchley, ele conseguiu observar um protocolo rigoroso e uniforme na estrutura das mensagens e reconheceu

que a palavra *tempo* sempre estava presente no início do texto. Finalmente, fazendo a comparação do texto original com as palavras cifradas que correspondiam a ela, Turing trabalhou focado em basicamente descobrir a conexão que havia entre elas, ou seja, quais eram os ajustes realizados na Enigma que faziam esta conversão. Esse processo foi conhecido como *cola.*

Enfim, considerando a estratégia de Rejewski, combinado como o emprego das colas e com base no projeto de máquinas matemáticas inicialmente pensado em Cambridge, entre outros detalhes observados, deu a Turing elementos mentais fundamentais para projetar a complexa máquina também chamada de bomba.

A concretização do seu projeto resultou em um extraordinário trabalho de criptoanálise, sendo reconhecido por seus pares como um gênio em decifrar códigos. Finalmente a Enigma foi desvendada por Turing e em relação a esta conquista Crily (2017, p. 164) observa que “foi um desafio formidável, mas o código sempre foi vulnerável a chave era transmitida como parte da mensagem.”

Em 1940, conforme Turing imaginava, os alemães deixaram de usar a chave duplicada. Felizmente, no mesmo ano, o primeiro protótipo da bomba foi entregue e aperfeiçoado, de maneira que as novas bombas atendessem às expectativas de seu idealizador.

Durante a Segunda Guerra Mundial, as informações obtidas pelo departamento de cifras passavam, apenas, pelas mais altas patentes militares e importantes membros do gabinete de guerra. As decisões tomadas foram historicamente surpreendentes, até mesmo retratadas no filme de 2014, *O Jogo da Imitação*, baseado na história de Alan Turing, dirigido por Morten Tyldum.

Por medida de precaução e com a intenção de não levantar suspeitas pelos Alemães, os aliados, apesar de conhecer a localização de alguns submarinos, deixavam passar, pois se atacassem a todos, certamente os alemães chegariam à conclusão óbvia de que suas mensagens cifradas pela Enigma estavam sendo decifradas pelos aliados.

Com essa estratégia e, lamentavelmente, apesar de todas as vidas perdidas em decorrência disso, os quebradores de códigos de Bletchley foram responsáveis pela abreviação da Guerra em mais ou menos três anos.

> O historiador David Kahn resume o impacto da quebra da Enigma: ‘Ela salvou vidas. Não apenas vidas aliadas e russas, ao encurtar a guerra, mas vidas alemãs, italianas e japonesas também. Algumas das pessoas que estavam vivas depois da Segunda Guerra Mundial não teriam sobrevivido se não

> fossem essas soluções. Esta é a dívida que o mundo tem para com os quebradores de códigos, este é o valor humano de seus triunfos.' (SINGH, 2014, p. 209).

Os segredos de Bletchley foram guardados até a década de 70. Infelizmente, muitos desses heróis de guerra não tiveram suas contribuições, publicamente, reconhecidos a tempo. Para Alan Turing, além de não ser reconhecido pela sua extraordinária contribuição à criptoanálise, foi condenado por sua homossexualidade, sendo publicamente humilhado devido a decisão do julgamento ter sido noticiada pelos jornais. Consequência disso, ele foi proibido de fazer suas pesquisas relacionadas ao seu projeto de desenvolvimento do computador e obrigado a se submeter a terapias de hormônios que resultaram em depressão e suicídio aos 42 anos de idade.

2.13 O grande problema do século XX

Durante o período Pós-Guerra, conforme descreve Singh (2014), grandes avanços tecnológicos se deram a partir das máquinas eletromecânicas que vieram superar as bombas de Turing. Uma delas de grande importância tecnológica, é o Colossus, projetado por Max Newman e concretizada por Tommy Flowers, em 1943. A Colossus foi considerada uma máquina precursora do computador moderno, por apresentar componentes eletrônicos com capacidade de programação e de velocidade.

Logo após a Colossus, outras máquinas surgiram com maior capacidade de processamento. Consequência dessa evolução, era o nascimento dos computadores modernos. Embora seu uso fosse restringido àqueles que possuíssem computadores, ou seja, ao governo e aos militares, os criptoanalistas tiveram acesso a uma ferramenta com alto poder de quebra de todo tipo de cifras.

Na década de 1960, não tardou muito para que os computadores se tornassem amplamente acessíveis e mais baratos. Com isso, mais empresas puderam adquirir computadores e utilizá-los pra trocas de informações importantes. Portanto, era necessário proteger as mensagens através da criptografia.

Nessa nova perspectiva, Stallings (2015) apresenta a cifra de Feistel, criada por Horst Feistel, que em 1973, propôs, formalmente, um sistema padronizado de cifragem, conhecido como *Lucifer*. Como esse sistema de cifragem era considerado

um dos mais poderosos comercialmente conhecido. Então foi aceito pela Agência de Segurança Nacional (NSA). Contudo, impuseram uma condição, limitaram o número de chaves, o que correspondia a 56 bits escrito em linguagem binária. Dessa forma, nenhum computador civil tinha o poder de decifrar e com isso, gerava um grande nível de segurança. Porém os computadores da NSA tinham este poder, o que lhes proporcionavam uma forma de controle.

Por fim, em 23 de novembro de 1976, a cifra Lucifer de Feistel, foi o mais importante e complexo sistema de cifras simétricos que culminou oficialmente como Padrão de Cifras de Dados (DES) - Data Encryption Standard e continua sendo o padrão oficial americano de cifragem.

Naturalmente, junto com todo esse progresso em tecnologia de informação, veio um grande problema, *a distribuição de chaves*. Pois as formas de criptografia ainda eram através de substituição e transposição, logo era necessário que emissor e receptor tivessem acesso as chaves secretas que permitiam a segurança do sistema. Portanto os custos tornavam elevados demais, pois a dificuldade logística com o fluxo cada vez maior de informações as tornava inviáveis. “Não importa o quão segura seja uma cifra em teoria, na prática ela pode ser prejudicada pelo problema da distribuição de chaves.” (SINGH, 2014, p. 276).

Assim, no século XX, a solução para o grande problema da distribuição de chaves foi considerada um dos maiores avanços desde a invenção da cifra monoalfabética. Segundo Hefez (2013), essa conquista se deve a três grandes fascinados por matemática e obcecados em desvendar este grande problema, Whitfield Diffie, Martin Hellman e Ralph Merkle. Juntos procuraram um método prático de resolver essa questão. Esses três norte-americanos, após diversas tentativas fracassadas e com muita persistência e entusiasmo, conseguiram encontrar a solução.

Suas pesquisas estavam concentradas em funções matemáticas consideradas de mão única, ou seja, operações matemáticas que transformam um número em outro e possuem a característica de ter o processo irreversível. Essas qualidades tem como base a *aritmética modular,* também conhecida como a aritmética do relógio. Por exemplo, ao imaginar o mostrador de um relógio, a partir do 9 e avançando 7 posições, chega-se na posição representado pelo 4, ou seja, na linguagem de congruência modular, tem-se:

$$9 + 7 \equiv 4 \pmod{12}$$

A ideia de Hellman foi publicada por Hefez (2013), Singh (2014) e Stallings (2015), através de personagens que representavam o emissor, receptor e o interceptador da mensagem, por meio de Alice, Bob e Eva.

> O esquema para troca de chaves de Diffie-Hellman-Merkle, como é conhecido, permite que Alice e Bob estabeleçam um segredo através de um debate público. Esta é uma das descobertas mais racionais da história da ciência e forçou todo o estabelecimento criptográfico a reescrever suas regras. Diffie, Hellman e Merkle demonstraram publicamente sua descoberta na Conferência Nacional de Computação, em junho de 1976, ante um público perplexo de especialistas em criptografia. No ano seguinte eles requereram a patente. (SINGH, 2014, p. 292).

Segundo Stallings (2015), depois que Diffie-Hellman-Merkle estudaram a aritmética modular por dois anos, conseguiram encontrar uma função de *mão única* do tipo $Y^x(mod\ P)$, em que Y e P eram dois valores escolhidos por Alice e Bob, desde que $Y < P$. Estabelecido os números, mesmo sendo interceptado por Eva, através de uma escuta na linha telefônica, observa-se como a função de mão única resulta em um processo difícil de ser revertido, principalmente quando escolhidos grandes valores.

Como exemplo, suponha que Alice e Bob tenham escolhidos os seguintes valores $Y = 7$ e $P = 11$. Então o processo ocorre conforme descrito na tabela 3.

Tabela 3 – Esquema da função de mão única genérica de Diffie-Hellman-Merkle

Alice	**Bob**	
Alice, secretamente, escolhe um valor para A. Por exemplo: A=3.	Bob, também escolhe um valor para B. B=6.	*Etapa 1*
Alice substitui o número escolhido na função $Y^x(mod\ P) \rightarrow 7^3(mod\ 11) \equiv 343(mod 11) \equiv 2(mod 11)$,.	Bob, também faz o mesmo processo com o valor dele, $Y^x(mod\ P) \rightarrow 7^6(mod\ 11) \equiv 117.649(mod 11) \equiv 4(mod 11)$.	*Etapa 2*
Alice envia seu resultado para Bob como $\alpha = 2$	E Bob envia para Alice o seu resultado como $\beta = 4$	*Etapa 3*
Neste momento, Alice e Bob trocam as informações. Isto é , Alice recebe o valor de β e Bob o valor de α. Podendo usar a mesma linha telefônica em que Alice e Bob escolheram os valores de Y e P, mesmo sendo interceptado por Eva, ainda assim os números trocados não é a chave secreta, e por isso não faz diferença que Eva os conheçam.		*A troca*
Alice calcula a solução usando o resultado de Bob. $\beta^A(mod\ 11) \rightarrow 4^3(mod\ 11) \equiv 64(mod 11) \equiv 9(mod 11)$.	Bob calcula a solução usando o resultado de Alice. $\alpha^B(mod\ 11) \rightarrow 2^6(mod\ 11) \equiv 64(mod 11) \equiv 9(mod 11)$.	*Etapa 4*

Logo, Alice e Bob encontram o mesmo número 9. Portanto 9 é a chave procurada.

Fonte: Adaptado pelo autor de O Livro dos Códigos

Analisando o esquema da função de mão única pela perspectiva de Eva. Se houver uma interceptação da conversa, Eva conhecerá a função e os valores de α e β, porém não saberá o valor de A e B, pois foram mantidos em segredo por Alice e Bob. No entanto Alice e Bob, facilmente, conseguirá revertê-la, mas escolhidos valores grandes, será muito difícil para Eva reverter o processo.

Para Hefez (2013), esse processo de reverter a função de mão única, pode ser computacionalmente inviável, quando há uma boa escolha para Y ou *P.* Ainda Complementa: “O sistema, porém, tem um grande defeito, pois serve apenas para a troca de chaves secretas entre dois indivíduos de cada vez e isso em um mundo globalizado é totalmente insatisfatório.” (HEFEZ, 2013, p. 319).

Infelizmente, os norte-americanos não conseguiram resolver este problema, mas deixou a notável ideia da Chave Pública (*assimétrica*), pois todo processo de cifragem visto até aqui, trata-se de chaves *simétricas*, onde é necessário usar a mesma chave secreta para cifrar e para decifrar. Essa foi uma ideia extraordinária para o desenvolvimento da chave pública, embora não tenham conseguido mostrar como seria implementada, trilhou caminhos que foram valorosamente aproveitados por outros três grandes criptógrafos.

2.14 Descoberta da Criptografia RSA

As ideias revolucionárias em criptografia de Hellmam-Diffie-Merkle, contribuíram, significativamente, para o avanço de um novo conceito de cifragem e decifragem, cuja relevância é inerente a ideia da chave assimétrica.

> O desenvolvimento da chave pública é a maior e talvez a única verdadeira revolução na história inteira da criptografia. Desde o seu início até os tempos modernos, praticamente todos os sistemas criptográficos têm sido baseados nas ferramentas elementares da substituição e permutação. (STALLINGS, 2015, p. 199).

Em 1975, Diffie publicou o resumo de sua teoria em relação a chave *assimétrica*, que ficou conhecida como chave pública e chave privada. Conforme classifica Stallings (2015), o sistema de chave pública é de conhecimento de todos os

interessados que desejam enviar uma mensagem para o destinatário, ou seja, àquele que detêm a chave privada para decifrar as mensagens recebidas. Infelizmente, Diffie não chegou a uma função de mão única que satisfizesse os critérios das duas chaves. Contudo, ele “não conseguiu implementar a sua ideia na prática, mas a publicou para que outros pudessem resolver o problema”. (HEFEZ, 2013, p. 319).

O que tornava a chave assimétrica tão especial, de acordo com Singh (2014), era o fato de solucionar o problema de distribuição das chaves, pois não eram mais necessárias as trocas secretas. A chave pública era amplamente divulgada de modo que qualquer interessado pudesse cifrar uma mensagem e enviá-la. Porém, apenas o dono da chave privada poderia decifrá-la. Portanto, o sistema aparentemente simples, precisava de uma função matemática que cumprisse essa condição.

Estimulados pelo grande desafio, outro trio de pesquisadores se interessou em encontrar a cifra assimétrica. Segundo informa Coltinho (2014), a equipe era formada por dois pesquisadores cientista em computação; Ron Rivest e Adi Shamir e o terceiro integrante, era Leonard Adleman, um matemático. Juntos formavam uma equipe de pesquisadores do Laboratório de Ciências de Computação em Massachussets Institute of Technology (M.I.T.).

Finalmente, em 1977, Rivest-Shamir-Adleman conseguiram encontrar a cifra mais usada na criptografia moderna e o sistema ficou conhecido como RSA, que correspondem as iniciais de seus nomes. “O método se baseia num teorema com 200 anos de idade de um ramo da matemática famoso por ser o mais inútil de todos.” (CRILLY, 2017, p. 164). O que concorda com as seguintes observações:

> Até então, a Teoria dos Números, da qual a Aritmética é a parte mais elementar, era considerada uma das áreas mais puras e abstratas da Matemática, desprovida de aplicações práticas. Esse Panorama muda completamente a partir do desenvolvimento da Teoria da Informação, que compreende a Criptografia entre outros assuntos, motivada pela evolução e popularização dos computadores e a facilidade de conexão com as grandes redes mundiais. (HEFEZ, 2013, p. 310).

Devido ao considerável valor do sistema RSA para a efetiva segurança da informação, notáveis autores escreveram sobre o assunto, dentre eles destacam-se; Coltinho(2014), Singh(2014), Hefez (2013), Stallings (2015), Crilly(2017). Em comum, todos relatam de forma semelhante a descoberta do método RSA e descrevem como se deu este processo de chaves assimétricas.

Basicamente, o método consiste em encontrar dois grandes números *primos, p* e *q*. O produto entre eles resulta no valor de *N.* Sendo definido número primo, como um número que não possui divisores, exceto ele mesmo ou 1. O valor de *N* representa a chave de decifragem pública*,* que poderá ser divulgada a quaisquer meios de comunicação e de informação.

A seguir, outro elemento, também público, representado por e, tal que cumpra a condição de que $(e, \varphi(m)) = 1$. Onde $\varphi(m) = (p-1)(q-1)$, em que e e $\varphi(m)$ são primos entre si. O que significa que entres eles não há divisores comuns, exceto o 1, ou seja, o máximo divisor comum (mdc) entre eles é 1. Enfim, *N* e e, são chamados de chaves públicas e *p* e *q* são as chaves privadas.

Inicialmente, para que alguém possa enviar uma mensagem à pessoa que detêm a chave privada, precisará das informações dos valores de *N* e e. Posteriormente, deverá converter as letras em números, conforme tabela 10, sugerida no capítulo 3 como aplicação para o ensino de matemática. E para finalizar a fase denominada de pré-codificação, deverá observar as seguintes regras básicas:

I. Os espaços entre as palavras serão substituídos pelo número 99;
II. Os valores adotados na tabela 9 deverão iniciar com dois algarismos, pois evita ambiguidades, visto que se A for 1 e B, 2, o código 12 não deixará claro se refere a L ou AB (localizado na posição 12ª do alfabeto);
III. Ao unir os números pré-codificados, a separação será realizada por bloco, observando que o valor de cada bloco deverá ser menor que o valor de *N.*

No Programa de Iniciação Científica, Coltinho (2007), observa ainda que, como cada bloco não representa necessariamente uma unidade linguística, então a decodificação por análise de frequência também seria impossível.

Por fim, como será visto na parte de aplicações, no capítulo 3, a codificação propriamente dita, será calculada pela função de mão única a partir de cada bloco *b* e a mensagem codificada será a sequência dos blocos codificados C(*b*), nessa ordem. O cálculo de cada bloco é dado por:

C(*b*) = resto da divisão de b^e por *N,* ou seja, pela aritmética modular, pode-se calcular C(*b*) $\equiv b^e (mod\ N)$. De modo que, segundo Coltinho (2014), o par *(N,* e) é denominado de *Chave de Codificação* do sistema RSA.

Para decifrar a mensagem o destinatário que tem a posse da chave privada e dos valores de *p* e *q*, deve calcular o valor de outro elemento essencial, conhecido como chave da decifragem d. Para encontrá-lo, basta inserir na função:

$$ed \equiv 1(mod(\varphi(m))$$

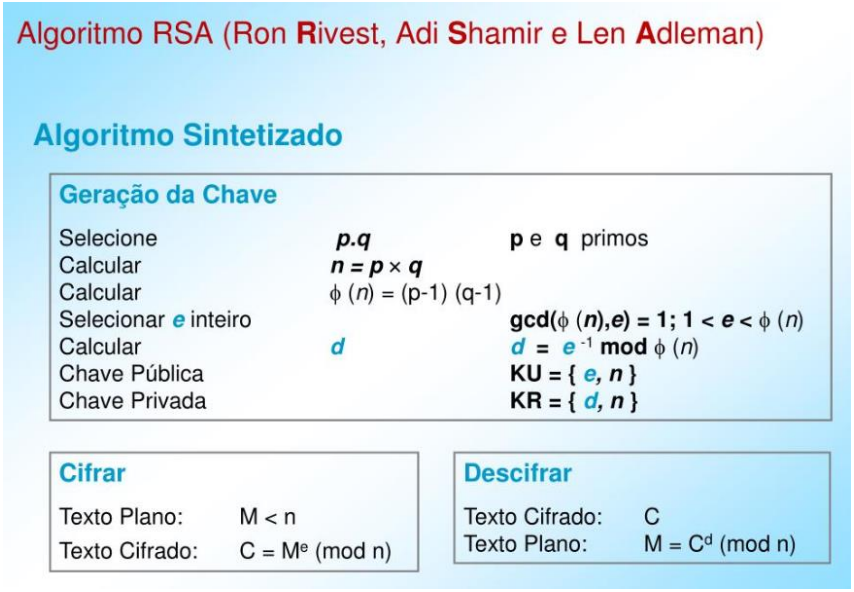
Para efetuar o cálculo desta congruência, pode-se também resolver aplicando o algoritmo euclidiano estendido ou equação modular, assim ao obter o valor de d, utiliza-se a próxima fórmula para finalizar o processo de decifragem da mensagem.

$$D(b) \equiv C^d(modN)$$

Portanto, esse processo será finalizado ao utilizar a tabela inicial para converter os códigos encontrados em sequência numérica, tomados dois a dois, obtém-se os valores originais cuja representação implica nas letras do texto claro.

Em síntese, Rivest, Shamir e Adleman conseguiram criar uma função de mão única em que a partir dos valores primos grandes, *p* e *q* secretos, o processo poderá ser revertido. A vantagem consiste em usar a função de mão única para que qualquer pessoa possa utilizar a chave pública *N* para cifrar a mensagem. No entanto, somente a pessoa que detém a chave de decifragem *d*, definida a partir dos primos escolhidos poderá revertê-la. Para melhor compreensão, observe a figura 4 onde é descrito o algoritmo RSA.

Figura 4 – Algoritmo sintetizado RSA



Fonte: Slide Serve[5]

[5] SLIDE SERVE. **Algoritmo RSA**, 2020, p.6. Disponível em: https://www.slideserve.com/milos/meditar-produz-sabedoria. Acessado em: 14 abr. 2020.

Certamente, o método RSA é um dos sistemas mais moderno de criptografia. A Teoria dos Números é a base matemática que garante a segurança dele. Pois se a escolha de *p* e *q* representar números primo muito grandes, o produto resulta em um valor maior ainda, assim o processo de reversão pela fatoração torna-se impossível.

Para Coltinho (2014), são equivalentes as expressões decifrar o código RSA e fatorar o valor de *N*. Essa observação se completa ao afirmar que, “se *N* for um número suficientemente grande, será virtualmente impossível deduzir os valores de *p* e *q* a partir de *N* e este é talvez o aspecto mais belo e elegante da cifra assimétrica RSA.” (SINGH, 2014, p. 301).

Singh (2014), apresenta valores como exemplos que ocorrem em transações bancárias, na ordem de $N = 10^{308}$, o que corresponderia ao tempo de mais de mil anos para quebrar a cifra pelo simples processo de fatoração. E isso, somente seria possível se unissem algo em torno de cem milhões de microcomputadores para realizar tal tarefa. Atualmente, os valores imensamente grandes para *N* são triviais. E como ainda não existe um processo de fatoração que seja rápido suficiente, o sistema RSA continua sendo imbatível.

Por fim, a “chegada dos telégrafos e finalmente dos computadores revolucionaram a Teoria da informação.” (HEFEZ, 2013, p. 316). Esses fatos foram fundamentais para caracterizar a evolução criptográfica. E neste contexto, percebe-se o quanto a matemática contribuiu em todos os aspectos.

Por último, o método RSA, considerado a maior descoberta em criptografia, teve a Teoria dos Números como a base matemática para o desenvolvimento do sistema que, atualmente, é utilizado com segurança para proteger todo tipo de comunicação.

3 EDUCAÇÃO PROFISSIONAL E INTEGRAÇÃO ENTRE MÉDIO E TÉCNICO

Neste capítulo, inicialmente, será abordado a breve história da educação profissional no Brasil; em um segundo momento, pretende-se apresentar as bases legais do atual Ensino Médio e da Educação Profissional e, por fim, o Ensino Médio Integrado à Educação Profissional, sobretudo nos Institutos Federais de Educação constituídos no Brasil.

3.1 A origem da Educação Profissional no Brasil

Historicamente, a educação profissional no Brasil, se deu no início do século XVIII, por força do Decreto Presidencial 7.566, em 23 de setembro de 1909, com a criação das 19 *Escolas de Aprendizes Artífices*. Segundo Paiva (2013), essa iniciativa teve caráter assistencialista, pois tinha como objetivos oferecer qualificação àqueles desassistidos socialmente, com grande potencial a marginalidade e inseri-los ao mercado de trabalho. Assim, essas medidas reduziriam um grande problema social de aumento da criminalidade e solucionaria o problema da deficiência de mão de obra para atividades primárias do trabalho.

A origem da educação profissional, também determina o início de uma trajetória marcada de sentidos adversos, como se pode observar através dos posicionamentos dos principais autores discorrendo sobre essas teorias, denominadas de **dualidade** na educação. Conceitualmente, de um lado estão os menos desfavorecidos com o ensino limitado e voltado para a classe operária e, do outro lado, o ensino que privilegiava a elite, proporcionando alto nível de educação não conclusivo.

As autoras, (Ciavatta; Ramos, 2011), destaca essa dualidade como um elemento presente ao longo da história da educação profissional:

> No caso do ensino médio e da educação profissional, essa visão dual ou fragmentada expressa-se, historicamente, desde a Colônia, pela reprodução das relações de desigualdade entre as classes sociais, na separação entre a educação geral, como preparação para os estudos superiores, e a preparação imediata para o mercado de trabalho, funcional às exigências produtivas. (CIAVATTA; RAMOS, 2011, p. 28).

Seguindo com os principais fatos apontados neste contexto, a Era Vargas, durante o período ditatorial, outorgou por meio do texto constitucional de 1937, algumas mudanças voltadas para a educação. Uma delas foi a transformação destas Escolas em ensino profissional, ou seja, houve uma ampliação do conceito para novamente atender às necessidades de uma sociedade que precisava de mão de obra qualificada a ser introduzida nas fábricas e nas indústrias.

No que se refere a essas mudanças, (Piletti; Piletti, 2014) ressaltam que houve muita polêmica e divergências. De um lado, os educadores simpatizantes do Estado Novo, consideravam que a formação primária oferecida pelo Estado para a população mais carente era um avanço em termos de democracia. E, em oposição, outros educadores intuíam uma situação antidemocrática e discriminatória, na medida que

se aplicava um tipo de educação favorecendo à elite, contrapondo a outra, considerada limitada e destinada a classe trabalhadora.

Esse último ponto de vista, corrobora com a afirmação de que “esse processo é reiterado na República desde os primórdios e ganha uma estrutura orgânica legal no primeiro governo Vargas, no auge do poder do Estado Novo, nos anos 1940.” (CIAVATTA; RAMOS, 2011, p. 29). Ainda lista leis orgânicas e a criação do Senai em 1942, como ações que reforçaram as distintas finalidades entre os cursos técnicos e os propedêuticos. Este último voltado a formação profissional da Elite, permitindo a continuidade dos estudos através do ensino Superior, ao passo que o técnico, tinham objetivos de qualificar pessoas para o trabalho manufatureiro, limitando a continuidade na sua formação.

Com isso, as bases legais nesta perspectiva, demonstravam, em matéria de Educação, a distinção ao tratamento dado as diferentes classes sociais, ou seja, a dualidade caminhando paralelamente às decisões políticas subordinadas a tendência da economia e a formação básica integral, contemplado pelo trabalho, ciência, tecnologia.

Nesse sentido, Paiva (2013), também concorda com essa posição, ao expor que a educação técnica-profissional, estava muito distante das vantagens da educação secundária. Essa última favorecia a minoria, representada pela alta sociedade. E consequentemente, era o meio de acesso ao ensino Superior, o que contrastavam com a primeira, pois além de ser voltada para atender as carências do mercado, não permitia ao indivíduo que desse continuidade ao ensino Superior.

Novamente, outra medida legal foi tomada no âmbito da Educação Profissional, porém não teve a eficácia desejada após a sua aprovação. A Lei 5.692/71, alterava todo o ensino médio para profissionalizante, de maneira compulsória para todo o território nacional. Para Paiva (2013), foi uma estratégia desastrosa, pois não havia estrutura material e qualificação suficiente dos educadores para cumprir essa obrigatoriedade imposta pela Lei. Consequentemente, sem eficácia prática, mais tarde a Lei foi revogada.

Em 1996 foi criada a Lei de Diretrizes e Bases da Educação Nacional (LDB), nº 9.394/96. Desde a sua aprovação, houve muitas modificações em seu teor especialmente, no que tange a educação profissional. Atualmente, a LDB é o referencial mais importante em matéria de educação no Brasil.

Contudo, anterior a aprovação da lei, muito se debateu e discutiu entre os responsáveis pela elaboração do texto legal. A preocupação era editar uma lei que estivesse voltada ao sujeito e não, somente, a economia e as necessidades de capacitação para o trabalho. Notadamente, no decorrer dos anos 80, percebe-se uma tendência educacional defendida por alguns autores ao discorrer sobre “a luta dos educadores comprometidos com a educação pública e a superação das desigualdades de classe em todas as suas expressões e, particularmente, na educação, foi pela defesa da educação unitária, *omnilateral* e politécnica.” (CIAVATTA; RAMOS, 2011, p. 30).

Ainda acrescenta, que após a vigência da LDB, o ideário mudou, pois já não se preconizava a preparação para o trabalho e sim, tinham uma interpretação muito mais ampla, ou seja, uma formação geral para a vida. Essa nova vertente proporcionava aos cidadãos maiores alternativas de escolhas diante às adversidades sociais e econômicas.

Uma das modificações ocorridas na LDB foi por meio do Decreto 2.208/97. No que se refere ao ensino médio profissional, Paiva (2013), afirma que em termos de currículo, ocorreu uma maior integração na formação do educando, comparando com o que antes tinha um caráter estritamente técnico.

Em contra partida, a nova alteração dada pelo decreto, “restabeleceu o dualismo entre educação geral e específica, humanista e técnica, destroçando, de forma autoritária, o pouco ensino médio integrado existente, mormente da rede CEFET.” (FRIGOTTO, 2007, p. 1139). É o que se constava, através do artigo 1º, inciso I, tornando claro essa dualidade ao afirmar: “promover a transição entre a escola e o mundo do trabalho, capacitando jovens e adultos com conhecimentos e habilidades gerais e específicas para o exercício de atividades produtivas”. (BRASIL, 1997, p.1)

Categoricamente, mostrou que foi uma medida que inviabilizou os espaços exclusivamente dedicados a educação politécnica ou tecnológica, cuja as bases proporcionam “fundamentos científicos gerais de todos os processos de produção e das diferentes dimensões da vida humana”. (FRIGOTTO, 2007, p. 1139).

Certamente, as mudanças ainda eram exíguas, pois não atingiam o ideal pensado por muitos educadores. De um lado, havia pessoas preocupadas na formação humana, visando uma preparação para a vida e voltada para o educando. E, por outro lado, ocorriam pressões decorrentes do capitalismo, incorporado pelas

necessidades e carências que o desenvolvimento do comércio e indústrias demandavam.

Essa realidade, claramente revertia-se em efeitos e cobranças de medidas voltadas a atender as necessidades econômicas. Neste contexto, (Ciavatta; Ramos, 2011), destacam que em todos os projetos apresentados para o ensino médio e para a Educação Profissional, nunca foram voltadas para a formação do aluno, e sim, predominava o caráter economicista da educação.

Contudo, ressalta a necessidade de elaborar um projeto de superação deste dualismo, ou seja, “entre formação específica e formação geral e desloque o foco de seus objetivos do mercado de trabalho para a formação humana, laboral, cultural e técnico-científica, segundo as necessidades dos trabalhadores.” (CIAVATTA; RAMOS, 2011, p.31).

Finalmente, buscando ações inovadoras no âmbito das políticas de educação profissional e tecnológica, o Decreto foi revogado pelo novo Decreto 5.154 de 2004, ratificado pela Lei 11.741 de 2008, conferindo ao ensino técnico, o seu atual formato.

Enfim, este dispositivo legal em seu artigo 4º representou um benefício conquistado por estas reivindicações, onde o texto estabelece que: “A educação profissional técnica de nível médio, nos termos dispostos do § 2º do art. 36, art. 40 e parágrafo único do art. 41 da Lei 9.394, de 1996, será desenvolvida de **forma articulada com o ensino médio**.” Assim, a LDB 9.394/96 eleva a formação integral do aluno a um novo patamar, cujo dispositivo legal favorece a inserção social e estabelece novas oportunidades.

Nesse contexto, Paiva (2013), salienta que a publicação do Decreto 5.154/2004, iniciou um processo de resgate do ensino técnico, devido a divulgação dada pelo Ministério da Educação e Cultura e a implantação de novos institutos. Porém, o ensino técnico não perdeu seu caráter produtivista da educação profissional.

Atualmente, no que se refere aos princípios da Educação em sua forma mais geral, a Constituição Federal do Brasil, promulgada em 1988, corrobora com a Lei de Diretrizes e Bases da Educação Nacional, Lei 9.394 de 1996, garantindo direito universal e obrigação do Estado e da família, visando proteger a formação do cidadão, principalmente, agregando valor ao trabalho como parte do pleno desenvolvimento da pessoa. Segue o teor, respectivamente, das Leis; CF/1988 e LDB 9.9394/96:

CAPÍTULO III
DA EDUCAÇÃO, DA CULTURA E DO DESPORTO

> Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. (BRASIL, 1988, p.1)

> DA EDUCAÇÃO
> Art. 1º A educação abrange os processos formativos que se desenvolvem na vida familiar, na convivência humana, no trabalho, nas instituições de ensino e pesquisa, nos movimentos sociais e organizações da sociedade civil e nas manifestações culturais.
> Art. 2º A educação, dever da família e do Estado, inspirada nos princípios de liberdade e nos ideais de solidariedade humana, tem por finalidade o pleno desenvolvimento do educando, seu preparo para o exercício da cidadania e sua qualificação para o trabalho.
> § 2º A educação escolar deverá vincular-se ao mundo do trabalho e à prática social. (BRASIL, 1996, p.1)

Nessa perspectiva, esses dispositivos legais sinalizam que “a escola realmente cumpra a sua verdadeira função social. Comprometida com a democratização da educação brasileira.” (BRANDT, 2016, p. 3737). Intensificando uma garantia da qualificação profissional integrada ao desenvolvimento pleno da pessoa. Nesse sentido, fica protegido o direito ao exercício da cidadania, bem como garantir que os espaços na sociedade sejam ocupados por todos de forma democrática, justa e solidária.

Por fim, a legislação educacional tão pensada e almejadas pelos educadores foi, finalmente, outorgada. Nesse sentido, vimos que a formação humana esta interligada com a qualificação para o trabalho. Ou seja, foi incorporado o conceito de omnilateralidade tão defendido por muitos notáveis educadores.

A este respeito, a lei vigente, em seus artigos 22 e 27 da LDB 9.394/96 no que tange a educação básica, tem como finalidade para a educação, garantir o desenvolvimento de uma formação comum, assegurando-lhe o pleno exercício da cidadania, trabalho e estudos posteriores. Também estrutura a educação básica em educação infantil, ensino fundamental e ensino médio. Logo seus efeitos protegem e atingem desde a formação inicial dos menores.

Acerca do ensino médio, a LDB em seu artigo 35, incisos I a V, amplia o conceito de educação e flexibiliza os níveis e modalidades de educação, focalizando a formação integral do aluno e sua inserção social.

> DO ENSINO MÉDIO
> Art. 35. O ensino médio, etapa final da educação básica, com duração mínima de três anos, terá como finalidades:
> I - a consolidação e o aprofundamento dos conhecimentos adquiridos no ensino fundamental, possibilitando o prosseguimento de estudos;

> II - a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação ou aperfeiçoamento posteriores;
> III - o aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico;
> IV - a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina;
> V - formação técnica e profissional. (BRASIL, 1996, p.1).

Na mesma direção, determinam os Parâmetros Curriculares Nacionais (Ensino Médio) – Bases legais, (PCN/2000), diretrizes que norteiam o sistema de educação, sob a égide da LDB e reforça o vínculo do ensino médio ao mundo do trabalho e à prática social, ou seja, mediante a Lei, “integra esse nível de ensino que integra, numa mesma e única modalidade, finalidades até então dissociadas, para oferecer, de forma articulada, uma educação equilibrada, com funções equivalentes para todos os educandos” (PCN/2000, p. 10).

Além disso, propõe a formação geral em detrimento da formação específica, desenvolvendo as capacidades de buscar o conhecimento de acordo com as habilidades.

> A facilidade de acessar, selecionar e processar informações está permitindo descobrir novas fronteiras do conhecimento, nas quais este se revela cada vez mais integrado. Integradas são também as competências e habilidades requeridas por uma organização da produção na qual criatividade, autonomia e capacidade de solucionar problemas serão cada vez mais importantes, comparadas à repetição de tarefas rotineiras. (PCN/2000, p.58).

A LDB em seu artigo 35-A, por meio de seus parágrafos, descreve a Base Nacional Comum Curricular, definindo direitos e objetivos de acordo com as áreas de conhecimento. Onde a flexibilização para os currículos deverá estar em harmonia com a Base Nacional Comum Curricular, levando em consideração o contexto histórico, econômico, social, ambiental e cultural.

Em relação ao currículo, a LDB em seu artigo 35-A, § 7º, ao apresentar algumas considerações para o ensino médio, elenca os elementos essenciais para a formação integral da pessoa.

> § 7º Os currículos do ensino médio deverão considerar a formação integral do aluno, de maneira a adotar um trabalho voltado para a construção de seu projeto de vida e para sua formação nos aspectos físicos, cognitivos e socioemocionais. (BRASIL, 1996, p.1).

No que se refere aos itinerários formativos, esclarece Kuenzer (2007), são organizações de diferentes arranjos curriculares, onde há flexibilização quanto ao contexto e as possibilidades de ensino. Fixando assim, as disciplinas obrigatórias de língua Portuguesa e Matemática por todo o percurso, sendo as demais obrigatórias, porém com a possibilidade de ser ofertada em menor percurso. Em caráter opcional, a flexibilização pode ocorrer, também, na ofertar de outras línguas estrangeiras, com exceção da língua inglesa.

Nesta flexibilização, em relação ao currículo no Ensino Médio, apresentados nos Artigos 35 e 36 da LDB, o **trabalho** ganha uma nova e importante dimensão como princípio básico de organização do currículo. Com efeito, o trabalho já não se caracteriza apenas como ensino profissionalizante, a normativa legal estabelece que todos devem ser educados nesta perspectiva, reconhecendo uma das principais atividades humanas.

> ...a preparação para o trabalho [...] destacará a relação da teoria com a prática e a compreensão dos processos produtivos enquanto aplicações das ciências, *em todos os conteúdos curriculares*. A preparação básica para o trabalho não está, portanto, vinculada a nenhum componente curricular em particular, pois o trabalho deixa de ser obrigação – ou privilégio – de conteúdos determinados para integrar-se ao currículo como um todo. (PCN/2000, p. 57).

Em síntese, “pode-se afirmar que o trabalho foi, é e continuará sendo princípio educativo do sistema de ensino em seu conjunto.” (SAVIANI, 1994, p. 13). No plano ideológico, mantém-se em conformidade com a LDB e os PCNs, pois o trabalho não está vinculado a uma modalidade específica, como ocorre no ensino profissionalizante, mas é um elemento intrínseco a todo o currículo ofertado em todas as áreas do conhecimento. Assim, determina uma tendência, no contexto das tecnologias avançadas, a sua unificação.

Os PCNs determinam diretrizes quanto a estas atividades, agregando às escolhas profissionais, formação do exercício à cidadania e “processo de produção de bens, serviços e conhecimentos com as tarefas laborais que lhes são próprias”. (PCN/2000, p. 79).

Finalmente, apresentam dois fatores a considerar. O primeiro abrange a revolução do conhecimento, transformando a organização do trabalho e a forma como as pessoas se relacionam e, o segundo, está relacionada ao aumento da demanda

da escola pública e seu fator de qualidade, ou seja, uma exigência de uma sociedade moderna.

3.2 O Ensino Médio Integrado ao Técnico

Inicialmente, a trajetória da Educação Profissional apresentada foi intencionalmente direcionada a integração do Ensino Médio. Atualmente, a Lei de Diretrizes e Bases 9.394/96, destaca uma renovação em termos educacionais, da qual daremos ênfase devido ao posicionamento deste capítulo. Trata-se da Educação Profissional Técnica de Nível Médio.

Dessa maneira, o artigo 36 da LDB, aponta as formas, articuladas com o ensino médio, são elas: **subsequente**, para aqueles que já cursaram o ensino médio; **concomitante**, ocorre paralelamente ao ensino médio em outras instituições ou na mesma instituição, desde que as matrículas sejam efetuadas distintamente e a **integrada**, cuja forma se dá conforme descrição do Inciso I da Lei:

> I - integrada, oferecida somente a quem já tenha concluído o ensino fundamental, sendo o curso planejado de modo a conduzir o aluno à habilitação profissional técnica de nível médio, na mesma instituição de ensino, efetuando-se matrícula única para cada aluno. (BRASIL, 1996, p.1).

Essa nova modalidade de ensino médio integrado ao técnico foi dada pela redação da Lei nº 11.741/2008, e denomina em seu art. 39 da LDB, de **Educação Profissional Técnica de Nível Médio**, observando os objetivos da educação nacional e exercendo as dimensões do trabalho, da ciência e da tecnologia.

Acerca da interpretação teórica dada a *integração,* (Ciavatta; Ramos, 2011), apresenta um conceito bem mais abrangente. Em primeiro lugar, a expressão remete a formação humana em todas as dimensões da vida, como o trabalho, a ciência e a cultura, proporcionando todo o processo formativo, ou seja, está fundamentada sobre uma perspectiva de formação politécnica e *omnilateral* dos trabalhadores. E, afirma a concepção do trabalho como princípio educativo.

Tal afirmação vem corroborar com Saviani (1994), que considera que educação e trabalho são indissociáveis. Quando há separação, consequentemente, revela o aspecto improdutivo da educação. Para ele, o trabalho está na essência do homem, faz parte de sua existência.

O que se pode inferir, pelo menos teoricamente, é uma maior articulação, entendida de forma mais ampla da formação geral do indivíduo e abrangendo os distintos aspectos envolvidos na questão da educação profissional. Assim, prevê-se a articulação de esforços das áreas da educação, do trabalho e emprego, e da ciência e tecnologia.

Nesse sentido, a articulação entre o Ensino Médio e a Educação Profissional, implicam em várias possibilidades de preparação básica para o trabalho, na primeira modalidade, inclui a formação geral e a preparação para o trabalho. E, na segunda modalidade de ensino, compreende os estudos específicos do curso em formação, obedecendo aos limites mínimos de duração da educação básica.

Contudo, (Ciavatta; Ramos, 2011), advertem para o fato de que na prática, o ensino médio integrado ao técnico, tem sido compreendido como uma preparação imediata ao mercado de trabalho, bem como uma possibilidade para chegar ao ensino Superior. O que não quer dizer que estas razões não sejam importantes no contexto social, de ordem economicista, para a classe dominante. Porém há uma forte contradição com as ideias de intelectuais comprometidos com uma nova concepção de educação para um novo ensino médio integrado que proporcionasse a politecnia, incorporando princípios de integração ao trabalho, ciência e cultura.

Em relação aos profissionais em educação, compreende-se que há uma certa resistência por parte dos professores em aceitar estas ideias, muitos apontamentos são feitos por (Ciavatta; Ramos, 2011) para descrever esta dificuldade, os principais são: a chegada das mudanças de forma impositiva, mentalidade conservadora, desconhecimento dos conceitos legais, falta de estrutura e de condições materiais, ausência de apoio de uma gestão mais participativa e democrática, condições de trabalhos e salários, entre outras.

Diante do exposto, os PCNs (2000), ressalta que a situação do Brasil no contexto da educação do Ensino Médio é alarmante quando comparada ao cenário mundial. Nesse sentido, ainda é um ideal a ser colocado em prática. Contudo, apesar dos imensos desafios, as diretrizes e bases expressas na LDB estão em consonância com as reformas do ensino médio adotadas em muitos países em evidência no que tange a educação de nível médio. Com isso, a educação brasileira pode vislumbrar um futuro de muitas possibilidades.

Finalmente, são mudanças que precisam ser muito bem definidas pelas instituições de ensino, com condições de abarcar todos os envolvidos para que a letra da lei, não seja utópica e sim, percebidas por ações efetivamente concretas.

3.3 Os Institutos Federais de Educação, Ciência e Tecnologia

Diante das adversidades enfrentadas decorrente da implantação da educação profissional integrada ao ensino médio, hoje os Institutos Federais se configuram como importante estrutura para que os jovens tenham efetivo acesso à educação profissional.

A origem dos Institutos Federais de Ciência e Tecnologia (IF) encontra-se no portal do Ministério da Educação do Brasil (MEC). Inicialmente, pelas informações apresentadas, pode-se extrair que os IFs foram criados pela Lei nº 11.892/2008.

Em conformidade com a história relatada, conferidas pelo portal do Ministério da Educação do Brasil, o marco inicial da Rede Federal de Educação Profissional, teve início em 1909, com aquelas 19 Escolas de Aprendizes e Artífices mencionadas no começo sobre a Educação Profissional e Tecnológica - EPT. Houve várias transformações destas escolas no decorrer do tempo, a mais relevante, foi ter originado os Centros de Educação Profissional e Tecnologia (Cefet), por meio do dispositivo legal, Lei nº 6.545/1978.

Em 29 de dezembro de 2008, a maior parte da Rede Federal de Ensino Profissional, entre eles os Cefets, Escolas Agrícolas, Escolas Técnicas Federais e escola federais vinculadas às Universidades, passaram a constituir por força da Lei 11.892/2008, os Institutos Federais de Ciência e Tecnologia.

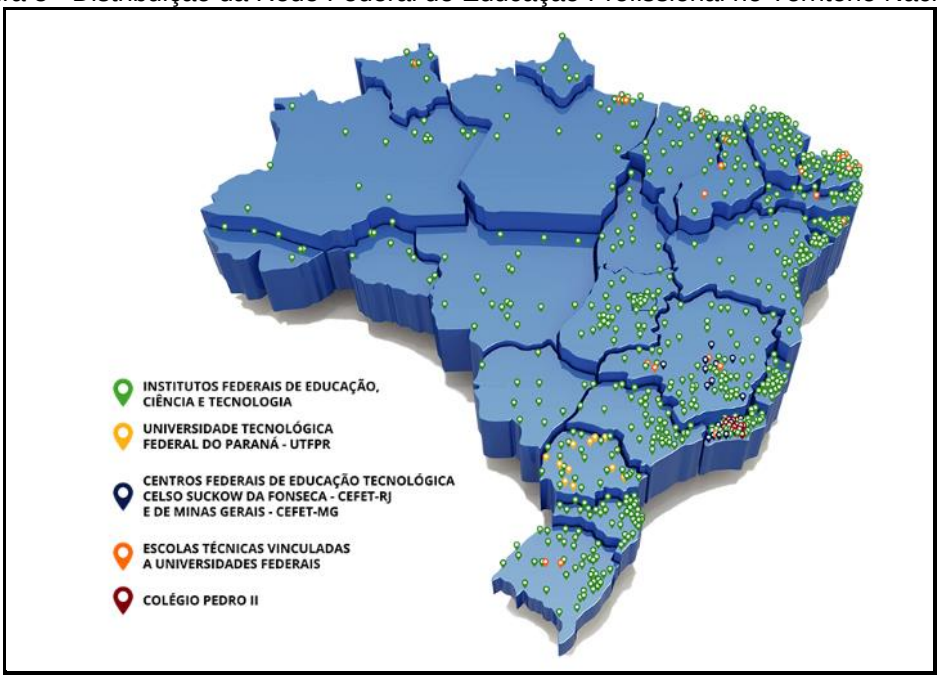
Atualmente, os Institutos Federais configuram como uma importante rede de educação profissional e tecnológica, com oferta pública, inclusive, com acesso garantido por meio de cotas, garantia dada pela publicação da Lei 12.711/2012.

Anterior a esta regulamentação jurídica, as instituições de ensino profissional concentravam-se majoritariamente nas capitais dos Estados, principalmente na região sudeste. Posteriormente, a expansão dos IFs rompeu um patamar histórico da educação profissional, tendo ampliado o seu número de unidades e vagas em todo o país. Na contemporaneidade, a Rede Federal de Educação Profissional foi instituída por todo território nacional e a distribuição de mais de 650 instituições estão ilustradas

na figura 5. Em síntese, o Ministério da Educação divulga dados referente a esta expansão da EPT:

> Em 2019, já são mais de 661 unidades sendo estas vinculadas a 38 Institutos Federais, 02 Centros Federais de Educação Tecnológica (Cefet), a Universidade Tecnológica Federal do Paraná (UTFPR), a 22 escolas técnicas vinculadas às universidades federais e ao Colégio Pedro II. (SETEC/MEC, 2016).

Figura 5 - Distribuição da Rede Federal de Educação Profissional no Território Nacional



Fonte: Adaptado do Ministério da Educação e Cultura. (MEC)

A importância dos Institutos Federais em matéria de Educação Profissional e tecnológica está vinculado a “missão de qualificar profissionais para os diversos setores da economia brasileira, realizar pesquisa e desenvolver novos processos, produtos e serviços em colaboração com o setor produtivo.” (SETEC/MEC, 2016).

A falta de perspectivas para o trabalho e renda fixa aos jovens das classes populares, depositam na educação profissional uma oportunidade. De encontro a isso, segundo o Ministério da Educação, os Institutos Federais, especializados na oferta de educação profissional e tecnológica (EPT), por força da Lei vigente, são obrigados a dedicar-se no mínimo 50% ao ensino médio integrado ao técnico. Dessa forma, está em consonância com a Lei de Diretrizes e Bases 9.394/96.

Nesse sentido, cabe à rede Federal de Educação Tecnológica a responsabilidade de priorizar o ensino médio integrado. “Não se trata de negar a

prerrogativa do ensino superior, mas de garantir o ensino médio integrado como uma de suas prioridades. (FRIGOTTO, 2007, p. 1146).

Discutir a criação dos Institutos Federais, Ciência e Tecnologia se faz pertinente, pois enquanto as escolas pública e privadas, em sua maioria, não se adaptam as diretrizes básicas e as novas normas estabelecida pela Lei 9.394/96 e incorpore o trabalho como condição fundamental a natureza humana, segundo destaca Saviani (1994), o ensino médio integrados dos IFs é uma das modalidades de ensino que melhor interpreta o texto legal, fornecendo aspectos que se mostram inovadoras quanto à sua reorganização.

Certamente, essa reconfiguração propõe uma melhor qualificação na formação profissional, de forma a levar às áreas produtivas e ao desenvolvimento econômico o aprimoramento proporcionado pelo ensino, trabalho e ciência. Nesse sentido, “os Institutos Federais tem o propósito de ofertar uma formação integral e integradora, na qual a qualificação profissional também é pensada como parte da educação mais ampla, transversal e cidadã.” (BRAGATO, 2018, p. 10).

O Ministério da Educação apresenta características importantes, além das que foram elencadas. A instituição é equiparada a Universidades e possui uma estrutura multicampi, cuja implantação está presente em todo território nacional. Além do mais, possui a incumbência de desenvolver pesquisa, extensão e ensino.

Portanto, os Institutos Federais inauguram uma educação profissional diferenciada no Brasil, conforme publicado por Bragato (2018), no V Congresso Nacional em Educação – CONEDU;

> A criação dos Institutos federais, portanto, é uma política pública de educação profissional inovadora que traz novos precedentes para a história educacional do Brasil. Sendo assim, cabe aos pesquisadores estudos que investiguem qualificadamente e criticamente a implantação dos Institutos Federais e os seus desdobramentos e resultados, tendo em vista a sua proposta de criação. (BRAGATO, 2018, p. 11).

A discussão levantada neste capítulo, permite-nos compreender as diversas mudanças ocorridas na história da educação profissional, a dualidade que permearam todas as decisões em relação à matéria, as demandas oriundas da economia e as pressões decorrentes dos embates da política nacional de educação e do ideal almejado pelos educadores e por pessoas que esperam uma formação geral mais completa com domínio e acesso à ciência, trabalho e tecnologia.

Diante de todas as adversidades apresentadas, em especial, ao Ensino Médio no Brasil, estamos distantes de representar um modelo educacional, ainda são muitas as dificuldades e precariedades apresentadas na atual conjuntura vivenciadas pelos jovens brasileiros.

Outros fatores que impactam negativamente na vida dos brasileiros tem sido a instabilidade econômica. Segundo estatística realizada pelo Instituto Brasileiro de Geografia e Estatística, “a taxa de desemprego no Brasil ficou em 11,2% no trimestre encerrado em janeiro, atingindo 11,9 milhões de pessoas, segundo a Pesquisa Nacional Por Amostra de Domicílios Contínua Mensal (PNAD Contínua)” (IBGE/2017), bem como tem externado dados alarmantes de pessoas que não estão procurando emprego e nem trabalhando, totalizando a 65,73 milhões, registrando um recorde desde o ano de 2012.

Nessa lógica, apesar da realidade apresentadas pelo desemprego, reduzidas possibilidades de formação profissional qualificada, o Brasil possui normais legais voltadas para a formação integral da pessoa, com condições de atender as demandas do mercado e além disso, para uma educação de qualidade, que se proponha uma formação para o homem em sua totalidade.

> Os IFs representam uma política educacional com enorme potencial inovador social, econômico e cultural. Todavia, muitos são os desafios que se apresentam à continuidade, melhoria e ampliação da Rede dos Institutos Federais. Para isso, exige-se que o Brasil assuma a Educação Profissional como política de Estado, de longo prazo, que não pode ser deixada a livre vontade do mercado, sujeita a interesses mais imediatos. (BRAGATO, 2018, p. 11).

De fato, a criação dos Institutos Federais de Ciência e Tecnologia, segundo o autor “trouxe uma nova visibilidade ao cenário da política pública de educação profissional brasileira, os quais estão em pleno funcionamento, gerando mudanças por todo território nacional.” (BRAGATO, 2018, p.10). Através desta instituição, uma nova perspectiva foi dada a educação profissional e tecnológica, conferindo uma maior expansão e interiorização, reestabelecendo o processo de democratização no ensino e melhores condições de acesso ao ensino público de qualidade com vistas a inserção qualificada no mundo do trabalho e na continuidade dos estudos, proporcionado pelo ensino Superior.

Portanto, é notório que os Institutos Federais contribuem no desenvolvimento socioeconômico do Brasil. No entanto, em um país onde há uma grave crise social e econômica, delineada pelo grande número de desemprego, pelos baixos índices de

crescimento econômico e uma Educação com muitos percalços, desafios, longe de apresentar um ensino de qualidade e igualitário para todos, mesmo levando em consideração todos os avanços conquistados, é inevitável a presença da dualidade na educação. Pois atinge dois setores carentes na política nacional. Enfim, acredita-se que não há crescimento econômico, social, cultural, científico e tecnológico de um país sem dar a devida prioridade a educação.

4 A APLICABILIDADE DA CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO CONTEXTO DA EDUCAÇÃO PROFISSIONAL

Através da presente dissertação tem-se o intuito de demonstrar como a criptografia pode contribuir para o ensino de matemática no Ensino Médio, especificamente Integrado ao curso Técnico de Informática.

Nessa lógica, cabe primeiramente ressaltar o papel da tecnologia na sociedade da informação, bem como a importância da criptografia na motivação para a aprendizagem, agregando a interdisciplinaridade entre matemática e informática e, finalmente, apresentar técnicas criptográficas com base em conteúdo de matemática, sugerindo propostas de aplicações ao professor, a fim de serem utilizados ou adaptados em sala de aula.

4.1 As Tecnologias na Sociedade da Informação

A sociedade atual tem apresentado muitas mudanças onde a tecnologia tem exercido um papel significativo, sendo indispensável para a sua evolução. Motivo pelo qual há um consenso entre alguns autores em atribuir a denominação de *Sociedade da Informação*. Entre eles, Sousa (2011), ressalta que essa sociedade contemporânea tem como base o conhecimento, onde encontra-se em pleno processo de expansão e de formação global. Além disso, exerce um papel essencial na produção de riquezas, bem como proporciona o bem-estar e a qualidade de vida às pessoas.

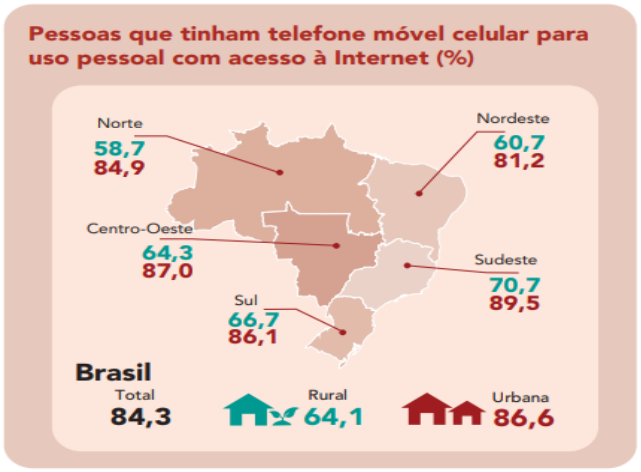
Esta definição corrobora com Brandt (2016), e ainda complementa que essas transformações ocorridas se devem ao desenvolvimento das TICs, onde a evolução acontece em uma velocidade vertiginosa, impactando diretamente no comportamento social. Segundo o autor, as TICs:

> [...] têm alterado profundamente a economia, a política, a cultura, a geografia, o mundo do trabalho, a saúde, a ecologia, a forma de conviver das pessoas, de acessar informação, de comprar e de se comunicar, de se relacionar com os outros e consigo mesmo, de se divertir, além de transformações em muitas outras áreas, atividades e possibilidades até então inimagináveis, que atingem diretamente a vida do homem no mundo e em sociedade. (BRANDT, 2016, p. 3722).

Nesse contexto, destaca-se que “A internet é responsável por grandes transformações sociais e culturais e tornou-se indispensável para a sociedade” (SOUSA, 2011, p. 749). Para que se possa ter uma melhor compreensão do que é a Internet, necessário se faz trazer sua conceituação, a qual consiste em uma rede mundial de computadores interligados. Ainda acrescenta, sendo um canal mundial de distribuição de serviços, bens e empregos. Consequentemente, sendo responsável por importantes mudanças na economia, além de influenciar no comportamento dos consumidores.

Segundo dados fornecidos pelo Instituto Brasileiro de Geografia e Estatística (IBGE), foi realizado pelo processo de Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD-Contínua), em 2017 sobre Tecnologia da Comunicação e Informação – TIC. Um desses levantamentos, conforme apresentado pela fig. 6 destaca o percentual de 84,3% de pessoas que possuem aparelhos de telefonia móvel com acesso à Internet no Brasil.

Figura 6 - Pessoas que tinham telefone móvel celular para uso pessoal com acesso à Internet



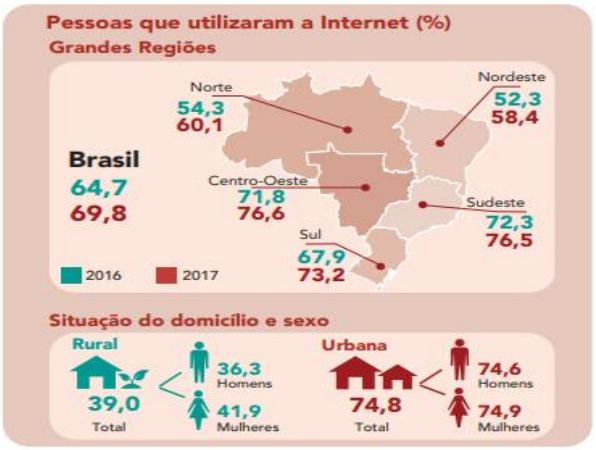
Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios Contínua 2017.

Diante desses dados fornecidos, pode-se observar o quão as pessoas estão conectadas à rede mundial de computadores, assim como utilizam os aparelhos de

celulares para se comunicarem. Dessa maneira, pode-se inferir que também utilizam para outras finalidades tais como: para se informar, aprender, realizar transações bancárias, apropriando-se de todas as vantagens que a tecnologia pode proporcionar.

Outro importante dado apresentado pela PNAD-Contínua (2017) é o percentual de pessoas que utilizam Internet no Brasil, equivalente a 68,8%, indicando um aumento em relação ao ano anterior, sendo apresentado o percentual por regiões conforme mostrado na figura nº 7. Com isso, constata-se que a maioria da população brasileira tem acesso à Internet, quaisquer que sejam os meios de acesso a ela.

Figura 7 - Pessoas que utilizaram a Internet



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios Contínua 2017.

É evidente que a atual Sociedade da Informação tem influenciado a economia mundial, pois a globalização e a interconectividade atingem a todos os setores de forma global. Nessa perspectiva e em face da velocidade e quantidade que transita a informação, cabe analisar os impactos na Educação, pois as novas exigências da aquisição do conhecimento provocam também uma adequação nas instituições de ensino.

A questão que se expõe hoje, decorre do fato que os jovens têm acesso às TICs, nasceram nesta realidade e desenvolvem facilmente habilidades no universo das tecnologias. O que implica pensar o papel do educador, pois dificilmente as aulas tradicionais e a transmissão de conhecimento por si só, motivarão a aprendizagem dos alunos, uma vez que os conteúdos e conceitos da forma como são apresentados

em sala de aula, muitas vezes não fazem sentido e nem satisfazem as expectativas que os jovens esperam da educação.

Nessa nova configuração, destacam-se duas importantes atribuições dos professores na sociedade da informação. Em primeiro lugar, “como a educação e a comunicação são indissociáveis, o professor pode utilizar-se de um aparato tecnológico na escola visando à transformação da informação em conhecimento.” (SOUSA, 2011, p. 210). E, em segundo, compreender que ele não é mais a única fonte de informação, mas é uma delas.

Com isso fica evidente a necessidade dos professores em inovar e acompanhar essas tecnologias, o que não quer dizer que será substituído por elas, mas criará possibilidades de mudanças em sua metodologia, envolvendo formas de ensinar condizentes com o modelo da sociedade do conhecimento.

4.2 A Criptografia como um veículo motivador no Ensino de Matemática

A história da criptografia foi amplamente apresentada no primeiro capítulo. Além disso, ao longo da história relatada, foi abordado como se deu a evolução, enfatizado as mais importantes técnicas presentes em cada época e por fim, foi discorrido acerca do maior avanço em termos de criptografia, o sistema RSA.

De acordo com os objetivos deste trabalho é interessante entender o quanto a matemática faz parte deste processo e mostrar que a criptografia é motivadora para o aprendizado dos conteúdos relacionados à disciplina. Sobretudo salientar o quanto a relação entre a criptografia e a matemática, se deve a evolução das TICs.

A criptografia está diretamente relacionada a segurança da informação, definida por Stallings (2015, p. 6), como a área de segurança de rede e de internet que apresenta critérios para “desviar, prevenir, detectar e corrigir violações de segurança que envolvam a transmissão de informações.” No mesmo sentido o Manual de Segurança de Computadores da National Institute of Standards and Technology (NIST), estabelece:

> ...a proteção oferecida pra um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação (incluindo hardware, software, firmware, informações /dados e telecomunicações). (apud STALLINGS, 2015, p. 6).

Essa segurança tem como requisitos básicos, a *confidencialidade, integridade e disponibilidade,* conforme esclarece o Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil – Cartilha de Segurança para Internet, (2005), como conceitos em que nenhum sistema computacional pode ser declarado totalmente seguro sem a presença destes recursos:

> A **confidencialidade** diz que a informação só está disponível para aqueles devidamente autorizados; a **integridade** diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a **disponibilidade** diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários. (CERT.BR, 2005, p. 30, grifo nosso).

Finalmente, Stallings (2015), complementa que são conceitos que abrangem os objetivos fundamentais de segurança, tanto no que diz respeito a dados quanto a serviços de computação e informação. Além disso, ressalta dois conceitos adicionais: *autenticidade e responsabilização*. Este último, está relacionado ao fato de não haver um método de segurança que garanta 100% de eficácia, então cabe responsabilização a prejuízos oriundos de violação ao sistema de segurança. Quanto ao primeiro, equivale a garantia de se verificar a confiabilidade da fonte.

No mundo atual, a tecnologia da informação e comunicação está em constante evolução e junto a esse crescimento, está o uso dos computadores para desenvolverem inúmeros trabalhos diários, como citado pela cartilha do CERT. São exemplos de transações financeiras, como as relacionadas a compra e venda de produto ou de ordem bancárias, comunicação por e-mails, armazenamentos de dados empresariais, comerciais ou, simplesmente, pessoais.

Enfim, todos os usuários desejam que suas senhas e números de cartão sejam protegidos, assim como possam ter a garantia da não violação de suas contas de acesso à internet, seus dados pessoais e assegurar que o funcionamento de seu computador não seja comprometido por ataques maliciosos.

Nesse contexto, surge a criptografia, onde o CERT apregoa que ela é um campo de estudos que abrange as comunicações secretas e destaca algumas finalidades:

> - autenticar a identidade de usuários;
> - autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
> - proteger a integridade de transferências eletrônicas de fundos. (CERT.BR, 2005, p.115).

Além disso, reforça a necessidade de ter garantida a privacidade da mensagem, que seja assinada, assegurando a capacidade de identificar o remetente e perceber se a mensagem não foi modificada.

Diante do exposto, a criptografia é uma ciência muito eficiente e utilizada nas transações até mesmo imperceptíveis pelos usuários. Através dela é possível realizar trocas de informações e comunicações em segurança. Logo, pode-se concluir que a segurança da Informação depende da criptografia, assim como a criptografia depende da matemática, como visto no capítulo 1.

4.3 A Interdisciplinaridade no Ensino Médio Integrado ao Técnico em Informática

Nos Institutos Federais, o curso Técnico em Informática, na modalidade Integrado ao Ensino Médio, pertencente ao Eixo Tecnológico de Informação e Comunicação e são ofertados em muitos *campus*. Em particular, no Instituto Federal de Rondônia - IFRO, *campus* Cacoal, o Projeto Pedagógico do Curso (PPC), baseia-se nas orientações do Catálogo Nacional dos Cursos Técnicos (CNCT) com articulação das áreas do conhecimento.

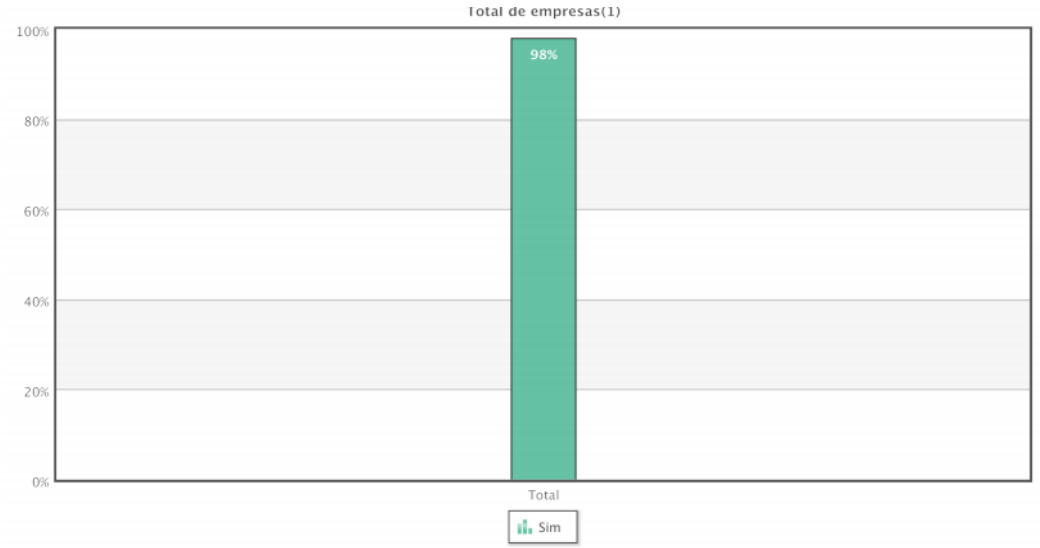
Este instrumento teórico metodológico apresentam os seguintes objetivos:

> OBJETIVO GERAL
> Oferecer formação profissional técnica de qualidade em informática integrada ao ensino médio, na perspectiva de desenvolvimento de sistema. (PPC, 2017, p. 37).
>
> OBJETIVO ESPECÍFICO DO CURSO
> a) Integrar o ensino médio à educação profissional, de modo a promover a formação global e a preparação para o mercado de trabalho. (PPC, 2017, p. 37).

Dessa forma, esses objetivos estão em conformidade com uma das modalidades de ensino e princípios estabelecidos para educação na LDB. O primeiro objetivo específico do PPC, destaca-se por estar de acordo com os requisitos essenciais presentes na elaboração do projeto. Entre eles, assegurar a formação plena, omnilateral dos sujeitos. E, sobretudo ofertar mão de obra qualificada em desenvolvimento de software e infraestrutura de tecnologia da informação em consonância com a demanda local, sem perder de vista a preparação para a vida em sociedade.

O Centro Regional de Estudos para o desenvolvimento da Sociedade da Informação (CETIC), realizou uma pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas empresas brasileiras em 2017, conforme fig. 8, onde é possível observar que quase a totalidade das empresas brasileiras possuem e fazem uso das TICs.

Figura 8 – Empresas que utilizaram computadores nos últimos 12 meses



Fonte: Centro Regional de Estudos para o desenvolvimento da Sociedade da Informação (cetic.br).[6]

Constata-se, com isso, que no universo das TICs, o computador e a Internet consagram-se como poderosas ferramentas. Essa constatação demonstra a necessidade e a importância da oferta do Curso Técnico em Informática Integrado ao Ensino Médio no IFRO, pois independente da região, a informática é uma realidade presente em todas as áreas.

Por fim, “cabe ao IFRO a missão de formar mão de obra qualificada de nível técnico a fim de suprir a demanda das empresas por profissionais de tecnologia da informação.” (PPC, 2017, p. 25). Assim, cumprir com seu papel de instituição responsável em oferecer uma educação integral e contribuir com o desenvolvimento socioeconômico local.

[6] CGI.br/NIC.br. Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br). **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nas empresas brasileiras TIC Empresas 2017**, p.1. Il. color. Disponível em: http://data.cetic.br/cetic/explore?idPesquisa=TIC_EMP. Acesso em: 12 abr. 2020.

Neste cenário, o ementário do curso técnico em Informática Integrado ao Ensino Médio, do IFRO campus Cacoal, apresenta a Matemática como pertencente ao núcleo comum e, especificamente, no núcleo profissionalizante, consta a disciplina Introdução a Tecnologia da Informação. Destaca-se, essencialmente, a seguinte ementa:

> História da tecnologia da informação. Práticas em Sistemas Operacionais de plataformas abertas e fechadas. Noções básicas de Rede de Computadores. Aplicativos de escritório: edição de textos, planilhas eletrônicas, software de apresentação. Uso da internet como ferramenta de pesquisa. Noções básicas de segurança em informação. (PPC, 2017, p. 63).

Em conformidade com os objetivos propostos nesta dissertação, a interdisciplinaridade entre matemática e informática, será apresentado como uma das formas de motivação e de melhor contextualização e complemento da aprendizagem de matemática.

A interação entre as duas disciplinas é inevitável. Os maiores e mais relevantes métodos criptográficos vistos no capítulo 1, teve a matemática como base. No Ensino Médio Integrado ao curso de Informática, mesmo que a ementa do curso apresente noções básicas de segurança da informação, os professores das disciplinas relacionadas podem planejar suas aulas de forma interdisciplinar, como ressaltado nos PCNs (2000).

Além do mais, os PCNs (2000), expressamente indica que a interdisciplinaridade, pode ser considerada além da mera justaposição de disciplinas e, principalmente na “possibilidade de relacionar as disciplinas em atividades ou projetos de estudo, pesquisa e ação, que a interdisciplinaridade poderá ser uma prática pedagógica e didática adequada aos objetivos do Ensino Médio.” (PCN, 2000, p. 75).

Com isso, o conceito de interdisciplinaridade apesar de ser muito abrangente, poderá partir da simples comunicação de ideias até a integração mais complexas das áreas do conhecimento. É imprescindível entender que “todo conhecimento mantém um diálogo permanente com outros conhecimentos”. (PCN, 2000, p.75). É o que preconiza os Parâmetros Curriculares Nacionais, pois quaisquer formas de interdisciplinaridade possibilitam os alunos um novo olhar para o mesmo objeto sob diferentes perspectivas.

Nesse contexto, acredita-se que os alunos do curso técnico em Informática, familiarizados com a tecnologia da informação e o conceito de criptografia, sintam-se motivados pela interação entre essas teorias e os conteúdos de matemática consolidados pela proposta curricular do curso. Com a interdisciplinaridade, pretende-se provocar a valorização da aplicação matemática aprendida em sala de aula em conhecimentos tão relevantes ao universo das TICs.

No entanto, a criptografia é uma tecnologia que provoca curiosidade para quaisquer pessoas usuárias de redes sociais e tecnologias de modo geral. Com isso, as propostas que serão apresentadas não limita-se apenas a aplicação no ensino médio integrado ao técnico, pois como a grade curricular de matemática é considerado base comum, então os professores da educação básica, mesmo do fundamental, poderá dispor destas propostas, visando contribuir com a aprendizagem de seus alunos através da interação entre a criptografia e a matemática.

Finalmente, "o educador precisa buscar alternativas de dinamizar suas aulas, e principalmente capacitar-se, para que este possa explorar mais e com qualidade os recursos advindos das Tecnologias de Informação e Comunicação (TICs)." (SOUSA, 2011, p. 799). Desse modo, concorda com uma concepção inovadora a muito tempo defendida por D'Ambrósio (1993, p. 37), onde preconiza que "para atingir um ambiente de pesquisa matemática onde a curiosidade e o desafio servem de motivação intrínseca aos alunos, é necessário modificar a dinâmica da sala de aula".

Dessa maneira, o professor poderá enriquecer e planejar suas aulas de forma a estimular os alunos, promover a interação entre a matemática, a tecnologia da informação e comunicação através da criptografia e, espera-se com isso, um novo despertar para o ensino da matemática.

4.4 O uso da Criptografia no Ensino de Matemática

A Criptografia é uma ciência incorporada as Tecnologia de Informação e Comunicação. Além disso é uma temática recorrente quanto trata-se de códigos secretos, segurança da informação, das comunicações, das redes sociais, transações bancárias e comerciais, enfim a tudo que se deseja ter caráter confidencial. Por esse motivo é um objeto que desperta interesse e fascínio às pessoas.

> Dada a crescente demanda por sistemas de comunicação mais rápidos, principalmente com o aumento do tráfego de informações, também aumenta a demanda pela segurança da informação. Basta observar a relevância de tudo isto na vida moderna, por meio, das transações bancárias realizadas de forma online, correspondências via correio eletrônico, acesso as mídias eletrônicas e a proteção de informações pessoais. (PEREIRA, 2015, p. 38)

A proposta inicial é abordar os conceitos básicos de Criptografia e elencar alguns fatos históricos relevantes no processo evolutivo, visando melhores formas e inspirações para o ensino de Matemática. Por meio desta contextualização espera-se que os alunos compreendam a importância do tema e crie expectativas quanto a sua aplicabilidade, favorecendo o processo de ensino aprendizagem.

D'Ambrósio (1993), defende que ao ensinar matemática, o professor deve ter consciência que o conteúdo precisar ser útil ao aluno, assim cabe ao educador ajudá-los a compreender melhor a realidade em que pertencem para melhor aplicar e aproveitar esta concepção. Ainda reforça, que a matemática é uma disciplina dinâmica, envolvendo espaços de criatividade e emoção, por esse motivo, os alunos em particular e a sociedade de modo geral, precisam legitimar essa ideia.

> Aprender Matemática de uma forma contextualizada, integrada e relacionada a outros conhecimentos traz em si o desenvolvimento de competências e habilidades que são essencialmente formadoras, à medida que instrumentalizam e estruturam o pensamento do aluno, capacitando-o para compreender e interpretar situações, para se apropriar de linguagens específicas, argumentar, analisar e avaliar, tirar conclusões próprias, tomar decisões, generalizar e para muitas outras ações necessárias à sua formação. (PCN+, 2000, p.111).

Nesta etapa introdutória, a criptografia é uma ciência produtiva à interdisciplinaridade contemplando as áreas de códigos e linguagens, bem como as ciências humanas. Assim a história da criptografia além de fornecer aos alunos uma visão geral de todo o processo de evolução da temática, inevitavelmente, ensina vários fatos relevantes que marcaram a história da humanidade. Conforme os PCNs (2000), a proposta curricular contempla todos os segmentos, ou seja, a interdisciplinaridade vai além de linguagens e códigos, alcançando também, às ciências humanas e exatas. Expressa:

> Em nossa sociedade, o conhecimento matemático é necessário em uma grande diversidade de situações, como apoio a outras áreas do conhecimento, como instrumento para lidar com situações da vida cotidiana ou, ainda, como forma de desenvolver habilidades de pensamento. (PCN, 2000, p. 111).

Em decorrência dos objetivos desta dissertação é imprescindível ressaltar que a criptografia além de fornecer um material de grande abordagem matemática para o ensino médio nos mais diversos níveis de aprendizagem, ainda contribui para o desenvolvimento de fundamentos básicos da computação, tais como o desenvolvimento de algoritmos, mesmo de forma simples, em plataformas computacionais. Considerando os fatos históricos, os alunos entenderiam que a matemática contribuiu para a origem dos computadores.

> Quando o aluno estuda técnicas para criptografar mensagens, palavras, frases ou textos através de permutações, funções, matrizes, entre outros, ele visualiza situações reais e consegue chegar mais facilmente a um resultado, além de estimular a aprendizagem, a utilização da criptografia também é um meio de concretizar esses saberes. (GANASSOLI, 2015, p. 23).

Essa linha de raciocínio, complementa-se quando “uma abordagem dos tópicos matemáticos deve contemplar desde os aspectos históricos, fundamentação teórica e aplicação prática para que o educando possa conhecer o tema em todas as suas dimensões.” (PEREIRA, 2015, p.13).

Cabe ainda ressaltar que a proposta da aplicação de criptografia no ensino de matemática se dá de forma simples e conceitual, levando em consideração que o surgimento de vários sistemas complexos, como temos hoje, tem como base conteúdos que serão abordados no ensino médio. Logo a seguir, Tamarozzi (2004), propõem aplicações para o ensino de funções e matrizes, no entanto faz as seguintes considerações:

> Os métodos tratados neste trabalho têm apenas caráter instrutivo. Na prática atual tais processos são poucos utilizados pela inconveniência de exigirem trocas prévias de chaves entre os usuários. Portanto, são inviáveis na descrição de transações eletrônicas nas quais um único receptor recebe dados de milhares de emissores, como ocorre em vendas pela Internet, transações bancárias e outras. Mesmo nesses casos mais complexos, a Matemática resolveu a trama, e desta vez, quem diria, o ramo da Teoria dos Números. (TAMAROZZI, 2004, p. 72).

Com isso, o autor esclarece, o que já foi relatado na evolução da história da criptografia. O que não deixa de ser extremamente interessante aos alunos compreender esse processo, sendo a origem dos sistemas mais complexos, que serão abordados na disciplina de informática em Tecnologia da Segurança.

4.5 A Criptografia no Ensino de Funções

Na coleção Explorando o Ensino de Matemática, Tamarozzi (2004), propõe o uso da criptografia para enfatizar e estimular o aprendizado de Funções e Matrizes, conteúdos presentes no Núcleo Comum, disciplina de Matemática, nos 1º e 2º anos.

De acordo com o autor, a criptografia desde a antiguidade, contínua com o mesmo princípio básico: “encontrar uma transformação (função) injetiva *f* entre um conjunto de mensagens escritas em um determinado alfabeto (de letras, números ou outros símbolos) para um conjunto de mensagens codificadas.” (TAMAROZZI, 2004, p.69).

Considerando que o conteúdo de funções é um conhecimento previamente adquirido pelos alunos e, partindo dessa premissa, o professor ao utilizar o emprego de criptografia com abordagem em funções, pretende fixar os conceitos, apresentar uma aplicação para a matemática, bem como estimular a curiosidade, ressignificando a importância em estudar funções. Contudo, cabe ressaltar algumas definições, de Lima (2013), que são requisitos básicos de funções para aplicação da criptografia:

> **Funções**: Dados os conjuntos X, Y, uma *função* $f: X \to Y$(lê-se ‘uma função de X em Y’) é uma regra (ou conjunto de instruções) que diz como associar a cada elemento $x \epsilon X$ um elemento $y = f(x) \epsilon Y$ (leia-se ‘y igual a *f* de x’). O conjunto X chama-se o *domínio* e Y é o *contra-domínio* da função *f*. Para cada $x \epsilon X$, o elemento $f(x) \epsilon Y$, chama-se a imagem de x pela função *f*, ou o valor assumido pela função *f* no ponto $x \epsilon X$. Escreve-se $x \mapsto f(x)$ para indicar que *f* transforma (ou leva) x em $f(x)$. (LIMA, 2013, p. 40).
>
> **Função Injetiva**: Uma função $f: X \to Y$ chama-se *injetiva* quando elementos diferentes em X são transformados por *f* em elementos diferentes em Y. Ou seja, f é injetiva quando
> $x \neq x'$ em $X \implies f(x) \neq f(x')$. (LIMA, 2013, p. 41).
>
> **Função Inversa**: Diz-se que a função $g: Y \to X$ é a inversa da função $f: X \to Y$ quando se tem $g\big(f(x)\big) = x$ e $f\big(g(x)\big) = y$ para quaisquer $x \epsilon X$ e $y \epsilon Y$. Evidentemente, g é inversa de f se, e somente se, f é inversa de g. (LIMA, 2013, p.188).

Estas definições são amplamente estudadas no 1ª ano do ensino médio, onde a função inversa recebe a simbologia de f^{-1}. Pois, “o fato de *f* ser invertível é a garantia de o processo ser reversível e as mensagens poderem ser reveladas pelos receptores.” (TAMAROZZI, 2004, p. 69). Esse é um método criptográfico por simétrica, ou seja, aquele que necessita de uma chave secreta entre emissor (para codificar) e

receptor (para decodificar). A chave em questão será a função invertível escolhida adequadamente. Assim a tabela 4 esquematiza o percurso da mensagem.

tabela 4 - Processo de conversão da mensagem

	Emissor		Receptor	
Mensagem original	$\xrightarrow{f}$	Mensagem codificada	$\xrightarrow{f^{-1}}$	Mensagem original

Fonte: Adaptado pelo autor da Coleção Explorando o Ensino de Matemática

A partir do método criptográfico a ser proposto por Tamarozzi (2004), envolvendo funções, o professor poderá dispor, inclusive, para o ensino fundamental, uma vez que os alunos iniciam a compreensão das noções básicas de funções, na última ano do ensino fundamental. Dessa forma, aprendendo a criptografar o aluno figura um novo significado ao conteúdo estudado, satisfaz a curiosidade sistêmica e observa uma das inúmeras aplicações de funções.

Inicialmente, o alfabeto será associado a números, em que o valor do número 0 será representado por um símbolo qualquer, por exemplo (#), para indicar os espaços entre as palavras que ocorrem em uma frase, conforme a tabela 5.

Tabela 5 – Conversão de letras em sequência numérica

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

Fonte: Adaptado pelo autor de Coleção Explorando o ensino Matemática

O processo seguinte, será dado pela escolha de uma função invertível e uma mensagem a ser cifrada. Escolhe-se uma função, por exemplo do 1º grau, denominada de função Afim, que apresenta a seguinte forma $f(x) = ax + b$, em que $a, b \in \mathbb{Z}$, sendo $a \neq 0$, definidas no conjunto $\{0, 1, 2, 3, \dots, 26\}$.

Suponha que Olivia e Maitê queiram trocar mensagens e, secretamente, escolhem a seguinte função $f(x) = 2x - 1$, para cifrar a mensagem:

A MATEMÁTICA ESTÁ EM TUDO

Olivia usa a tabela 5 como base e associa a frase a seguinte sequência numérica, o que resulta em:

1 0 13 1 20 5 13 1 20 9 3 1 0 5 19 20 1 0 5 13 0 20 21 4 15

No entanto, transmite a Maitê a sequência numérica obtida pelas imagens de *f,* ou seja,

$$f(1) = 2(1) - 1 = 2 - 1 = 1;$$
$$f(0) = 2(0) - 1 = 0 - 1 = -1;$$
$$\vdots \qquad\qquad \vdots$$
$$f(15) = 2(15) - 1 = 30 - 1 = 29$$

Obtém-se a sequência:

1 -1 25 1 39 9 25 1 39 17 5 1 -1 9 37 39 1 -1 9 25 -1 39 41 7 29

Ao receber esta sequência numérica, Maitê de posse da chave secreta, precisa encontrar a inversa da função escolhida afim de reverter o processo, aplicando à função aos valores numéricos que foram enviados. Assim calculando o inverso da função original, tem-se:

$f(x) = 2x - 1 \rightarrow x = 2y - 1 \rightarrow x + 1 = 2y \rightarrow y = \frac{x+1}{2} = f^{-1}(x)$, logo;

$f^{-1}(x) = \frac{x+1}{2}$, substituindo pelos valores numéricos criptografados, têm-se:

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

$f^{-1}(-1) = \frac{-1+1}{2} = \frac{0}{2} = 0;$

$f^{-1}(25) = \frac{25+1}{2} = \frac{26}{2} = 13;$

$\vdots \qquad\qquad \vdots$

$f^{-1}(29) = \frac{29+1}{2} = \frac{30}{2} = 15;$

Note que esse processo, garante que a operação seja revertida, voltando assim aos números originais, os quais Maitê, utilizará a tabela para converter os números em letras e assim, decodificar a mensagem.

Quanto a aplicação da criptografia no ensino de funções, Tamarozzi (2004), apresenta algumas sugestões para atividades relacionadas a este conteúdo.

> Depois de os alunos dominarem o processo, seria oportuno que o professor propusesse situações em que um intruso tente decifrar mensagens apoderando-se das sequências numéricas codificadas. Como estamos utilizando funções afins, para tanto é suficiente apenas duas associações corretas entre números das sequências original e codificada. Admitindo conhecidas essas associações, é um exercício interessante para os alunos determinarem *f.* (TAMAROZZI, 2004, p. 71).

Com essas considerações, o aluno pode entender as noções básicas do papel da criptoanálise e uma nova forma de aprender, usando a matemática, intuição e raciocínio lógico para quebrar o código.

Cabe ao professor, estimular esse processo de investigação nos alunos em desvendar a chave secreta. E ainda, com autonomia, escolher dentre vários tipos de funções estudadas conforme o conteúdo programático, podendo até mesmo desenvolver um projeto de ensino que percorra ao longo do ano letivo, adaptando as aplicações conforme os tipos de funções estudadas, como a Função Afim aqui apresentada, Função Quadrática, Função Exponencial, entre outras, levando em consideração a condição de que a função escolhida seja invertível.

4.6 A Criptografia no Ensino de Matrizes

Este método, também sugerido por Tamarozzi (2004), está relacionado ao conteúdo de matrizes, inserida na ementa curricular do 2ª ano do ensino médio. Apesar de usar o mesmo sistema de codificação, ou seja, aquele que assegura que a matriz possua uma inversa e o processo possa ser revertido, ele é considerado mais seguro comparado à função.

Algumas definições básicas de matrizes serão apresentadas, pois são essenciais ao desenvolvimento do método criptográfico utilizado:

> **Definição**
> Sejam m e n números naturais não nulos.
> Uma matriz do tipo m x n é uma tabela de $m.n$ números dispostos em m linhas (filas horizontais) e n colunas (filas verticais).
> Representamos usualmente uma matriz colocando seus elementos (números) entre parênteses ou entre colchetes [...].
> Representaremos uma matriz A do tipo m x n por $A = (a_{ij})_{mxn}$, em que $1 \leq i \leq m$, $1 \leq j \leq n$, e a_{ij} é um elemento qualquer de A. (IEZZI, 2010, p. 80, grifo nosso).
>
> **Matriz Quadrada:** É uma matriz que possui número de linhas igual ao número de colunas.[...] Os elementos de A cujo índice da linha é igual ao índice da coluna constituem a **diagonal principal** de A. Se A é uma matriz

> quadrada de ordem 3, os elementos a_{11}, a_{22} e a_{33}, formam a diagonal principal de A. (IEZZI, 2010, p. 82).
>
> Matriz Identidade
> **Definição.** Seja A uma matriz quadrada de ordem *n*. A é denominada **matriz identidade de ordem *n*** (indica-se por I_n) quando os elementos de sua diagonal principal são todos iguais a 1, e os demais elementos são iguais a zero. (IEZZI, 2010, p. 94).
>
> Igualdade de Matrizes
> **Igualdade**. Duas matrizes A e B do mesmo tipo m x n são iguais quando todos os seus elementos correspondentes são iguais, isto é, sendo $A = (a_{ij})_{m \times n}$ e $B = (b_{ij})_{m \times n}$, temos que A = B quando $a_{ij} = b_{ij}$, para todo *i* (i = 1, 2, 3, ..., m) e para todo *j* (j = 1, 2, 3, ..., n). (IEZZI, 2010, p. 84).
>
> Multiplicação de Matrizes
> **Definição.** Dadas as matrizes $A = (a_{ij})_{m \times n}$ e $B = (b_{jk})_{n \times p}$, chama-se produto de A por B, e se indica por A.B, a matriz $C = (c_{ik})_{m \times p}$, em que $c_{ik} = a_{11} . b_{1k} + a_{12} . b_{2k} + a_{13} . b_{3k} + ... + a_{in} . b_{nk}$; para todo $i \in \{1, 2, ..., m\}$ e todo $k \in \{1, 2, 3, ..., p\}$. (IEZZI, 2010, p. 91).
>
> Matriz Inversa
> **Definição.** Seja A uma matriz quadrada de ordem *n*. A matriz A é dita inversível (ou invertível) se existe uma matriz B (quadrada de ordem *n*), tal que:
> **$A . B = B . A = I_n$**
> Neste caso, B é dita **inversa** de A e é indicada por **A^{-1}**. (IEZZI, 2010, p.101).

Após o aprendizado do conteúdo de matrizes pelo aluno, o professor poderá propor a eles atividade para criptografar uma mensagem, usando o conhecimento adquirido de matrizes.

Suponha que Olivia e Maitê desejam realizar a mesma troca de mensagem acima utilizado no subtópico 4.5:

A MATEMÁTICA ESTÁ EM TUDO

Para isso, elas escolhem a matriz $A = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$ para que seja a chave secreta e, assim realizar a troca da mensagem. A seguir, Olivia constrói uma matriz mensagem M, organizando a sequência numérica que representa a conversão das letras do alfabeto original em números, conforme tabela 5 e, associa em ordem de colunas e completa a posição restante com 0, nos casos em que a quantidade da sequência numérica for ímpar, obtém-se:

$$M = \begin{pmatrix} 1 & 13 & 20 & 13 & 20 & 3 & 0 & 19 & 1 & 5 & 0 & 21 & 15 \\ 0 & 1 & 5 & 1 & 9 & 1 & 5 & 20 & 0 & 13 & 20 & 4 & 0 \end{pmatrix}$$

Em seguida codifica-a usando o produto da matriz *A* (chave) pela matriz *M*, formada pela sequência numérica. Note que, como a matriz *A* de ordem 2 é formada

por duas colunas, pela definição, para que haja o produto entre elas é necessário que a matriz *M* seja organizada de forma a ter duas linhas, $M_{2 \times k}$, onde *k* representa o número de colunas, formado pela sequência numérica originada da conversão das letras dada pela tabela 5, completando a matriz, como segue:

$$A.M = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}. \begin{pmatrix} 1 & 13 & 20 & 13 & 20 & 3 & 0 & 19 & 1 & 5 & 0 & 21 & 15 \\ 0 & 1 & 5 & 1 & 9 & 1 & 5 & 20 & 0 & 13 & 20 & 4 & 0 \end{pmatrix},$$

multiplicando cada linha de *A* por cada coluna de *M*, tem-se:

$a_{11} . m_{11} + a_{12} . m_{21} = 3 . 1 + 2 . 0 = 3 + 0 = 3;$

$a_{11} . m_{12} + a_{12} . m_{22} = 3 . 13 + 2 . 1 = 39 + 2 = 41;$

$\vdots \qquad\qquad\qquad\qquad \vdots$

$a_{11} . m_{113} + a_{12} . m_{213} = 3 . 15 + 2 . 0 = 45 + 0 = 45;$

$\vdots \qquad\qquad\qquad\qquad \vdots$

$A_{21} . m_{113} + a_{22} . m_{213} = 1 . 15 + 1 . 0 = 15 + 0 = 15;$

$$A.M = \begin{pmatrix} 3 & 41 & 70 & 41 & 78 & 11 & 10 & 97 & 3 & 41 & 40 & 71 & 45 \\ 1 & 14 & 25 & 14 & 29 & 4 & 5 & 39 & 1 & 18 & 20 & 25 & 15 \end{pmatrix}$$

Assim, Olivia transmite a sequência:

3 1 41 14 70 25 41 14 78 29 11 4 10 5 97 39 3 1 41 18 40 20 71 25 45 15

Ao receber a mensagem, Maitê precisa da matriz inversa de A, para que assim possa reverter o processo.

Usando a definição apresentada por Iezzi (2013), pode-se obter:

$A . A^{-1} = A^{-1}. A = I_n \rightarrow A . A^{-1} = I_n,$ sendo $A = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$, $A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, resultando na seguinte equação matricial:

$\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} . \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$

$\begin{pmatrix} 3a + 2c & 3b + 2d \\ a + c & b + d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, igualando as matrizes tem-se:

$\begin{pmatrix} 3a + 2c = 1 & 3b + 2d = 0 \\ a + c = 0 & b + d = 1 \end{pmatrix}$, resolvendo os sistemas I e II:

I) $\begin{cases} 3a + 2c = 1 \\ a + c = 0 \end{cases} \rightarrow \ a = -c$ subst. na 1ª eq. $\rightarrow \ -3c + 2c = 1 \ \rightarrow \boldsymbol{c = -1}$,

retomando, $a = -(-1) \rightarrow \boldsymbol{a = 1}$

II) $\begin{cases} 3b + 2d = 0 \\ b + d = 1 \end{cases} \rightarrow \ b = -d + 1$ subst.. na 1ª eq. $\rightarrow \ 3(-d + 1) + 2d = 0 \ \rightarrow$

$-3d + 3 + 2d = 0 \rightarrow \ -d = -3 \rightarrow \boldsymbol{d = 3}$ retomando, $\boldsymbol{b = -2}$

Logo, $A^{-1} = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$

Para restaurar a matriz *AM*, Maitê utiliza a chave da matriz inversa encontrada A^{-1} e, em seguida, pode recuperar *M* através da identidade matricial

$$M = A^{-1}(AM)$$

$$M = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} 3 & 41 & 70 & 41 & 78 & 11 & 10 & 97 & 3 & 41 & 40 & 71 & 45 \\ 1 & 14 & 25 & 14 & 29 & 4 & 5 & 39 & 1 & 18 & 20 & 25 & 15 \end{pmatrix}$$

Aplicando o processo de multiplicação entre matrizes novamente, temos:

$$M = \begin{pmatrix} 1 & 13 & 20 & 13 & 20 & 3 & 0 & 19 & 1 & 5 & 0 & 21 & 15 \\ 0 & 1 & 5 & 1 & 9 & 1 & 5 & 20 & 0 & 13 & 20 & 4 & 0 \end{pmatrix}$$

Observe que M, representa a matriz equivalente a sequência original e, com isso, tem-se o processo revertido. Para Maitê ler a mensagem, basta utilizar a tabela para encontrar as letras que correspondem a sequência numérica.

Por fim, é interessante destacar que a aplicação da criptografia no ensino de matrizes, sugere a possibilidade do professor em criar questões envolvendo situações cotidianas que oriente aos alunos a criptografar, assim como em decifrar a mensagem utilizando-se, para isso, do processo exemplificado acima.

4.6.1 Cifra de Hill

A cifra de Hill, segundo descreve Stallings (2015), desenvolvida pelo matemático Lester Hill em 1929, tem como base o conhecimento de matrizes e determinantes, além de explorar a Aritmética Modular, que será visto, mais adiante, em detalhes. A vantagem desta cifra em relação à anterior é proporcionar maior segurança.

O ponto forte da cifra de Hill é que ela oculta completamente as frequências de única letra. De fato, com Hill, o uso de uma matriz maior esconde mais informações de frequência. Assim, uma matriz 3 X 3 encobre não apenas informações de frequência de única letra, mas também de duas letras.

Considerando algumas definições apresentadas anteriormente por Iezzi (2010) para matriz e dada a matriz $A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$, a fim de exemplificar a cifra de Hill, tem-se, inicialmente, neste caso, que aplicar o conceito de determinante para encontrar o Inverso da matriz, para isso apresenta os seguintes conceitos:

> Para qualquer matriz quadrada *(m x n)*, o **determinante** é igual à soma de todos os produtos que podem ser formados apanhando-se exatamente um elemento de cada linha e um de cada coluna com certos termos do produto precedidos por um sinal de menos. Pra uma matriz 2x2,
>
> $$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$
>
> o determinante é $k_{11}.k_{22} - k_{12}.k_{21}$. Para uma matriz 3X3 o valor do determinante é $k_{11}.k_{22}k_{33} + k_{21}.k_{32}k_{13} + k_{31}.k_{12}k_{23} - k_{31}.k_{22}k_{13} - k_{21}.k_{12}k_{33} - k_{11}.k_{32}k_{23}$. Se uma matriz quadrada A tiver um determinante diferente de zero, então o **inverso da matriz** é calculado como $[A^{-1}]_{ij} = (\det A)^{-1}(-1)^{i+j}(D_{ji})$, onde (D_{ji}) é o subdeterminante formado pela exclusão da linha j e coluna i de A, det(A) é o determinante de A e (detA)$^{-1}$ é o inverso multiplicativo de (det A) mod 26. (STALLINGS, 2015, p. 31, gripo nosso).

Logo, se $A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \rightarrow 5.3 - 8.17 = 15 - 136 = -121 \rightarrow detA = -121 \neq 0$,

Expressando -121 pelo algoritmo de Euclides da Aritmética Modular, tem-se:

$$-121 = -4\,x\,26 - 17 \rightarrow -121 \equiv -17 \equiv 9\,mod\,26.$$

Ou seja, a divisão de -121 por 26 (alfabeto com 26 letras), resulta no resto -17 equivalente a 9, pois -17 + 26 = 9.

A criptografia pela Aritmética Modular, será visto com mais detalhes, por enquanto, pode-se notar que este conteúdo está relacionado a valores do Conjunto dos Números Inteiros, simbolizado por $\mathbb{Z}$, também conhecido como a aritmética do relógio, cujos resultados, nestes caso específico, correspondem aos restos da divisão por 26, onde $0 \leq r \leq 25$.

Observe que $(\det A)^{-1} = (9)^{-1} = 3$, pois $9x3 = 27 \equiv 1 mod 26$

Assim o inverso de A será dado por:

$$A^{-1}\,mod\,26 = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3\begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

4.6.2 O Algoritmo de Hill

Para encriptar o texto claro (original), o algoritmo de Hill utiliza *m* letras do alfabeto original e substituí por *m* letras do alfabeto cifrado em forma de equações lineares. Conforme a ordem das letras é atribuído um valor numérico, em que (a = 0, ..., z = 25), de acordo com a tabela 6:

Tabela 6 – Conversão numérica para Cifra de César

a	b	c	d	e	f	G	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	T	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Adaptado pelo autor de Criptografia e Segurança de Redes

Assim obtém-se o seguinte sistema:

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) mod\ 26$$
$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) mod\ 26$$
$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) mod\ 26$$

Estas equações lineares podem ser expressas através de vetores de linha e matrizes:

$$(c_1 \quad c_2 \quad c_3) = (p_1 \quad p_2 \quad p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} mod\ 26$$

Ou $C = PK\ mod\ 26$, onde C e P são vetores de coluna de tamanho 3, representando, respectivamente, o texto claro e o texto cifrado, e K é uma matriz 3X3, indicando a chave de encriptação. As operações são realizadas com mod 26.

Por exemplo, considere que o texto claro **ALGORITMO** é utilizado a chave K para encriptar, onde:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

As letras **ALG** são representadas, de acordo com a sequência numérica da tabela 6 por (0 11 6). Aplicando a equação linear;

$(\ 0 \quad 11 \quad 6\ )$.k = $(0 \quad 11 \quad 6).\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$, aplicando o produto de matrizes, tem-se:

$= (\ 0 + 231 + 12 \quad 0 + 198 + 12 \quad 0 + 231 + 114)$

$= (243 \quad 210 \quad 345\ ).$

Como $243 \equiv 9\ mod\ 26$, $210 \equiv 2\ mod\ 26$ e $345 \equiv 7\ mod\ 26$, então:

$(243\ 210 \quad 345) = (9 \quad 2 \quad 7)$ = **JCH**

Fazendo o mesmo processo para as demais letras, têm-se:

ORI = $(14 \quad 17 \quad 8) = (238 + 357 + 16 \quad 238 + 306 + 16 \quad 70 + 357 + 152\ )$

$= (611 \quad 560 \quad 579) = (13 \quad 14 \quad 7) =$ **NOH**

TMO $= (19 \quad 12 \quad 14) = (323 + 252 + 28 \quad 323 + 216 + 28 \quad 95 + 252 + 266\ )$

$= (603 \quad 567 \quad 613) = (5 \quad 21 \quad 15) =$ **FVP,** assim o texto cifrado será dado por:

JCHNOHFVP

Como visto na Criptografia com aplicação em matrizes por Tamarozzi (2004), também para decriptar o algoritmo de Hill, é necessário aplicar a matriz inversa:

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

cuja demonstração será verificada da seguinte forma:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} mod\ 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Recuperar o texto claro, fica fácil ao aplicar a matriz inversa K^{-1} ao texto cifrado. Em termos gerais, o algoritmo de Hill pode ser expresso pelas fórmulas:

$$C = E(K, P) = PK\ mod\ 26$$

$$P = D(K, C) = CK^{-1} mod\ 26 = PKK^{-1} = P$$

Stallings (2015) define as notações $C = E(K, P)$ e $P = D(K, C)$ da seguinte maneira:

> Com a mensagem X e a chave de encriptação K como entradas, o algoritmo de encriptação produz o texto cifrado Y = [$Y_1, Y_2, ..., Y_n$]. Podemos escrever isso como:
>
> $$Y = E(K, X)$$
>
> Essa notação indica que Y é produzido usando-se o algoritmo de encriptação. E como função do texto claro X, com a função específica determinada pelo valor da chave K.
> O receptor legítimo, de posse da chave, é capaz de inverter a transformação: $X = D(K, Y)$. (STALLINGS, 2015, p. 22).

Adaptando ao exemplo demonstrado pelo autor, pode-se concluir que, de fato, este algoritmo apesar de ser bem mais seguro, também é mais complexo, de forma que o professor, poderá aplicar após os conceitos estudados de aritmética modular e sistemas algébricos. Contudo, a tarefa de cifrar e conseguir reverter o processo, espera-se proporcionar aos alunos satisfação em conseguir se apropriar destes métodos apresentados, além de oferecer mais profundidade ao ensino de matriz.

Como forma de integração interdisciplinar e diante da disciplina de algoritmo pertencente a ementa de informática, o professor pode propor situações práticas e conduzir os alunos a apropriar-se de meios tecnológicos, como o uso de laboratórios para realizar cálculos e construir seus próprios exemplos, por meio de trocas de matrizes chaves, aprimorar o cálculo da matriz inversa, enfim ter contato com todos os elementos que requer o desenvolvimento da cifra de Hill.

Portanto, ao entender a aplicabilidade da matemática neste contexto, bem como perceber que sem ela não seria possível desenvolver este algoritmo, espera-se que os alunos experimentem e sejam estimulados pelos processos matemáticos exigidos por esta técnica criptográfica.

4.7 A Criptografia no Ensino de Análise Combinatória

Os primeiros métodos de criptografia apresentados no primeiro capítulo, conhecidos como criptografia por substituição, passou por um longo processo de evolução, onde buscava-se desenvolver uma cifra com maior segurança, toda vez que a criptoanálise conseguia vencê-la.

Conforme vista, a cifra de César é o mais antigo registro histórico sobre criptografia. Apesar de sua simplicidade, pode-se analisar a matemática que a envolve.

O conteúdo de Análise Combinatória consta na ementa do PPC do 2ª ano do Ensino Médio. Ao estudá-lo, o aluno compreende o universo das possibilidades, arranjos, combinações e permutações. Dante (2005), apresenta as definições para melhor compreensão do estudo de contagem:

> Princípio Fundamental da Contagem – PFC
> Se um evento é composto por duas etapas sucessivas e independentes de tal maneira que o número de possibilidades na primeira etapa é **m** e para cada possibilidade da primeira etapa o número de possibilidades na segunda etapa é **n**, então o número total de possibilidades de o evento ocorrer é dado pelo produto **mn.** (DANTE, 2005, p.284).
>
> Permutação simples e fatorial de um número
> De modo geral, se temos **n** elementos distintos, quantas filas podemos formar? Podemos escolher o primeiro elemento da fila de **n** maneiras. Agora, de quantas maneiras podemos escolher o segundo elemento da fila? De **n-1** maneiras. Prosseguindo dessa forma e usando o princípio multiplicativo, fica claro que o número de agrupamentos ordenados que podemos obter com todos esses **n** elementos é dado por:
> n(n-1)(n-2)...3.2.1
> Esses agrupamentos ordenados (diferem pela ordem) recebem o nome de permutações simples. Indicamos por $\mathbf{P_n}$ o número de permutações simples de **n** elementos:
> $P_n = n(n-1)(n-2)...3.2.1$ (DANTE, 2005, p. 285).
> A permutação de n elementos dos quais $\boldsymbol{\alpha}$ são de um tipo, $\boldsymbol{\beta}$ de outro e $\boldsymbol{\gamma}$ de outro, com $\boldsymbol{\alpha} + \boldsymbol{\beta} + \boldsymbol{\gamma} = \boldsymbol{n}$, é dado por
> $\boldsymbol{P_n^{\alpha,\beta,\gamma}} = \frac{\boldsymbol{n!}}{\boldsymbol{\alpha!\beta!\gamma!}}$ (DANTE, 2005, p. 292).
>
> Combinação
> Combinação simples de **n** elementos tomados **p** a **p** (**p** $\leq$ **n**) são os subconjuntos com exatamente **p** elementos que se podem formar com os **n** elementos dados.
> Indica-se por$\boldsymbol{C_{n,p}}$, $\boldsymbol{C_n^p}$ ou $\binom{\boldsymbol{n}}{\boldsymbol{p}}$ o número total de combinações de **n** elementos tomados **p** a **p** e calcula-se por
> $\boldsymbol{C_{n,p}} = \frac{\boldsymbol{n!}}{\boldsymbol{p!(n-p)!}}$ (DANTE, 2005, p. 290).

4.7.1 A Cifra de César

A análise combinatória possui ampla possibilidade de explorar os primeiros métodos criptográficos. Um deles é a cifra de *César*, considerado o "uso mais antigo que conhecemos de uma cifra de substituição, e o mais simples, foi feito por Júlio César. A cifra de César envolve substituir cada letra do alfabeto por aquela que fica três posições adiante". (STALLINGS, 2015, p. 25). Por essa simplicidade, vale a pena iniciar tanto a parte histórica quanto a parte matemática envolvida no código secreto.

Com base nos estudos de contagem e do número de possibilidades, a matemática embutida no método de César, pode ser uma rica experiência para ter

uma dimensão do número de possibilidades existentes nesta cifra, assim como estimular os alunos a criarem seus próprios métodos.

Na cifra de César, como ressaltou Stallings (2015), as substituições ocorrem a partir do alfabeto original representados por letras minúsculas, dando origem ao alfabeto cifrado, da seguinte forma:

Tabela 7 – Conversão para a cifra de César

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	w	y	z
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: Adaptado pelo autor

Para cifrar a frase: **CIFRA DE CESAR**, obtém-se:

FLIUD GH FHVDU

Considerando que as letras aparecem de forma ordenada, vale ressaltar que mesmo sendo criado novas regras de substituição, torna-se relevante perceber que o alfabeto original já é uma possibilidade, da qual não será utilizada, pois não faria sentido codificar. Assim, qualquer outra substituição, respeitando a ordem alfabética, forneceria mais 25 possibilidades, ou seja, para fixar a substituição da letra **a**, haveria 25 possibilidades, uma vez que não seria usado a própria letra. As demais letras viriam na sequência.

Por outro lado, desordenadamente, pode-se obter quaisquer formas de arranjos, excluindo o alfabeto original. Ou seja, para substituir o **a**, têm-se 26 possibilidades, para substituir o **b**, têm-se 25 possibilidades e assim por diante, até substituir a letra **z**, da qual resultaria uma possibilidade. Matematicamente, a ideia empregada nesta contagem trata-se do Princípio Multiplicativo ou a Permutação das letras. Assim, o resultado é determinado pela seguinte Permutação:

$P_{26} = 26! - 1$ O que equivale a

$= (26.25.24.23....3.2.1) -1$

$= 403.291.461.126.605.635.584.000.000 – 1$

$= 403.291.461.126.605.635.583.999.999$

$= 4,032914611266056355839999999 \times 10^{26}$

Stallings (2015) apresenta uma técnica de encriptação para a cifra de César, em que atribui a cada letra um valor equivalente numérico, de acordo com a tabela 6.

Essa técnica consiste em representar as letras do alfabeto por *p* e as letras do texto cifrado por *C*, expressas pelo seguinte algoritmo:

$$C = E\ (3, p) = (p + 3) mod 26$$

Considerando que o deslocamento pode ser feito de qualquer magnitude, a fórmula geral é dada por:

$$C = E\ (k, p) = (p + k) mod 26$$

"onde *k* assume um valor no intervalo de 1 a 25. O algoritmo de decriptação é simplesmente $p = D\ (k, C) = (C - k) mod 26$." (STALLINGS, 2015, p. 26).

Essa fórmula encontra-se no contexto da aritmética modular, que será abordada ainda neste capítulo. Contudo o autor define que $a\ mod\ n$ é o resto da divisão de *a* por *n.*

Tomando o mesmo exemplo acima **MATEMÁTICA É DIVERTIDA** e considerando k = 42, de acordo com a tabela 6, a frase terá a sequência numérica:

12 0 19 4 12 0 19 8 2 0 4 3 8 21 4 17 19 8 3 0

$$C = E\ (3, p) = (p + 42) mod 26$$
$$C = (12 + 42) mod 26$$
$$C = 54\ mod 26$$
$$C = 2\ mod 26$$
$$C = E\ (3{,}32) = (0 + 42) mod 26$$
$$C = (42) mod 26$$
$$C = 16\ mod 26$$
$$C = E\ (3{,}32) = (19 + 42) mod 26$$
$$C = (61) mod 26$$
$$C = 9 mod 26$$
$$\vdots$$

Então a sequência numérica que representa o texto criptografado é dada por:

2 16 9 20 2 16 9 24 18 16 20 19 24 11 20 7 0 9 19 16

Para reverter o processo, basta utilizar a seguinte fórmula:

$$p = D\ (42{,}2) = (2 - 42) mod 26$$
$$p = (-40) mod 26$$
$$p = (-14) mod 26$$
$$p = 12\ mod 26$$

Observe que o resto -14 equivale a 12, pois -14 + 26 = 12, ou seja o resultado do texto original que corresponde a letra do alfabeto M.

A aritmética modular, apesar de explicitamente não ser estudada no ensino Médio, em muitos conteúdos abordados estão presentes a ideia intuitiva dela. Por exemplo, no 2º ano, o estudo de ângulos na Circunferência Trigonométrica é indispensável esta noção, pois no círculo trigonométrico, os alunos precisam saber o valor que corresponde um ângulo de 2220°. Nesse caso, é imprescindível o conceito de aritmética modular.

Considere α um ângulo equivalente, então pela aritmética modular, tem-se;

$\alpha \equiv 2220\ mod\ 360 \rightarrow \alpha \equiv 60\ mod\ 360$, ou seja $\alpha = 60°$.

Vale ressaltar que na prática obtém-se o resto da divisão de 2220 por 360 o que equivale a 60.

No que se refere ainda a cifra de Cesar, segundo Singh (2014), essa técnica é classificada como monoalfabética, por substitui letras do alfabeto original por outras letras, inclusive, por símbolos, uma vez determinada o algoritmo, emissor e receptor precisam conhecer e ter secreto a chave de cifragem.

No entanto, apesar de ser um processo simples, combinar a chave poderia ser bem mais complexo, assim o autor destaca uma versão do método de César que foi amplamente utilizada pelos criptógrafos, pois além de ser considerada segura, a troca de chaves era bem mais acessível.

A proposta consiste em escolher uma palavra-chave ou frase-chave, por exemplo, TEORIA DOS NÚMEROS. Para encontrar o alfabeto criptografado, desconsidera-se os espaços e as repetições de letras e obtém-se a palavra-chave TEORIADSNUM. Na sequência, essa será aplicada ao início do alfabeto criptografado, completando-o com as letras do alfabeto que são sequências da palavra-chave, sem repetições. Assim, o alfabeto original representado na primeira linha, resulta no alfabeto criptografado, conforme a exibido na segunda linha.

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

Por exemplo, para cifrar a frase **MATEMÁTICA É DIVERTIDA**, obtém-se a cifra:

QTCIQTCNOTIRNGIZCNRT

4.7.2 Cifra Playfair

O uso de uma palavra ou frase-chave neste método criptográfico é identificado por Stallings (2015) na *Cifra Playfair*. Este é baseado no uso de uma matriz de ordem 5, ou seja, 5X5, onde a palavra-chave escolhida preenche a matriz na ordem da esquerda para a direita e de cima para baixo, com as letras I e J juntas. Veja como seria a configuração para decifrar a frase **MATEMÁTICA É DIVERTIDA,** aplicando na tabela 8, utilizando a mesma frase chave **TEORIADSNUM**, originada de TEORIA DOS NÚMEROS, têm-se:

Tabela 8 – Cifra de Playfair

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

Fonte: Adaptado pelo Autor de Criptografia e segurança de Redes

No entanto, a cifra de Playfair é bem mais complexa, pois possui regras de encriptação própria, onde o texto original, denominado de texto claro, organizado em pares de duas letras de cada vez, são definidas pelas regras:

i. As letras repetidas em um par são separadas por uma letra de preenchimento como a letra X, ou seja, para cifrar CARRO, equivale a cifrar CA RX RO;
ii. Duas letras que pertencem a mesma linha, de forma rotativa, serão substituídas pelas letras à direita, onde a última da linha equivale a primeira letra da linha, por exemplo: NU será cifrado como UA;
iii. Duas letras que pertencem a mesma coluna, de forma rotativa, terá a primeira letra substituída pela letra seguinte abaixo, sendo o primeiro elemento da coluna a sequência do último. Por exemplo: a cifra de TF equivale a AT;
iv. Se nenhuma das duas condições anteriores ocorrerem, considerando os pares de letras claro como extremidades de uma diagonal, elas serão cifradas pela

extremidade da diagonal contrária. Assim, DK equivale a cifra NG, OC equivale a cifra IZ ou JZ.

Essa Cifra monoalfabética foi um avanço para época, pois foi utilizada e considerada, “como sistema de campo padrão pelo Exército britânico na Primeira Guerra Mundial, e ainda gozava de um uso considerável pelo Exército dos Estados Unidos e outras forças aliadas durante a Segunda Guerra Mundial.” (STALLINGS, 2015, p. 30).

Este método apresenta uma proposta interessante, pois o professor no conteúdo de matrizes e análise, poderá instigar os alunos a criarem suas próprias regras para cifrar textos utilizando-se de uma palavra chave.

4.7.3 O quadrado de Vigenère

O quadrado de Vigenère é a versão mais complexa deste método, pois ao escolher uma palavra ou frase-chave, pode-se utilizar vários alfabetos para cifrar a mensagem original. De fato, a segurança desse método se deve a esta particularidade.

Cabe recordar, que este foi o método aplicado para iniciar a introdução deste trabalho, contudo vale destacar que as palavras-chaves utilizadas para cifrar o título foram: DISSERTAÇÃO-MESTRADO-PROFMAT, cuja ordem da chave, sem repetição das letras, foi dada por **DISERTACOMPF**, utilizando-se assim, 12 distintos alfabetos criptografados.

Como exemplo, vamos criptografar a frase **A ARTE DA ESCRITA SECRETA**, usando a palavra-chave **MATEMÁTICA**.

Inicialmente, desconsiderando as letras repetidas da palavra-chave MATEMÁTICA, obtêm-se MATEIC. A seguir, aplica-se na tabela para melhor visualizar qual será o alfabeto cifrado que correspondem as letras de MATEIC, assim;

Palavra chave	**M**	**A**	**T**	**E**	**I**	**C**	**M**	**A**	**T**	**E**	**I**	**C**	**M**	**A**	**T**	**E**	**I**	**C**	**M**	**A**	**T**
Texto Original	**A**	**A**	**R**	**T**	**E**	**D**	**A**	**E**	**S**	**C**	**R**	**I**	**T**	**A**	**S**	**E**	**C**	**R**	**E**	**T**	**A**
Texto criptografado	**M**	**A**	**K**	**X**	**M**	**F**	**M**	**E**	**L**	**G**	**Z**	**K**	**F**	**A**	**L**	**I**	**K**	**T**	**Q**	**T**	**T**

Note que, para poder empregar o alfabeto criptografado de acordo com a palavra-chave, utiliza-se a tabela 2, o quadrado de Vigenère apresentado no capítulo 1.

A seguir, para cifrar a primeira letra do texto original, **A,** usa-se o alfabeto da linha 12 que corresponde a letra **M** da palavra-chave. O resultado será a intersecção da coluna da letra **A** do alfabeto original com a linha da letra **M**, cujo resultado também é **M**. A próxima letra **A**, usa-se a linha 26 que corresponde a letra **A** da palavra-chave resultando também na letra **A**. A letra **R** do texto original, equivale a letra **K** do texto cifrado, também resultado da interseção da coluna **R** do alfabeto original com a linha 19 que corresponde a letra **T** da palavra-chave e assim por diante. Note que para cifrar todas as letras **E** do texto original, foram usados, respectivamente, **I (**linha 8)**, A** (linha 26), **E** (Linha 4) e o **M** (linha 12), ou seja, quatro alfabetos criptografados.

Logo, o texto criptografado será transmitido da seguinte forma:

MAKXMFMELGZKFALIKTQTT

Desse modo, para criptografar toda a mensagem, a partir da palavra-chave MATEIC, utilizou-se 6 alfabetos criptografados, por esse motivo decorre a dificuldade de se aplicar a análise de frequência, o que tornou o método absolutamente seguro por alguns séculos, pois uma mesma letra pode ser representada por várias letras diferentes, provocando uma grande confusão para o decifrador de códigos.

Portanto, ao aplicar a criptografia no ensino de análise combinatória, os alunos, além de ter a oportunidade de lidar com as coordenadas, ainda poderão escolher suas próprias palavras chaves, enviar mensagens cifradas e, com isso, calcular o número de possibilidades a partir da escolha da palavra chave. Dessa maneira, pode-se observar que mesmo reduzindo a quantidade de possibilidades, ainda assim geram inúmeras possibilidades garantindo a segurança do processo.

4.7.4 Seleção didática para o conteúdo de Análise Combinatória

O conteúdo de Análise Combinatória já é considerado propício à aplicação, assim ao relacionar à criptografia, torna-se a prática mais produtiva. Portanto, o professor poderá explorar a criptografia para enriquecer a aprendizagem deste conteúdo em sala de aula e tornar mais interessante e atrativo a compreensão deles.

As sugestões que seguem, orienta-se a agrupar os alunos. Dessa forma, o professor poderá escolher uma frase para que os alunos combinem entre eles uma chave e com ela codifiquem a mensagem, podendo dessa forma seguir as seguintes propostas;

i. **Criptografar** a mensagem a seguir utilizando a chave dada com base na permutação.

   Mensagem original**: ESTUDAR PARA A AVALIAÇÃO**

   Chave: separar a frase em bloco de três letras nesta ordem. Trocar a 1ª e a 3ª letra de cada bloco.

   EST UDA RPA RAA AVA LIA ÇÃO

   TSE ADU APR AAR AVA AIL OÃÇ

   Mensagem cifrada: **TSEADUAPRAARAVAAILOÃÇ**

Primeiro, espera-se que os alunos realizem a contagem da quantidade de letras contidas na frase, neste caso são 21 letras e verifiquem se ao agrupar as letras, esse número será divisível pelo valor escolhido, ou seja, 21 é divisível por 3, logo tem-se exatamente 7 grupos com 3 letras. E em segundo, os alunos vão criar suas próprias chaves. Para isso, a dica é explorar o conteúdo de permutação e perceber que um agrupamento maior haverá mais opções, assim o processo além de ficar mais complexo, aumenta a segurança do código. Também a outras possibilidades, como a permutação entre os blocos.

ii. A prática pode ser invertida. O professor poderá criar um situação-problema e entregar a mensagem criptografada para que os alunos consigam decifrá-la. Assim os alunos compreenderão melhor o significado da criptoanálise, sendo um grande estímulo para o desenvolvimento do raciocínio lógico, bem como descobrir qual foi a permutação aplicada a mensagem, ou seja, encontrar a chave.

iii. A proposta para essa atividade é apresentar aos alunos uma mensagem cifrada e orientá-los para que decifrem utilizando a cifra de César.

iv. A partir da ideia da cifra de Cesar, propor aos alunos que cifrem uma frase criando sua própria cifra, ou ainda aplicar a fórmula $C = E\,(k, p) = (p + k) mod 26$, utilizada no subtópico 4.7.1.

v. Outra sugestão relacionada a este tópico é propor aos alunos que confeccione o disco de cifras, conforme fig. 2, do capítulo 1 e utilize-o para criptografar.

A cifra polialfabética de Vigenère é uma interessante abordagem para que os alunos compreendam a importância dela em termos de segurança para a época. Assim, os alunos poderão através do quadrado de Vigenère, cifrar mensagens e aplicar os conceitos de coordenadas ao encontrar e substituir letras, pois é com base nessas coordenadas que compreenderão a complexidade do quadrado, composto de 25 alfabetos criptografados por meio da cifra de Cesar.

vi. A atividade a seguir, é proposta por Pereira (2015):

> Com a palavra-chave CÓDIGO, cifre o verso abaixo de Memória Carlos Drummond de Andrade) pelo quadro de Vigenère.
>
> "Mas as coisas findas
> muito mais que lindas,
> essas ficarão."
>
> Chave: CÓDIGO, que em números é 03-15-04-09-07-15, de acordo com ordem no alfabeto.
> Processo: Completar a tabela abaixo seguindo coordenadas na tabela 2.

3 M	15 A	4 S	9 A	7 S	15 C	3 O	15 I	4 S	9 A	7 S	15 F	3 I	15 N	4 D	9 A
P	**P**	**W**	**J**	**Z**	**R**	**R**	**X**	**W**	**J**	**Z**	**U**	**L**	**C**	**H**	**J**
7 S	15 M	3 U	15 I	4 T	9 O	7 M	15 A	3 I	15 S	4 Q	9 U	7 E	15 L	3 I	15 N
Z	**B**	**X**	**X**	**X**	**X**	**T**	**P**	**L**	**H**	**U**	**D**	**L**	**A**	**L**	**C**
4 D	9 A	7 S	15 E	3 S	15 S	4 A	9 S	7 F	15 I	3 C	15 A	4 R	9 A	7 O	
H	**J**	**Z**	**T**	**V**	**H**	**E**	**B**	**M**	**X**	**F**	**P**	**V**	**J**	**V**	

> Verso cifrado:
>
> **PPW JZ RRXWJZ ULCHJZ**
> **RXXXX TPLH UDL ALCHJZ,**
> **TVHEB MXFPVJV**
>
> (PEREIRA, 2015, p.33).

Com este exemplo, o professor poderá se inspirar em criar versões para que os alunos realizem a cifragem utilizando do quadrado de Vigenère e, mais importante ainda, perceba a complexidade de aplicar vários alfabetos criptografados em uma única mensagem, impossibilitando a análise de frequência.

4.8 A Criptoanálise no Ensino de Porcentagem e Raciocínio Lógico

Os árabes inventaram a *criptoanálise* definida como a "ciência que permite decifrar uma mensagem sem conhecer a chave. [...] é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar mensagem secreta"

(SINGH, 2014, p. 32). Esta técnica pode ser considerada bem mais desafiadora, pois ao longo da história, observou-se que a aplicação desta ciência sempre estava relacionada a desvendar o segredo envolvido no processo criptográfico.

Por isso, analisar uma cifra e tentar quebrá-la exige muito raciocínio lógico, organização, conhecimentos matemáticos, noções de estatística e linguística, como visto nos relatos históricos apresentado no capítulo 1.

Enfim, decifrar é uma arte e os árabes ao estudar as cifras monoalfabéticas conseguiram decifrar um texto criptografado pela análise de frequência, uma técnica que consiste no estudo da ocorrência das letras e envolve, além de conhecimento da língua, o conteúdo de porcentagem e noções de contagem, estatística e probabilidade.

Para decifrar uma mensagem criptografada pelo método de substituição monoalfabético, Stallings (2015), sugere a análise de frequência, considerando o percentual de ocorrência de cada letra do alfabeto relativo ao idioma a ser descriptografado.

No caso da língua portuguesa, a análise é realizada pela tabela 1, apresentada no capítulo 1, observando as considerações de Coltinho (2014). Dessa forma, o conhecimento do comportamento característico das letras, conforme propõe Coltinho (2014), poderá auxiliar na composição da mensagem original.

A proposta inicial é apresentar um texto criptografado para que de posse da tabela 1 o aluno possa comparar. Para isso, precisará criar uma tabela para a frequência do texto criptografado. Uma vez criada e convertida em porcentagem, poderá realizar a comparação e assim, utilizando-se de raciocínio lógico e conhecimento da língua portuguesa, poderá ir trilhando o caminho do texto original.

Uma outra forma de explorar o assunto é dar oportunidade aos alunos para que eles possam, em grupo, construir suas próprias tabelas a partir de um texto, relativamente longo, em que sejam contadas o número de ocorrência de todas as letras e convertidas em porcentagem.

Dessa forma, os alunos, conforme os relatos históricos, terão uma noção de como se dava as quebras dos códigos.

4.9 A Criptografia no Ensino de números Binários

Com o advento dos computadores, no período pós-guerra, os criptógrafos evoluíram consideravelmente em relação as máquinas mecânicas, como por exemplo, a Enigma.

Este avanço, segundo Singh (2014), deve-se a três importantes distinções entre os computadores e as máquinas mecanizadas. A primeira diferença, destaca-se pela limitação, pois esta última, não poderia ser programada para executar operações complexas como um computador, ou seja, executar ações programadas e com variações a depender de uma condição dada. A segunda, está relacionada ao ganho de velocidade, pois é incomparável o avanço em processamento de cifragem no menor tempo possível. E a terceira vantagem está associada a linguagem dos computadores, pois utilizam apenas números binários.

> Os computadores lidam apenas com números binários seqüências de um e zero conhecidas como *digitos binários*, ou, abreviadamente, *bits* (de *binary digits*, em inglês). Esta conversão pode ser realizada de acordo com vários protocolos, tais como o American Standard Code for Information Interchange (Código Padrão Americano para Troca de Informações), conhecido pela sigla ASCII. (SINGH, 2014, p. 269).

Esse sistema de base 2 ou números binários equivalente a unidade bits, isto é, “a menor unidade de informação que pode ser armazenada ou transmitida, podendo assumir dois valores: 0 ou 1. O computador é projetado para armazenar instruções em múltiplos de bit.” (GANASSOLI, 2015, p. 19).

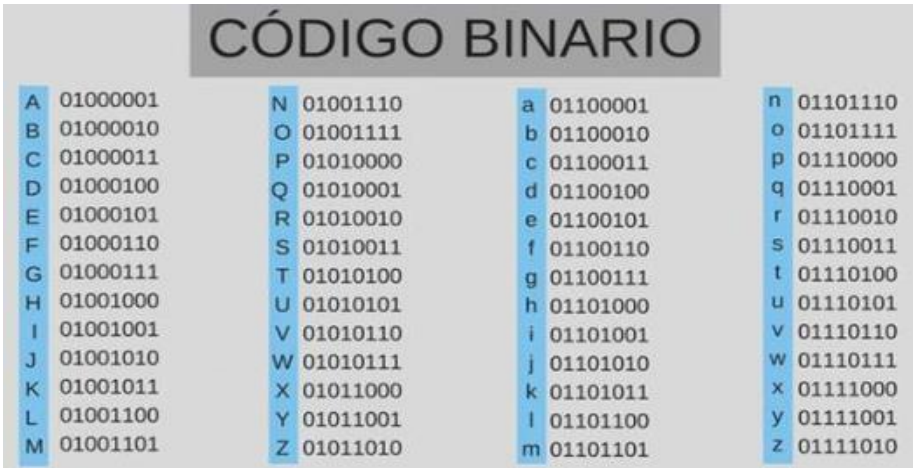
Esse processo se dá por meio do protocolo ASCII, onde cada letra, número e símbolos são representados por uma sequência de 8 dígitos, o que remete ao conceito de permutação, visto que para formar uma sequência de 8 dígitos de zero e um, para cada posição, tem-se duas possibilidades, o que resulta em $2x2x2x2x2x2x2x2 = 2^8 = 256$. Por exemplo, conforme a tabela 9, a letra **a** minúscula é representada por 01100001.

O Estudo de criptografia moderna está vinculada ao uso do computador, nesse sentido é de vital importância entender a linguagem binária e conhecer o sistema de numeração posicional de base 2, ou seja, a linguagem computacional.

Na mesma linha, Pereira (2015), observa que a apresentação do sistema binário aos alunos é importante pelo fato de poder rever conteúdos matemáticos, tais

como; o estudo dos restos, numeração decimal, entre outros conceitos que podem ser compreendidos melhores explorando a linguagem computacional.

Tabela 9 – Código Binário ASCII de 8 bits para Letras maiúsculas e minúsculas

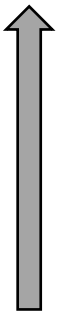


Fonte: Adaptado de Cálculo exato.net[7]

Por exemplo, a conversão do número decimal 217 em um número binário se dá pelo processo de divisões sucessivas por 2, ou simplesmente pode-se representar estas divisões pelo algoritmo de Euclides.

Assim:

$$217 = 2\,x\,108 + 1$$
$$108 = 2\,x\,54 + 0$$
$$54 = 2\,x\,27 + 0$$
$$27 = 2\,x\,13 + 1$$
$$13 = 2\,x\,6 + 1$$
$$6 = 2\,x\,3 + 0$$
$$3 = 2\,x\,1 + 1$$
$$1 = 2\,x\,0 + 1$$



Portanto, o número decimal 217 é representado por todos os restos, a começar pelo último encontrado. Logo:

$$217 = 11011001$$

[7] CÁLCULO EXATO. NET. **Código Binário: Conversor e números binários**. 2020, p.1, Il. color. Disponível em: https://www.calculoexato.net/codigo-binario/. Acesso em: 10 abr. 2020.

Para reverter o processo, ou seja, converter o número binário 11011001 em número decimal, tem-se:

$$1\,x\,2^7 + 1\,x\,2^6 + 0\,x\,2^5 + 1\,x\,2^4 + 1\,x\,2^3 + 0\,x\,2^2 + 0\,x\,2^1 + 1\,x\,2^0 =$$
$$1\,x\,128 + 1\,x\,64 + 0\,x\,32 + 1\,x\,16 + 1\,x\,8 + 0\,x\,4 + 0\,x\,2 + 1\,x\,1 =$$
$$128 + 64 + 0 + 16 + 8 + 0 + 0 + 1 = 217$$

Atualmente, um *byte* é composto por 8 *bits*, compreendendo 256 caracteres e cada letra, número ou símbolo equivale a um número binário de 8 dígitos. Com isso, possibilita diversas combinações de dígito para representar diversas informações, como números, palavras, cálculos, etc.

As tabelas ASCII fornecem os números binários que correspondem ao sistema decimal, alfabeto e símbolos diversos, utilizados para entradas de textos que compreendam todas as representações utilizadas na comunicação e informação. No entanto, sem perda de generalidade, mas através da tabela 9 (ASCII) para o alfabeto maiúsculo e minúsculo, pode-se ter uma noção da aplicabilidade da matemática neste processo criptográfico.

Por exemplo, para escrever **CIFRA** em números binários, conforme a tabela 9, tem-se a sequência de bits:

01000011 01001001 01000110 01010010 01000001.

Além disso, para melhor compreensão, Ganassoli (2015), ressalta dois exemplos. O primeiro utiliza-se do método de transposição e o segundo de substituição. No primeiro caso a regra consistem em trocas dos pares da sequência, onde o primeiro troca com o segundo, o terceiro com o quarto, e assim por diante. Logo podemos criptografar a palavra **CIFRA**, da seguinte maneira:

Palavra original: **01000011 01001001 01000110 01010010 01000001**
Palavra cifrada: **10000011 10000110 10001001 10100001 10000010**

No segundo método, escolhe-se uma palavra chave com a mesma quantidade de letras da palavra **CIFRA**, por exemplo, **ALUNO**. E aplica-se o algoritmo de substituição, se os dígitos das sequências das palavras transcritas em números binários forem iguais será representado por 0, caso sejam diferentes, a representação será dada pelo número 1. Assim, obtém-se na seguinte palavra cifrada:

Palavra original: **01000011 01001001 01000110 01010010 01000001**

Palavra-chave: **01000001 01001100 01010101 01001110 01001111**

Palavra cifrada: **00000010 00000101 00010011 00011100 00001110**

Além do mais, destacam-se as seguintes informações:

> Em 1970, Horst Feistel desenvolveu um dos algoritmos de cifragem mais usados, conhecido como Lucifer, no qual o emissor e o receptor só precisavam escolher um número para decidir qual chave seria usada. Uma versão de 56 *bits* da cifra Lucifer foi oficialmente adotada e batizada como Padrão de Cifragem de dados (DES–*Data Encryption Standard)*. A DES garantia a segurança das mensagens, encorajando as empresas a utilizarem a criptografia, havia apenas um problema, a distribuição de chaves. (GANASSOLI, 2015, p. 21).

Dessa forma, torna-se indispensável a abordagem desse sistema à criptografia, inclusive para os alunos técnicos em informática, uma vez que estão familiarizados a essa forma de representação. Logo, entender o sistema binário torna-se fundamental para a completa compreensão da aplicabilidade da criptografia em matemática, sendo concretizado através da conversão para a linguagem computacional.

Cabe ressaltar que todas as cifras obtidas, anteriormente, podem ser convertidas utilizando a tabela 9 (ASCII), sejam textos cifrados em números ou letras.

Contudo, qualquer aluno do ensino médio, especialmente do curso de Informática, poderá compreender melhor a associação dos números binários à criptografia e ter a noção do grande número de possibilidades em criar chaves e algoritmos para cifrar mensagens.

Para finalizar, as propostas apresentadas a seguir, tem como base as atividades de Ganassoli (2015) sobre números binários, utilizando-se a tabela 9 (ASCII). Tem-se:

i. O professor poderá criar situação-problema apresentando mensagens criptografadas através de postagens em redes sociais utilizando o código binário. O objetivo da questão é instigar os alunos a conseguirem decifrar a mensagem;

Espera-se que os alunos dividam a cifra em grupos de 8 blocos e pesquisem quais letras correspondem na tabela ASCII, transcrevendo a mensagem.

ii. Sugerir aos alunos que escolham uma palavra pra cifrar através do método de substituição, conforme visto no exemplo. Para isso, deverão utilizar a palavra-chave, previamente, escolhida pelo professor para a tarefa;

Espera-se que os alunos escolham livremente suas palavras e junto com a palavra-chave, transformem em código ASCII, aplicando a regra de substituição.

iii. Uma outra versão desta questão é fornecer ao aluno a palavra-chave e a mensagem cifrada. O objetivo é decifrar e descobrir a mensagem original, ou seja, aplicar o raciocínio lógico para reverter o processo;

Espera-se dos alunos que eles analisem a mensagem cifrada e concluam que se for zero, os dígitos serão iguais e ser for 1, os dígitos serão diferentes, assim descobrirá a mensagem original em números binários, bastando para isso consultar a tabela 9, a fim de compreender o que a mensagem representa.

iv. O professor ou os grupos de alunos poderão escolher uma palavra para aplicar o método de transposição e criar suas próprias regras, conforme exemplificado.

4.10 A Criptografia no Ensino de Aritmética Modular

A Aritmética Modular, não faz parte do conteúdo programático do ensino médio, porém é imprescindível que ela seja objeto de análise neste capítulo. Primeiro por estar presente de forma implícita em diversos conteúdos, bem como requisito básico em várias técnicas criptográficas, como vistas até aqui. Segundo por ser base de um dos mais importantes métodos de código da história, a criptografia RSA.

Segundo Coltinho (2014), Singh (2014), Hefez (2013) e Crilly (2017), todos os autores abordaram o método criptográfico, cuja base consiste em encontrar dois grandes números primos*, p* e *q*, em que o produto entre eles resulta no valor de *N.* De acordo com Hefez (2013, p. 140), “Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo”.

Para facilitar a ideia do método, suponha que Beto escolha para *p* e *q*, os seguintes valores primos: *p* = 17 e *q* = 11. Logo, o produto entre eles corresponde a *N* = *p.q,* cujo resultado é *N* = 17x11 = 187. A escolha de Beto resultou na chave de cifragem pública *N,* que poderá ser divulgada na Internet, publicada num diretório de chaves públicas de valores *N* de outras pessoas ou outros meios de comunicação. Contudo Beto mantém em segredo os valores de *p* e *q*.

Ela também escolhe outro valor que também será público, $e = 7$. Sendo que $(e, \varphi(m)) = 1$. Onde $\varphi(m) = (p-1)(q-1)$, em que e e $\varphi(m)$ são primos entre si. O

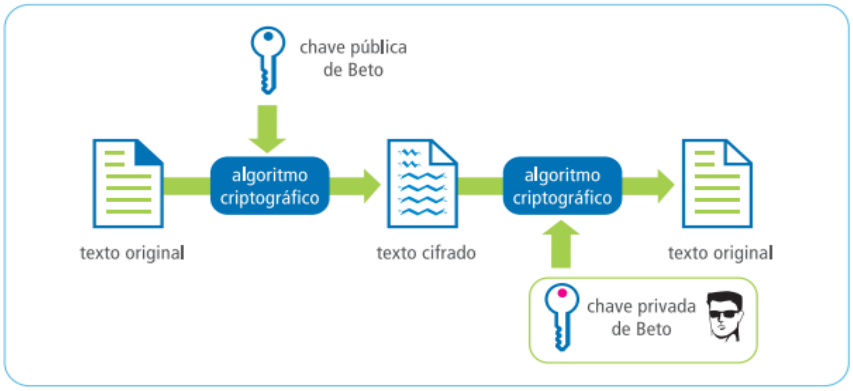
que significa que entres eles não há divisores comuns, exceto o 1, ou seja, o máximo divisor comum (mdc) entre eles é 1.

Assim $\varphi(m)$ é dado por: $\varphi(m) = (p-1)(q-1) \rightarrow (17-1)(11-1) = 16x10 = 160$.

Logo, $(e, \varphi(m)) = (7,160) = 1$, satisfaz as condições de primos entre si.

Enfim, *N* e e, são chamados de *chaves públicas* e *p* e *q* são as *chaves privadas* de Beto, observe figura 9 do esquema de chave assimétrica.

Figura 9 – Esquema de Chave assimétrica do algoritmo RSA



Fonte: Revisa de Empreendedorismo, Inovação e Tecnologia[8]

Na sequência, se Bob quiser enviar uma mensagem cifrada para Beto, ele precisará usar a chave pública *N* na função de mão única que também será de conhecimento público.

Em Números Inteiros e Criptografia RSA por Coltinho (2014), mostra como converter letras de uma mensagem a ser cifrada em números e denomina essa fase de pré-codificação. A conversão de letras em números é dada pela tabela 10 de conversão.

Ainda, no processo de pré-codificação, têm-se algumas considerações a observar:

- Os espaços entre as palavras serão substituídos pelo número 99;

[8] LADEIRA, Ricardo de La Rocha; RAUGUST, Anderson Schwede. **Uma análise da complexidade do algoritmo RSA implementado com o teste probabilístico de Miller-Rabin**. In: Revista de empreendedorismo, Inovação e tecnologia, Passo Fundo, vol. 4, n. 1 p. 24-33, Jan.-Jun. 2017 - ISSN 2359-3539 DOI: https://doi.org/10.18256/2359-3539/reit-imed.v4n1p24-33. Disponível em: https://seer.imed.edu.br/index.php/revistasi/article/view/1639/1296. Acesso em 06 jun. 2020.

- Os valores adotados na tabela a partir de dois algarismos evita ambiguidades, pois se A for 1 e B, 2, o código 12 não deixará claro se refere a L ou AB (localizado na posição 12ª do alfabeto);
- Ao unir os números pré-codificados, a separação por bloco, como veremos, será menor que o valor de *N.*
- Ao separar em blocos, evita-se iniciar um bloco com o algarismo 0.

Logo a seguir, tem-se a última fase da pré-codificação, que consiste em separar os números obtidos pelo processo de conversão em blocos, em que o valor de cada bloco será menor que *N*.

Tabela 10 – Conversão numérica para o sistema RSA

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: Adaptado pelo autor de O livro dos Códigos

Como exemplo, suponha que Bob deseje transmitir a Beto a frase:

AMO A OBMEP, fazendo a conversão, conforme a tabela 10, tem-se:

10222499109924112221425

Separando em blocos, que não precisa ser, obrigatoriamente, de uma única maneira e lembrando que *N* = 187, temos:

102 - 22 - 49 - 9 - 109 - 92 - 41 - 12 - 21 - 42 – 5

No Programa de Iniciação Cientifica, Coltinho (2007) observa ainda que, como cada bloco não representa necessariamente uma unidade linguística, então a decodificação por análise de frequência também seria impossível.

Iniciando o processo de codificação, propriamente dito, faz-se a cifragem em cada bloco e a mensagem criptografada será a sequência dos blocos codificados, nessa ordem.

O cálculo de cada bloco é dado por C(*b*) = resto da divisão de b^e por *N,* ou seja, pela aritmética modular, podemos calcular por meio da seguinte fórmula:

$$C(b) \equiv b^e (mod\ N)\ ,$$

sendo *N* = 187 e $e = 7$.

Para Coltinho(2014), o par *(n,e)*, utilizado na fórmula do sistema RSA é denominado de *Chave de Codificação*. Para facilitar o processo, usaremos a aritmética modular no primeiro bloco e apresentaremos os resultados dos demais blocos utilizando a calculadora científica:

$C(b) \equiv b^e (mod\ N)$,

$C(102) \equiv 102^7 \equiv 102^4 \text{x} 102^2 x102 \equiv 108.243.216x10404x102(mod187)$

$\equiv 136x119x102(mod187) \equiv 1.650.768 \equiv \mathbf{119}\ (mod\ 187)$

$C(22) \equiv 22^7 \equiv \mathbf{44}\ (mod\ 187)$

$C(49) \equiv 49^7 \equiv \mathbf{25}\ (mod\ 187)$

$C(9) \equiv 9^7 \equiv \mathbf{70}\ (mod\ 187)$

$C(109) \equiv 109^7 \equiv \mathbf{131}\ (mod\ 187)$

$C(92) \equiv 92^7 \equiv \mathbf{148}\ (mod\ 187)$

$C(41) \equiv 41^7 \equiv \mathbf{46}\ (mod\ 187)$

$C(12) \equiv 12^7 \equiv \mathbf{177}\ (mod\ 187)$

$C(21) \equiv 21^7 \equiv \mathbf{98}\ (mod\ 187)$

$C(42) \equiv 42^7 \equiv \mathbf{15}\ (mod\ 187)$

$C(5) \equiv 5^7 \equiv \mathbf{146}\ (mod\ 187)$

Portanto a união de todos os blocos resulta na mensagem cifrada:

119 – 44 – 25 – 70 – 131 – 148 – 46 – 177 – 98 – 15 – 146

Como Beto conhece os valores de *p* e *q*, ela calcula o valor de um número particular *d*, conhecido como a chave da decifragem. Para decodificar a mensagem, basta inserir na função

$$ed \equiv 1(mod(\varphi(m)) \rightarrow 7d \equiv 1(mod\ 160)$$

Pode-se resolver aplicando o algoritmo euclidiano estendido ou equação modular como se segue. Vale ressaltar que como o mdc (7,160) = 1, aplica-se a propriedade de congruência, multiplicando-se ambos os lados por um valor *c* = 23, pois dessa forma podemos chegar ao valor procurado *d.* Daí:

$$23.7d \equiv 23.1\ (mod 160)$$

$$161d \equiv 23(mod 160)$$

$$d \equiv 23\ (mod 160)$$

Logo *d* =23

Para decifrar a mensagem, Beto usa a seguinte função:

$$D(b) \equiv C^d (mod N)$$

Para facilitar o processo, usaremos a aritmética modular no primeiro bloco e apresentaremos os resultados dos blocos seguintes, utilizando a calculadora científica:

$D(119) \equiv 119^{23}(mod 187)$ → *agrupando dois a dois, temos:*

$\equiv 119^2 x 119^2 \ldots 119^2{}_{(11 vezes)} x 119^1 \ (mod 187)$

$\equiv 136^{11} x 119 \ (mod\ 187)$

$\equiv 136^2 x 136^2 \ldots 136^2{}_{5 vezes} x 136 x 119^1 \equiv (170)^5 x 16184 (mod 187)$

$\equiv 170^2 x 170^2 x 170 x 102 (mod 187) \equiv 102 x 102 x 17.340 \ (mod 187) \equiv 10.404 x 136$

$\equiv 119 x 136 \equiv 16.184 \equiv \mathbf{102} \ (mod 187)$;

$D(44) \equiv 44^{23}(mod 187) \equiv \mathbf{22} \ (mod 187)$;

$D(25) \equiv 25^{23}(mod 187) \equiv \mathbf{49} \ (mod 187)$;

$D(70) \equiv 70^{23}(mod 187) \equiv \mathbf{9} \ (mod 187)$;

$D(131) \equiv 131^{23}(mod 187) \equiv \mathbf{109} \ (mod 187)$;

$D(148) \equiv 148^{23}(mod 187) \equiv \mathbf{92} \ (mod 187)$;

$D(46) \equiv 46^{23}(mod 187) \equiv \mathbf{41} \ (mod 187)$;

$D(177) \equiv 177^{23}(mod 187) \equiv \mathbf{12} \ (mod 187)$;

$D(98) \equiv 98^{23}(mod 187) \equiv \mathbf{21} \ (mod 187)$;

$D(15) \equiv 15^{23}(mod 187) \equiv \mathbf{42} \ (mod 187)$;

$D(146) \equiv 146^{23}(mod 187) \equiv \mathbf{5} \ (mod 187)$;

Portanto a decifragem resulta na sequência de Blocos:

102 – 22 – 49 – 9 – 109 – 92 – 41 – 12 – 21 – 42 – 5

Fazendo a conversão dos códigos, pela tabela inicial, tomados dois a dois, temos:

10	**22**	**24**	**99**	**10**	**99**	**24**	**11**	**22**	**14**	**25**
A	**M**	**O**		**A**		**O**	**B**	**M**	**E**	**P**

Portanto, através deste algoritmo o processo torna-se revertido e obtém-se a mensagem original.

Observe na figura 4, capítulo 1, o algoritmo sintetizado do método de criptografia RSA.

É importante esclarecer aos alunos que no sistema RSA esquematizado “para pôr isso em funcionamento há muitas contas a serem feitas e isso só é possível com o uso de um computador. É também necessário ter acesso a números primos muito grandes e escolher com certo critério as chaves do sistema.” (HEFEZ, 2013, p.322). O autor também sugere que a mensagem seja traduzida para o código ASCII, o que torna mais interessante para o aluno de Ensino Médio técnico de Informática, principalmente, do curso Técnico, pois poderá treinar esta conversão utilizando de recursos tecnológicos, como o computador.

Stallings (2015), sugere como atividade de aplicação para o método RSA os seguintes exercícios. Dessa forma, os professores poderão aplicá-los em sala de aula a fim de proporcionar a prática do algoritmo, utilizando-se de valores possíveis de serem desenvolvidos por meio de calculadoras e com isso o aluno poderá contextualizar a base do complexo método do sistema RSA, veja:

1. Realize a encriptação e decriptação usando o algoritmo RSA, através da tabela 10 e a figura 4, para os seguintes valores:

   $a. p = 3;\ q = 11, e = 7\ ; M = 5$
   $b. p = 5;\ q = 11, e = 3\ ; M = 9$
   $c. p = 7;\ q = 11, e = 17\ ; M = 8$
   $d. p = 11;\ q = 13, e = 11\ ; M = 7$
   $e. p = 17; q = 31, e = 7; M = 2$

2. Em um sistema de chave pública usando RSA, você intercepta o texto cifrado $C = 10$ enviado a um usuário cuja chave pública é $e = 5\ , N = 35$. Qual o texto claro ***M***? (STALLING, 2015, p. 220).

Certamente pela complexidade da Criptografia RSA, cabe ao professor analisar a possibilidades de aplicar as atividades sugeridas pelo autor em sala de aula ou abordar a aplicação deste método de cifragem e decifragem.

Contudo, vale ressaltar que em decorrência da relevância que a teoria dos números tem para a criptografia, o professor poderá explorar a parte histórica que originou o método, demonstrar a aplicação e mostrar aos alunos o quanto a matemática é importante neste processo, bem como mostrar o quanto este método criptográfico contribui na segurança das Tecnologias da Informação e Comunicações, interferindo positivamente no dia a dia das pessoas usuárias desses recursos.

5 CONSIDERAÇÕES FINAIS

As Tecnologias da Informação e Comunicação – TICs estão inseridas na sociedade de forma global, parte deste avanço se deve à segurança em que as trocas de mensagens, compras online, transações bancárias, comunicação em redes sociais entre outros meios gerados pela conectividade, ocorre de forma segura. Notavelmente, é a criptografia que garante a confiabilidade dessas relações.

A evolução da criptografia, relatada nesta revisão bibliográfica e documental, constata-se que os avanços conquistados no decorrer do tempo foram motivados pelo empenho dos criptógrafos em garantir a segurança nas trocas de mensagens. Primeiro, nos primórdios da civilização, no curso de grandes guerras, proteção de comunicações militares e diplomáticas, entre outros importantes fatos históricos da humanidade e, em segundo, em transações e comunicações atuais, que se popularizaram nas relações comerciais, econômicas e pessoais, onde se requer um sistema de alta segurança e confiabilidade.

Nesse contexto, todos os importantes acontecimentos registrados pela história, resultou em sucessivas inovações de técnicas criptográficas e de criptoanálise. Pois a cada código decifrado por criptoanalistas, impulsionavam aos criptógrafos a encontrar cifras mais fortes e seguras. Resultado disso associado com a evolução das TICs é o que permite aos usuários dispor de comunicações visando o mais alto nível de confiabilidade.

Diante deste processo, é fundamental destacar que tanto a evolução criptográfica quanto os avanços tecnológicos dos meios de comunicação tiveram a matemática como a grande protagonista, principalmente, como base para criar novas cifras, aprimorar códigos e encontrar formas para quebrá-lo.

Isso posto e levando em consideração que os alunos pertencem a denominada Sociedade da Informação, logo trazem consigo habilidades apropriadas para lidarem com as tecnologias, além de cursarem o Técnico de Informática integrado ao médio. Então, naturalmente, infere-se que tenham o conhecimento necessário sobre a segurança da informação e dos conceitos de algoritmos inerentes a sua formação, assim espera-se que a aplicabilidade da criptografia reforce o interesse pela disciplina e que seja fascinante descobrir que a matemática é o embasamento teórico das técnicas criptográficas presentes em seu dia a dia.

Portanto, pesquisar a história da criptografia e da educação profissional no Brasil foi fundamental para compreender os parâmetros traçados à educação. Dessa forma, associar a aplicabilidade no ensino da matemática no contexto da educação profissional, primou pelo emprego da interdisciplinaridade, pois através desta interação, os conteúdos de funções, matrizes, aritmética, analíse combinatória entre outros com a disciplina de informática, alcançará resultados relevantes no contexto do ensino médio integrado ao técnico.

Porém, a pesquisa além de atingir os objetivos gerais através das propostas de atividades em sala de aula, ultrapassam os limites pré-estabelecidos, pois podem ser empregados no ensino médio e até nas últimas séries do fundamental, uma vez que o currículo de matemática é base comum.

Com base nesses estudos, procurou-se aqui o embasamento legal para verificar que a educação profissional está adequada com o que se pretende de uma educação de qualidade, onde se prima pela valorização da formação plena, omnilateral, com o intuito de prepará-lo para a inserção social, estabelecer novas oportunidades e que todos sejam educados nesta perspectiva.

Por fim, após a análise sobre a aplicabilidade de criptografia no ensino da matemática, pôde-se inferir que é uma temática com inúmeras possibilidades de investigação dos conteúdos matemáticos, particularmente no ensino médio. Prova disso, tem sido as diversas propostas apresentadas como aplicação em sala de aula. Assim o professor de matemática, poderá dispor destas sugestões, além de poder utilizar a ideia básica para adequar às suas aulas inovando ao valer-se dos recursos de criptografia para melhor compreensão dos conteúdos de matemática, despertando curiosidade e motivação.

Cabe ainda ressaltar que, em virtude do período de pandemia da Covid-19, que assola o Brasil e o mundo, infelizmente, não foi possível realizar as aplicações práticas dos métodos sugeridos. Contudo, apesar das aulas ocorrerem de forma remota, o que se pretende é dar continuidade à pesquisa, aplicando a proposta no âmbito da sala de aula.

Enfim, desenvolver este tema com esta finalidade além de contribuir para o ensino da matemática, também enriquece o desenvolvimento profissional do professor, bem como tem impactado positivamente na minha formação, contribuindo no incentivo à pesquisa, pois é vasto e inesgotável o tema. Prova dessa teoria é o sistema RSA, considerado o mais seguro e usado na atualidade, podendo ser objeto

de pesquisa com o objetivo de encontrar uma solução para a fatoração do produto de dois grandes números primos e assim, apesar de uma teoria simples da Aritmética seria uma descoberta extraordinária.

REFERÊNCIAS

BRAGATO, Josiane. Os Institutos Federais de Educação, Ciência e Tecnologia: Inovação da política de Educação Profissional no Brasil? *In*: CONGRESSO NACIONAL DE EDUCAÇÃO, 5., 2018, Centro de Convenções de Olinda. **Anais** [...]. Pernambuco: Universidade Federal Fluminense (UFF), 2018. *Online.* Disponível em: http://www.editorarealize.com.br/revistas/conedu/trabalhos/TRABALHO_EV117_MD1_SA3_ID7201_10092018230725.pdf. Acesso em: 03 abr. 2020.

BRANDT, Celia Finck; MORETTI, Méricles Thadeu (orgs.). **Ensinar e aprender matemática:** possibilidades para a prática educativa. Ponta Grossa: Editora UEPG. 2016. *E-book.* ISBN 978-78-7798-215-8.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2020 .Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 mar. 2020.

BRASIL. **Lei nº 9.394, de 20 de dezembro de 1996**. Estabelece as diretrizes e bases da educação nacional. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 12 de mar. de 2020.

BRASIL. **Lei nº 11.741, de 16 de julho de 2008**. Altera dispositivos da Lei nº 9.294, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional, para redimensionar, institucionalizar e integrar as ações da educação profissional técnica de nível médio, da educação de jovens e adultos e da educação profissional e tecnológica. Brasília, DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11741.htm. Acesso em: 07 mar. 2020.

BRASIL. **Lei nº 11.892, de 29 de dezembro de 2008**. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Brasília, DF: Presidência da República, [2008]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11892.htm. Acesso em: 07 de mar. 2020.

BRASIL. **Lei nº 12.711, de 29 de agosto de 2012**. Dispõe sobre o ingresso nas universidades federais e nas instituições federais de ensino técnico de nível médio e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12711.htm. Acesso em: 07 de mar. 2020.

BRASIL. **Decreto nº 2.208, de 17 de abril de 1997**. Regulamenta o § 2º do art. 36 e os arts. 39 a 42 da Lei nº 9.9394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional. Brasília, DF: Presidência da República, [1997]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2208.htm. Acesso em 10 mar. 2020.

BRASIL. **Decreto nº 5.154, de 23 de julho de 2004.** Regulamenta o § 2º do art. 36 e os arts. 39 a 41 da Lei nº 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional, e dá outras providências. Brasília, DF: Presidência da República, 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5154.htm#art9. Acesso em: 12 de mar. de 2020.

BRASIL. **Parâmetros Curriculares Nacionais para o Ensino Médio**: Bases Legais. Brasília: MEC, 2000. Disponível em: http://portal.mec.gov.br/seb/arquivos/pdf/14_24.pdf. Acesso em: 15 de mar. 2020.

BRASIL. **Parâmetros Curriculares Nacionais para o Ensino Médio (PCN+)**: Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais. Brasília: MEC, 2002. Disponível em: http://portal.mec.gov.br/seb/arquivos/pdf/CienciasNatureza.pdf. Acesso em: 12 mar. 2020.

BRASIL, Ministério da Educação (MEC). **Instituto Federal Concepções e Diretrizes.** Brasília: DF, [2016]. Disponível em: http:// http://redefederal.mec.gov.br/historico. Acesso em: 12 de mar. 2020.

BRASIL, Ministério da Educação (MEC). **Instituições da Rede Federal.** Brasília: DF, [2016]. Disponível em: http://portal.mec.gov.br/rede-federal-inicial/instituicoes. Acesso em: 12 de mar. 2020.

BRASIL, Ministério da Educação (MEC). **Centenário da Rede Federal**. Brasília: DF, 2017. Disponível em: http://redefederal.mec.gov.br/centenario-da-rede-federal. Acesso em: 12 mar. 2020.

BRASIL, Ministério da Educação (MEC). **Histórico**. Brasília: DF, 2016.Disponível em: http://redefederal.mec.gov.br/historico. Acesso em: 12 mar. 2020.

CENTRO DE ESTUDOS RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.Br). **Cartilha de Segurança para Internet** Parte 01: Conceitos de Segurança. Online, Portuguese Edition, 2005.

CIAVATTA, Maria; RAMOS, Marise. Ensino Médio e Educação Profissional no Brasil: dualidade e fragmentação. **Retratos da Escola**, 2011. v. 5, n. 8, p. 27-41. *online*. Disponível em: http://retratosdaescola.emnuvens.com.br/rde/article/view/45. Acesso em: 02 mar. 2020.

COUTINHO, Severino C. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2014.

COUTINHO, S. C. **Criptografia**. Programa de Iniciação Científica da OBMEP. Rio de Janeiro, 2007. v. 7.

CRILY, Tony. **50 Ideias de Matemática que você precisa conhecer**. São Paulo: Planeta, 2017.

D’AMBROSIO, Beatriz S**. Formação de professores de matemática para o século XXI***:* o grande desafio*.* Campinas: Pró-Posições, 1993. v. 4, n. 1, p. 10. Disponível em: https://www.fe.unicamp.br/pf-fe/publicacao/1757/10-artigos-ambrosiobs.pdf. Acesso em: 20 fev. 2020.

DANTE, Luiz Roberto. **Matemática.** São Paulo: Ática, 2008.

FRIGOTTO, Gaudêncio**. A relação da educação profissional e tecnológica com a universalização da educação básica**. Campinas: Educação & Sociedade, 2007*.* v. 28, n. 100, p. 1129-1152. ISSN 1678-4626. *Online*. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-73302007000300023&lng=pt&tlng=pt. Acesso em: 10 mar. 2020.

GANASSOLI, Ana Paula; SCHANKOSKI, Fernanda Ricardo. **Criptografia e Matemática.** 2015. Dissertação (Mestrado em Matemática) – Departamento de Matemática, Universidade Federal do Paraná, Curitiba, 2015. Disponível em: http://www.educadores.diaadia.pr.gov.br/arquivos/File/fevereiro2016/matematica_dissertacoes/dissertacao_fernanda_ricardo_scankoski.pdf. Acesso em: 24 mar 2020.

HEFEZ, Abramo. **Aritmética***.* Rio de Janeiro: SBM, 2014.

IBGE (PNAD-CONTÍNUA)**. Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal**, 2017. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 12 mar. 2020.

INSTITUTO FEDERAL DE EDUCAÇÃO DE CIÊNCIAS E TECNOLOGIA DE RONDÔNIA**. Resolução nº 3/REIT - CEPEX/IFRO, de 02 de janeiro de 2019.** Dispõe sobre a aprovação da Reformulação do Projeto Pedagógico do Curso Técnico em Informática Integrado ao Ensino Médio do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Campus Cacoal. Disponível em : file:///C:/Users/Josi/Downloads/Resoluo%20n%203%20-%20PPC%20Tc.%20em%20Informtica%20Integrado%20CACOAL%20(4).pdf. Acesso em: 12 de mar. 2020.

KUENZER, Acacia Zeneida. **Trabalho e escola:** A flexibilização do ensino médio no contexto do regime de acumulação flexível. Campinas: Educação & Sociedade, 2017. v. 38, n. 139, p. 331-354. ISSN 1678-4626. https://doi.org/10.1590/es0101-73302017177723. *Online.* Disponível em: https://www.scielo.br/scielo.php?pid=S0101-73302017000200331&script=sci_abstract&tlng=pt. Acesso em: 12 mar. 2020.

LIMA, Elon Lages. **Números e Funções Reais.** Rio de Janeiro: SBM, 2013.

PAIVA, Francisco da Silva. Ensino técnico: uma breve história. **Revista Húmus**, Maranhão, v. 3, n. 8, 2013. ISSN: 2236-4358. versão *online*. Disponível em: http://www.periodicoseletronicos.ufma.br/index.php/revistahumus/article/view/1677 . Acesso em: 10 fev. 2020.

PEREIRA, Nádia Marques Ikeda. **Criptografia:** uma nova proposta de ensino de matemática no ciclo básico. 2015. Dissertação (Mestrado em Matemática) – Instituto de Biociências, Letras e Ciências Exatas, Faculdade Júlio de Mesquita Filho, Universidade Estadual Paulista, São José do Rio Preto, 2015. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/127733/000844677.pdf?sequence=1&isAllowed=y. Acesso em: 10 fev. 2020.

PILETTI, Claudino; PILETTI, Nelson. **História da Educação**. São Paulo: Contexto, 2014.

SAVIANI, Dermeval. O trabalho como princípio educativo frente às novas tecnologias. In: SAVIANI, Dermeval. **Novas tecnologias, trabalho e educação**: um debate multidisciplinar. Petrópolis: Vozes, 1994. p. 147-164.

SINGH, Simon. **O Livro dos Códigos***:* a ciência do sigilo - do antigo Egito à criptografia quântica. 10. ed. Rio de Janeiro: Record, 2014.

SOUSA, Robson Pequeno de; MOITA, Filomena da M.C. da S. C.; CARVALHO, Ana Beatriz Gomes (orgs.). **Tecnologias digitais na educação**. Campina Grande: EDUEPB, 2011. *E-book.*

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education, 2015.

TAMAROZZI, Antônio Carlos. Codificando e Decifrando mensagens. In: Druck, Suely (ORG). **Coleção Explorando o Ensino Matemática**: Ensino Médio. Brasília. Ministério da Educação Secretaria de Educação Básica, v.3, p.69-72, 2004.